Slides week 23

Algebraic Structures

Paula Lins

University of Lincoln

Deep Dive Slides

2024/25

Deep Dive Slides

- These slides are similar to the lecture slides but include added motivations and explanations to enhance your learning experience.
- They are self-contained for independent study and do not provide additional material.
- Optional proofs are included (marked as optional).
- If you prefer a straightforward approach, you can study from the lecture slides without missing anything.

Week 21: Goals

Last time:

- Ideals,
- Principal Ideals,
- Quotient Rings,
- Field of Fractions.

Today:

- Characteristic of a ring,
- Polynomial Rings.

Characteristic of a ring

Multiplication of elements of rings by integers

Definition.

Let R be a ring.

Let $k \in \mathbb{N}$ (i.e. k is a positive integer) and $r \in R$, then

$$kr = \underbrace{r + r + \cdots + r}_{k \text{ times}}.$$

If k is a negative integer, then

$$kr = \underbrace{-r - r - \cdots - r}_{|k| \text{ times}}.$$

Example: $\mathbb{R}$

Example.

If $R = \mathbb{R}$, we know that

$$kr = \underbrace{r + r + \cdots + r}_{k \text{ times}},$$

$$(-k)r = \underbrace{-r - r - \cdots - r}_{k \text{ times}},$$

for all $k \in \mathbb{N}$ and all $r \in \mathbb{R}$.

Multiplication of elements of rings by integers

- The previous definition might seem a bit redundant at first.
- That is because we are used to $k \cdot r$ meaning r added k times.
- However, ring elements might not be numbers.
- E.g., imagine we have a ring R whose elements are fruits.
- In this case, what does $k \cdot F$ mean for a fruit F?
- We might not know "three times F", but we know that since R is a ring, it has a sum.
- In other words, when defining R, we must also define what $F_1 + F_2$ means for any two fruits F_1, F_2 in R.
- Thus, $3 \cdot F = F + F + F$ is also given by this operation.
- That means that $3 \cdot F$ is F operated with itself three times using the ring additive operation.

Example

Let $R = \mathrm{Mat}(2,\mathbb{R})$ and $k \in \mathbb{N}$.

Question: What is $k \cdot \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$?

By definition,

$$k \cdot \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \underbrace{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) + \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) + \cdots + \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)}_{k \text{ times}} = \left(\begin{smallmatrix} ka & kb \\ kc & kd \end{smallmatrix}\right).$$

Characteristic of a ring

- Knowing the **characteristic** of a ring can simplify calculations within the ring.
- For example, in a ring with characteristic $n > 0$, any element added to itself n times will result in zero.
- The characteristic also helps in classifying and understanding rings.
- For instance, fields of prime characteristic p have different properties compared to fields of characteristic 0, influencing the types of polynomials that can be solved, for instance.
- In the next slides, we will define the characteristic of a ring and provide examples of characteristics from rings we are already familiar with.

Characteristic of a ring

Definition.

Let R be a ring.
Assume there is a **positive** integer k such that

$$kr = 0_R, \quad \textbf{for all r} \in \mathbf{R}.$$

Then the **least** such k is called the **characteristic** of R.

If no such k exists, we say R has **characteristic zero**.

Example: $\mathbb{R}$

If $k \in \mathbb{N} = \{1, 2, 3, \ldots\}$, then

$$k \cdot 1 = k \neq 0.$$

Thus $\mathbb{R}$ is a ring of **characteristic zero**.

Examples

Example: $\mathbb{Z}/2\mathbb{Z}$

If $\overline{a} \in \mathbb{Z}/2\mathbb{Z}$, then

$$2 \cdot \overline{a} = \overline{a} + \overline{a} = \overline{2a} = \overline{0}.$$

Thus, $\mathbb{Z}/2\mathbb{Z}$ is a ring of **characteristic 2**.

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

If $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, then

$$n \cdot \overline{a} = \underbrace{\overline{a} + \overline{a} + \cdots + \overline{a}}_{n \text{ times}} = \overline{na} = \overline{0}.$$

Thus, $\mathbb{Z}/n\mathbb{Z}$ is a ring of **characteristic n**.

