Slides week 19

Algebraic Structures

Paula Lins

University of Lincoln

Lecture Slides

2024/25

Week 19: Goals

Last time:

- Subrings,
- Quick Subring Theorem,
- Zero divisors and Integral Domains.

Today:

- Reminder: Rings, subrings, zero divisors and Integral Domains.

Reminder: Ring Theory

Rings

A ring is a set R with **two** operations (usually denoted by) $+$ and $\cdot$ satisfying:

- R with $+$ is an abelian group,
- R is closed with respect to $\cdot$, (i.e. $a \cdot b \in R$, $\forall a, b \in R$)
- $\cdot$ is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
- For all $a, b, c \in R$, the **distributive laws** hold:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \text{ and } (a + b) \cdot c = a \cdot c + b \cdot c.$$

Notation.

Suppose R is a set.

If R is a ring with certain operations $\oplus$ and $\odot$, we write $(R, \oplus, \odot)$.

That is, we write $(R, \oplus, \odot)$ to specify the operations of R.

Additive group and multiplication

Let $(R, +, \cdot)$ be a ring.

- The group $(R, +)$ is called the **additive group** of R.
- the additive identity element 0_R is called the **zero** of the ring R.
- In general, R with multiplication is **not** a group. (Not necessarily has identity or inverses)

Examples of rings: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$

Example.

$(\mathbb{Z}, +, \cdot)$ is a ring. We already know that $(\mathbb{Z}, +)$ is an abelian group. Note that $(\mathbb{Z}, \cdot)$ is **not a group**, however, we have

- $\mathbb{Z}$ is closed with respect to $\cdot$,
- $\cdot$ is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for all $a, b, c \in \mathbb{Z}$,
- The **distributive laws** hold:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \text{ and } (a + b) \cdot c = a \cdot c + b \cdot c.$$

Example.

Similarly as for $(\mathbb{Z}, +, \cdot)$, one can show that the following are rings:

$$(\mathbb{Q}, +, \cdot), \qquad (\mathbb{R}, +, \cdot), \qquad (\mathbb{C}, +, \cdot).$$

Polynomial Rings

Let $\mathbb{R}[x]$ be the set of all polynomials in x:

$$\mathbb{R}[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in \mathbb{R},\ n \in \mathbb{N} \cup \{0\}\}.$$

This is a ring with sum and multiplication of polynomials:

$$(f+g)(x) = f(x) + g(x) \quad \text{and} \quad (f \cdot g)(x) = f(x) \cdot g(x).$$

Polynomials Rings

Similarly, we define the rings of polynomials with complex, rational and integer coefficients: $\mathbb{C}[x]$, $\mathbb{Q}[x]$, and $\mathbb{Z}[x]$.

Polynomial rings are **commutative** rings, that is, $a \cdot b = b \cdot a$.

More examples of rings from last time

- The integers mod n: $(\mathbb{Z}_n, +, \cdot\,)$.
- The set of 2×2 matrices with entries in $\mathbb{R}$: $(\mathrm{Mat}(2, \mathbb{R}), +, \cdot, \,)$.
- The set of multiples of n: $(n\mathbb{Z}, +, \cdot)$.

Remark

- $(\mathrm{Mat}(2, \mathbb{R}), +, \cdot, \,)$ is a ring that is **not** commutative and **does not** have all multiplicative inverses.
- $(n\mathbb{Z}, +, \cdot)$ is a ring **without** unity.

Subings

Definition.

Let $(R, +, \cdot)$ be a ring.

We say that a subset $S \subset R$ is a **subring** if $(S, +, \cdot)$ is itself a ring.

Notation: $S \leq R$.

As in the case of groups, there is a quicker way to show that a subset $S \subseteq R$ of a ring $(R, +, \cdot)$ is a subring.

Quick Subring Theorem (QST)

Quick Subring Theorem (QST)

A subset S of a ring R is a subring if and only if

1. S is non-empty,
2. S is closed under both addition and multiplication of R, and
3. S contains the negative (i.e. the additive inverse) of each of its elements.

Example

Last time, we applied the QST to show that the Gaussian numbers

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

form a subring of $\mathbb{C}$.

Example

3. **Closed under multiplication:** Given $a+bi, c+di \in \mathbb{Z}[i]$, we must show $(a+bi)\cdot(c+di) \in \mathbb{Z}[i]$.

$$(a+bi)\cdot(c+di) = (ac-bd)+(ad+bc)i \in \mathbb{Z}[i]$$

   because $ac-bd$, $ad+bc \in \mathbb{Z}$.

4. **Negatives:** Given $a+bi \in \mathbb{Z}[i]$, we must show that the additive inverse of $a+bi$ also belongs to $\mathbb{Z}[i]$.

$$-(a+bi) = -a-bi = -a+(-b)i \in \mathbb{Z}[i]$$

   because $-a$, $-b \in \mathbb{Z}$.

Thus, $(\mathbb{Z}[i], +, \cdot)$ is a subring of $\mathbb{C}$.

Zero Divisors

Zero Divisors: an example

Example

In $\mathbb{Z}$, we have

$$\text{If } x \neq 0 \text{ and } y \neq 0, \text{ then } xy \neq 0.$$

That is, if we multiply non-zero numbers, we obtain a non-zero number.

However, in $\mathbb{Z}/4\mathbb{Z}$, we have

$$\overline{2} \neq \overline{0} \quad \text{but} \quad \overline{2} \cdot \overline{2} = \overline{4} = \overline{0}.$$

This property has a name: we say $\overline{2}$ is a **zero divisor** in $\mathbb{Z}/4\mathbb{Z}$.

(We also say that $\mathbb{Z}$ has no zero divisors.)

Zero Divisors

Definition

Let R be a commutative ring (i.e. $a \cdot b = b \cdot a$ in R).

We say an element $r \in R$ is a **zero divisor** if $a \cdot b = 0$ for some element $b \neq 0$ of R.

Example

In $\mathbb{Z}/12\mathbb{Z}$, we have

- $\overline{2}$ is a zero divisor because $\overline{2} \neq \overline{0}$ and $\overline{2} \cdot \overline{6} = \overline{0}$ (and $\overline{6} \neq \overline{0}$),
- $\overline{3}$ is a zero divisor because $\overline{3} \neq \overline{0}$ and $\overline{3} \cdot \overline{4} = \overline{0}$ (and $\overline{4} \neq \overline{0}$).

This also shows that $\overline{6}$ and $\overline{4}$ are zero divisors.

Examples in $\mathbb{Z}/4\mathbb{Z}$

In $\mathbb{Z}/4\mathbb{Z}$, we have

- $\overline{1}$ is **not** a zero divisor because

$$\overline{1}\cdot\overline{1}=\overline{1},\quad \overline{1}\cdot\overline{2}=\overline{2},\quad \overline{1}\cdot\overline{3}=\overline{3}.$$

- $\overline{2}\cdot\overline{2}=\overline{0}$, thus $\overline{2}$ is a zero divisor.

- $\overline{3}$ is **not** a zero divisor because

$$\overline{3}\cdot\overline{1}=\overline{3},\quad \overline{3}\cdot\overline{2}=\overline{2},\quad \overline{3}\cdot\overline{3}=\overline{1}.$$

Integral domains

Integral domains

Definition

Let R be a **commutative** ring with **unity**.

We say that R is an **integral domain** if R has no zero divisors.

Example

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are integral domains:

- They are commutative,
- Their unity is 1,
- $a \cdot b = 0$ if and only if $a = 0$ or $b = 0$.

Non-Examples

$\mathbb{Z}/9\mathbb{Z}$ is not an integral domain

Although $\mathbb{Z}/9\mathbb{Z}$ is commutative and has unity $\overline{1}$, it is not an integral domain because

$$\overline{3} \cdot \overline{3} = \overline{0} \quad \text{and} \quad \overline{3} \neq \overline{0}.$$

$\mathrm{Mat}(2, \mathbb{R})$

$\mathrm{Mat}(2, \mathbb{R})$ is **not** an integral domain because it is not commutative.

$\mathbb{Z} \times \mathbb{Z}$

$\mathbb{Z} \times \mathbb{Z}$ is **not** an integral domain because it has zero divisors:

$$(1, 0) \cdot (0, 1) = (0, 0).$$

(However, it is commutative and the unity is $(1, 1)$.)

Examples from last time

$\mathbb{Z}/n\mathbb{Z}$

Exercise: Show that if n is not a prime, then $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain.

Exercise: Show that if p is prime, then $\mathbb{Z}/p\mathbb{Z}$ is an integral domain.

$\mathbb{Z}[x]$ is an integral domain

Last time, we showed that $\mathbb{Z}[x]$ is an integral domain.

Similarly, $\mathbb{C}[x]$, $\mathbb{R}[x]$ and $\mathbb{Q}[x]$ are also integral domains.

Cancellation laws

Lemma.

Let D be an integral domain with $a, b, c \in D$.

If $a \neq 0$, then

$$ab = ac \quad \text{implies } b = c.$$

Similarly,

$$ba = ca \quad \text{implies } b = c.$$

Proof.

$$\begin{aligned} ab = ac &\Longrightarrow ab - ac = 0 \\ &\Longrightarrow a(b - c) = 0 \end{aligned}$$

Now, since D is an integral domain, we must have $a = 0$ or $b - c = 0$.

We know that $a \neq 0$ so that $b = c$. □

Cancellations do not work in non-integral domains

Remark.

If R is a ring that is not an integral domain, then **cancellation laws might not work!**

Example

$\mathbb{Z}/12\mathbb{Z}$ is not an integral domain because $\overline{2} \cdot \overline{6} = \overline{0}$.

We have

$$\overline{4} \cdot \overline{1} = \overline{4} \quad \text{and} \quad \overline{4} \cdot \overline{4} = \overline{4},$$

however, we know that $\overline{1} \neq \overline{4}$.

So, cancellation does not work!

Next lecture

Next time...

- New algebraic structures: Fields!