Slides week 20

Algebraic Structures

Paula Lins

Lecture Slides

2024/25

Week 20: Goals

Last time:

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

Today:

- New algebraic structures: Fields!
- Subfields
- Quick Subfield Theorem
- Homomorphism of rings, ID and fields

Fields

Summary: Groups, rings, integral domains and fields

Group G with operation $*$

Operation $*$					
	Closed	**Associative**	**Identity**	**Inverse**	**Commutative**
Group	✓	✓	✓	✓	×
Abelian Group	✓	✓	✓	✓	✓

Reminder: Groups, rings and integral domains

Ring R and integral domain D with operations $+$ and $*$

Operation $+$					
	Closed	**Associative**	**Zero**	**Commutative**	**Inverse**
Ring	✓	✓	✓	✓	✓
ID	✓	✓	✓	✓	✓

Operation $*$					
	Closed	**Associative**	**Unity**	**Commutative**	**Inverse**
Ring	✓	✓	×	×	×
ID	✓	✓	✓	✓	×

(We also need that they are distributive, but this will be omitted.)

FIELDS CHECK ALL BOXES!

Fields tick all boxes!

Operation +					
	Closed	**Associative**	**Zero**	**Commutative**	**Inverse**
Ring	✓	✓	✓	✓	✓
ID	✓	✓	✓	✓	✓
Field	✓	✓	✓	✓	✓

Operation $*$					
	Closed	**Associative**	**Unity**	**Commutative**	**Inverse**
Ring	✓	✓	×	×	×
ID	✓	✓	✓	✓	×
Field	✓	✓	✓	✓	✓

(We also need that they are distributive, but this will be omitted.)

Examples of Fields

- $\mathbb{C}$, $\mathbb{R}$ and $\mathbb{Q}$ are fields,
- $\mathbb{Z}$ is an integral domain but not a field.
  - $\mathbb{Z}$ does not have multiplicative inverses.
- $2\mathbb{Z}$ is a ring, but not an integral domain or a field.
  - $2\mathbb{Z}$ does not have unity.

Formal definition

Definition

A **field** is a commutative ring in which the set of non-zero elements form a group with respect to multiplication.

In other words...

In other words, a set F with two operations $+$ and $*$ is called a **field** if:

- $(F, +)$ is an abelian group,
- $(F^*, \cdot)$ is an abelian group, (recall that $F^\times = F \setminus \{0_F\}$)
- for all $x, y, z \in F$,

$$x * (y + z) = x * y + x * z, \quad \text{and}$$
$$(x + y) * z = x * z + y * z.$$

Inclusions

Recall that Rings, ID and Fields satisfy all Abelian Group Axioms. They differ with respect to the following axioms:

Operation $*$					
	Closed	**Associative**	**Unity**	**Commutative**	**Inverse**
Ring	✓	✓	×	×	×
ID	✓	✓	✓	✓	×
Field	✓	✓	✓	✓	✓

Inclusions

The table above then shows that

$$\text{Fields} \subset \text{Integral Domains} \subset \text{Rings}.$$

Fields are Integral Domains

Technically, to show that fields are integral domains, we still need to show that fields do not have zero divisors.

Proof

Let F be a field. We need to show that if $x, y \in F$ are such that $xy = 0$, then either $x = 0$ or $y = 0$.

Without loss of generality, assume $x \neq 0$. