Slides week 19

Algebraic Structures

Paula Lins

UNIVERSITY OF LINCOLN

Deep Dive Slides

2024/25

Detailed Slides

Deep Dive Slides

The **Deep Dive Slides** are essentially the same as the lecture slides, but with added information for your convenience.

While the lecture slides come with my explanations, the detailed notes are self-contained to help you study independently!

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

Ring Theory

- Last semester, after completing the group theory section of this module, we were introduced to a new algebraic structure called a **ring**.
- We learned that rings and groups share some similarities, particularly in their axioms (or the "rules" that govern them).
- The key difference is that a ring has **two operations** instead of just one!
- Consequently, there are axioms associated with each of these operations.

Rings

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

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 $(\mathbb{Z}, +, \dot{\ })$, one can show that the following are rings:

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

Polynomial Rings

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:

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

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, $a \cdot b = b \cdot a$.

Proof

Proof. If you interested, here is a quick proof that $\mathbb{R}[x]$ is a ring. (The details are left as exercise.) The proof that $\mathbb{C}[x]$, $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$ are rings follows the exact same steps.

Let us first show that $(\mathbb{R}[x], +)$ is an abelian group:

- **Closed:** We know that adding two polynomials with coefficients over $\mathbb{R}$ gives a polynomial over $\mathbb{R}$.
- **Associativity:** This follows from the associativity of $\mathbb{R}$. I will give one example to illustrate: consider

  $$f(x) = x^2 - 1, \qquad g(x) = x^3 + \sqrt{2}x - 1, \qquad h(x) = x.$$

  Then

  $$\begin{aligned} (f(x) + g(x)) + h(x) &= (x^3 + x^2 - \sqrt{2}x - 1) + x \\ &= x^3 + x^2 + (1 - \sqrt{2})x - 1 \\ &= x^2 - 1 + \Big(x^3 + (1 - \sqrt{2})x\Big) \\ &= f(x) + (g(x) + h(x)). \end{aligned}$$

Proof-Part 2

Proof. Continuation:

- **Identity element:** We see that the zero polynomial $\mathbf{0}(x) = 0$, $\forall x \in \mathbb{R}$ is the identity element.

- **(Additive) inverses:** Given a polynomial

$$f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$$

with $a_i \in \mathbb{R}$, we see that

$$g(x) = -a_m x^m - a_{m-1} x^{m-1} - \cdots - a_1 x - a_0$$

is the (additive) inverse of $f(x)$. In fact

$$f(x) + g(x) = \mathbf{0}(x) = g(x) + f(x).$$

Proof-Part 3

Proof. Continuation: We have shown that $(\mathbb{R}[x], +)$ is a group. We still need to show it is abelian. In fact, given two elements

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0,$$
$$g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$$

of $\mathbb{R}[x]$, we have that their sum is

$$(a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0) + (b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0).$$

For simplicity, assume $m \geq n$. Then we get

$$f(x) + g(x) = a_m x^m + \cdots + a_{n+1}x^{n+1} + \cdots + (a_n + b_n)x^n + \cdots + (a_0 + b_0).$$

Now, since $a_i + b_i$ is a sum of real numbers and $(\mathbb{R}, +)$ is a abelian, we know that $(a_i + b_i) = (b_i + a_i)$. Therefore, $f(x) + g(x)$ equals

$$= a_m x^m + a_{m-1}x^{m-1} + \cdots + (b_n + a_n)x^n + \ldots (b_1 + a_1)x + (b_0 + a_0)$$
$$= (b_n x^n + \cdots + b_1 x + b_0) + (a_m x^m + \cdots + a_1 x + a_0)$$
$$= g(x) + f(x).$$

Proof-Part 4

Proof. Continuation: Now we know $(\mathbb{R}[x], +)$ is an abelian group. We are left to show the last ring axioms:

- **Closed with multiplication:** We know that multiplying two polynomials with coefficients over $\mathbb{R}$ gives a polynomial over $\mathbb{R}$.

- **Associativity of multiplication:** Similar to the sum.

- **Distributivity:** This follows from the associativity of real numbers. Since the coefficients of the polynomials are real numbers, and real numbers are associative under addition and multiplication, the polynomials themselves are also associative

More examples of rings from last time

More examples of rings from last time

Last time, we showed that the following are rings.

- 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.

Subrings

Next slides: subrings and QST

- We will now recall the notion of a subring. Similarly to groups, if a ring contains a subset that is itself a ring (with the same operations), we call the subset a **subring**.
- We will also recall the **Quick Subring Theorem/Test (QST)**, which is very similar to the Quick Sub**group** Theorem.
- The QST provides a faster way to determine whether a subset is a subring without needing to verify all ring axioms.
- Given that there are eight axioms to check (five to show that the additive structure is an abelian group, plus the further three ring axioms), having such a criterion is incredibly useful!

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 - all steps

Example

Let us recall how to use the QST to check whether the Gaussian numbers

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

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

1. **Non-empty:** Here, we have to show that $\mathbb{Z}[i]$ has at least one element. The easiest is to give an example:

   $$0 = 0 + 0i \in \mathbb{Z}[i] \text{ because } 0 \in \mathbb{Z}.$$

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

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

   because $a + b$, $c + d \in \mathbb{Z}$.

Example

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

Next slides: Zero divisors

Zero divisors

1. Zero divisors are simply elements that are non-zero but if you multiply them, you get zero.
2. **Not** having zero divisors makes computations easier.
3. In fact, as we will see, the usual cancellation law is only valid in rings not having zero divisors.

   For instance, in $\mathbb{Z}_6$, we know that $\overline{2}$ and $\overline{3}$ are non-zero elements (i.e. 2 and 3 are not zero mod 6). However, $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0} \mod 6$. (In other words, they are zero divisors.)

   Note also that in $\mathbb{Z}_6$
   $$\overline{2} \cdot \overline{2} = \overline{2} \cdot \overline{5},$$
   however, we cannot cancel out $\overline{2}$ from both equalities, otherwise we get $\overline{2} = \overline{5}$ which is not the case mod 6.

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.

Zero Divisors: Examples in $\mathbb{Z}/4\mathbb{Z}$

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

Next slides: Integral Domains

Integral Domains

- In the next slides we will define and see examples of **integral domains**.
- An integral domain D is a ring that has the following properties:
  - it has unity 1_D,
  - it is commutative (i.e. $a \cdot b = b \cdot a$ for all $a, b \in D$),
  - it has **no** zero divisors.
- We will see at the end of the section that the cancellation law only holds for integral domains (but not for rings in general).
- Recall that the cancellation law says:

$$a \cdot b = a \cdot c \Longrightarrow b = c \quad \text{and} \quad \cdot a \cdot b = c \cdot b \Longrightarrow a = c.$$

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 law

Cancellation law

- In the next slide, we show that if a ring does not have zero divisors (for instance, integral domains), then the cancellation law holds.
- After that, we will see an example of a ring (having zero divisors) where cancellation law does not hold.
- again, the cancellation law is

$$a \cdot b = a \cdot c \Longrightarrow b = c \quad \text{and} \ \cdot a \cdot b = c \cdot b \Longrightarrow a = c.$$

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!