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

For each $k \in \mathbb{N}$, we have

$$k \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ka & kb \\ kc & kd \end{pmatrix}.$$

In particular,

$$k \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Thus, $\mathrm{Mat}(2,\mathbb{R})$ is a ring of **characteristic zero**.

Computing the characteristic of a ring

- Calculating the characteristic of a ring using the definition can be tedious, especially for rings with many elements or difficult descriptions.
- Fortunately, there's a simpler method for rings with a **unity** element.
- Instead of verifying that $r \in R$ for all $r \in R$, and finding the smallest such k, we can focus on the unity element.
- That is, the next result shows that it is sufficient to check the case $r = 1_R$.

Lemma [Characteristic of a ring with unity]

Let R be a ring with unity e.
Then the characteristic of R is the **least** $k \in \mathbb{N}$ such that

$$k \cdot e = 0_R.$$

Proof.

Let R be a ring with unity e, and let $k \in \mathbb{N}$ be the least number in $\mathbb{N}$ such that

$$k \cdot e = 0_R.$$

Let us show that the characteristic of R is k.

Characteristic of a ring with unity e–Part 2

Proof.

Goal. For all $r \in R$, we must show

$$k \cdot r = 0_R,$$

and also k is the least number in $\mathbb{N}$ with this property.
In fact,

$$k \cdot r = k \cdot (e \cdot r) = (k \cdot e) \cdot r = 0_R \cdot r = 0_R. \checkmark$$

Proof.

Let us show k is the least such number.

Suppose $\ell \in \mathbb{N}$ is such that $\ell < k$ but

$$\ell \cdot r = 0_R, \text{ for all } r \in R.$$

In particular

$$\ell \cdot e = 0_R,$$

contradicting the minimality of k.

Thus, k is the least such positive number. ✓ □

Computing the characteristic of a ring with unity

- By the previous lemma, to compute the characteristic of a ring R with unity, we need to identify:
  - The unity element 1_R,
  - The zero element 0_R.
- Next, find the smallest **positive** integer k such that

$$\underbrace{1_R + 1_R + \cdots + 1_R}_{k \text{ times}} = 0_R.$$

- If such a k exists, then $\mathrm{Char}(R) = k$.
- If no such k exists, then $\mathrm{Char}(R) = 0$.

Characteristic of $\mathbb{C}$

Example

Let us find the characteristic of the field of complex numbers $\mathbb{C}$. Since $\mathbb{C}$ has unity, we can use the previous lemma.

- **Zero:** The zero of $\mathbb{C}$ is $0_{\mathbb{C}} = 0$.
- **Unity:** The unity of $\mathbb{C}$ is $1_{\mathbb{C}} = 1$.

Thus, it suffices to find the smallest **positive** $k \in \mathbb{Z}$ such that $k \cdot 1 = 0$.

Clearly, $k \cdot 1 = k > 0$ if k is positive.

Thus, $\mathrm{Char}(\mathbb{C}) = 0$.

Example

We can use the lemma to quickly show that $\text{Char}(\mathbb{Z}/n\mathbb{Z}) = n$.

- **Zero:** The zero of $\mathbb{Z}/n\mathbb{Z}$ is $0_{\mathbb{Z}/n\mathbb{Z}} = \overline{0}$.
- **Unity:** The unity of $\mathbb{Z}/n\mathbb{Z}$ is $1_{\mathbb{Z}/n\mathbb{Z}} = \overline{1}$.

We must find the smallest **positive** $k \in \mathbb{Z}$ such that $k \cdot \overline{1} = \overline{0}$.

Since $n \cdot \overline{1} = \overline{n} = \overline{0}$, we see that $\text{Char}(\mathbb{Z}/n\mathbb{Z}) \geq n$.

However, if $0 \leq k < n$, then $k \cdot \overline{1} = \overline{k} \neq \overline{0}$.

Thus, $\text{Char}(\mathbb{Z}/n\mathbb{Z}) = n$.

Characteristic of $\mathbb{Z}_2 \times \mathbb{Z}_7$

Example

Let us find $\mathrm{Char}(\mathbb{Z}_2 \times \mathbb{Z}_7)$.

- **Zero:** The zero of $\mathbb{Z}_2 \times \mathbb{Z}_7$ is $0_{\mathbb{Z}_2 \times \mathbb{Z}_7} = ([0]_2, [0_7])$[1].
- **Unity:** The unity of $\mathbb{Z}_2 \times \mathbb{Z}_7$ is $1_{\mathbb{Z}_2 \times \mathbb{Z}_7} = ([1]_2, [1]_7)$.

Now, we must find the smallest **positive** $k \in \mathbb{Z}$ such that

$$k \cdot ([1]_2, [1]_7) = ([0]_2, [0]_7).$$

[1] Here, $[a]_2$ means $a \mod 2$ and $[b]_7$ means $b \mod 7$.

Example

We must find the smallest **positive** $k \in \mathbb{Z}$ such that

$$k \cdot ([1]_2, [1]_7) = ([0]_2, [0]_7).$$

We have

$$\begin{aligned} 2 \cdot ([1]_2, [1]_7) &= ([2]_2, [2]_7) = ([0]_2, [2]_7) \\ 3 \cdot ([1]_2, [1]_7) &= ([3]_2, [3]_7) = ([1]_2, [3]_7) \\ 4 \cdot ([1]_2, [1]_7) &= ([4]_2, [4]_7) = ([0]_2, [4]_7) \\ &\vdots \end{aligned}$$

We see that $k \cdot ([1]_2, [1]_7) = ([0]_2, [0]_7)$ precisely when k is a multiple of 2 and 7.

We need the **smallest** such k, so it is the least common multiple: $k = 14$. Thus, $\mathrm{Char}(\mathbb{Z}_2 \times \mathbb{Z}_7) = 14$.

Characteristic of an integral domain

- Let us explore the possible characteristics of an integral domain.
- For example, we will discover why there is no integral domain with characteristic 4, but there is one with characteristic 3.
- First, let us recall the definition of an integral domain.

Reminder: Integral domains

$a * b = b * a$

Multiplicative unity 1_R

A **commutative** ring R with **unity element** is called an **integral domain** if it has no **zero divisors**.

$a \neq 0$ for which there is $b \neq 0$ such that $a * b = 0$

Proposition.

The characteristic of an integral domain D is either zero or a prime.

Proof.

Let D be an integral domain. Then, in particular, D has unity 1_D.

If D has characteristic zero, we are done.

Assume D has characteristic $k \in \mathbb{N}$. We must show that k is prime.

Recall that the characteristic k of D is the least positive integer satisfying

$$k \cdot d = 0_D, \text{ for all } d \in D.$$

Since $1 \cdot 1_D = 1_D \neq 0_D$, we have $k > 1$.

Characteristic of integral domains–Part 2

Proof.

Assume by contradiction that k is not prime.

Then $k = ab$ for some $a, b \in \mathbb{N}$ with $1 < a < k$ and $1 < b < k$.

Because $k \cdot 1_D = 0_D$, we have

$$(a \cdot 1_D) \cdot (b \cdot 1_D) = (ab) \cdot 1_D = k \cdot 1_D = 0_D.$$

As D is an integral domain, it has no zero divisors. Thus, either

$$a \cdot 1_D = 0_D \quad \text{or} \quad b \cdot 1_D = 0_D.$$

Lemma [Char. of rings with 1]: If $a1_D = 0_D$, then the characteristic of R is at most $a < k$, a contradiction.

Similarly, $b1_D = 0_D$ yields a contradiction. □

Polynomial Rings

Polynomial rings

- In the next lecture, we will explore how to construct fields of a fixed cardinality.
- To achieve this, we will use **polynomial rings**.
- Let us prepare by revisiting the definition of polynomial rings and the degree of a polynomial, and by exploring some examples.
- Finally, we will prove that if R is commutative with unity, then so is $R[x]$.

Definition

Let R be a commutative ring with unity 1_R.

The set

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

with operations

$$f(x) + g(x) = (f + g)(x)$$
$$f(x)g(x) = (fg)(x)$$

is a ring called a **polynomial ring**.

Examples: $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ and $\mathbb{C}[x]$

- $\mathbb{Z}[x]$: polynomials with integer coefficients,
- $\mathbb{Q}[x]$: polynomials with rational coefficients,
- $\mathbb{R}[x]$: polynomials with real coefficients,
- $\mathbb{C}[x]$: polynomials with complex coefficients.

Example

The polynomial ring $\frac{\mathbb{Z}}{n\mathbb{Z}}[x]$

$\frac{\mathbb{Z}}{n\mathbb{Z}}[x]$ is the ring of polynomials over $\mathbb{Z}/n\mathbb{Z}$.

Examples of elements of $\frac{\mathbb{Z}}{n\mathbb{Z}}[x]$:

$$f(x) = (\overline{n-1}) \cdot x^2 + \overline{2}$$
$$g(x) = x^2 = \overline{1} \cdot x^2.$$

Computations are as usual (but coefficients are taken mod n):

$$\begin{aligned} f(x) + g(x) &= ((\overline{n-1}) \cdot x^2 + \overline{2}) + (x^2) \\ &= (\overline{n-1} + \overline{1}) \cdot x^2 + \overline{2} \\ &= \overline{n} \cdot x^2 + \overline{2} \\ &= \overline{0} \cdot x^2 + \overline{2} \\ &= \overline{2}. \end{aligned}$$

Reminder: degree of a polynomial

Degree of a polynomial

Let $f(x) \in R[x]$. Then

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

with $a_i \in R$, $a_n \neq 0$, and $n \in \{0, 1, 2, \ldots\}$.

The **degree** of f is n. I.e., the highest power of x in $f(x)$.

Notation: $\deg(f) = n$.

Examples in $\mathbb{R}[x]$

1. $\deg(x^2) = 2$,
2. $\deg(2x^3 - 3x + 1) = 3$,
3. $\deg(1) = 0$,
4. $\deg(1 + 2x + 5x^2 - x^3 + x^5 - 2x^8) = 8$.

Examples in $\frac{\mathbb{Z}}{2\mathbb{Z}}[x]$

1. $\deg(x^2) = 2$,
2. $\deg(\overline{2}x^3 - \overline{3}x + \overline{1}) = 1$ because

$$\overline{2}x^3 - \overline{3}x + \overline{1} = \overline{0}x^3 - \overline{1}x + \overline{1} = x + \overline{1}.$$

Theorem.

If R is a commutative ring with unity, then so is $R[x]$.

Moreover, R can be regarded a subring of $R[x]$.

Proof.

To show that $R[x]$ is commutative, we must show that

$$f(x)g(x) = g(x)f(x),$$

for all $f(x), g(x) \in R[x]$.

Proof.

Write

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n,$$
$$g(x) = b_0 + b_1 x + \cdots + b_m x^m.$$

Then

$$\begin{aligned} f(x)g(x) &= (a_0 + a_1 x + \cdots + a_n x^n) \cdot (b_0 + b_1 x + \cdots + b_m x^m) \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0) \cdot x + \cdots + (a_n b_m) \cdot x^{n+m}. \end{aligned}$$

R is commutative: $ab = ba$ for all $a, b \in R$. Thus

$$\begin{aligned} f(x)g(x) &= b_0 a_0 + (b_1 a_0 + b_0 a_1) \cdot x + \cdots + (b_m a_n) \cdot x^{m+n} \\ &= (b_0 + b_1 x + \cdots + b_m x^m) \cdot (a_0 + a_1 x + \cdots + a_n x^n) \\ &= g(x) f(x). \end{aligned}$$

Proof that $R[x]$ has unity.

If R has unity 1_R, then the constant polynomial

$$\mathbf{1}(x) = 1_R$$

is the unity of $R[x]$:

$$\begin{aligned}\mathbf{1}(x) \cdot f(x) &= 1_R \cdot (a_0 + a_1 x + \cdots + a_n x^n) \\ &= (1_R \cdot a_0) + (1_R \cdot a_1)x + \cdots + (1_R \cdot a_n)x^n \\ &= a_0 + a_1 x + \cdots + a_n x^n \\ &= f(x).\end{aligned}$$

Similarly,

$$f(x) \cdot \mathbf{1}(x) = f(x).$$

Proof of theorem–Part 4

R is a subring of $R[x]$

If $r \in R$, we can define the constant polynomial

$$\mathbf{r}(x) = r.$$

We can then regard the elements of R as elements of $R[x]$.

With this identification, we can consider R as a subring of $R[x]$.

$\square$

Next lecture

Next time...

- Polynomial rings over fields.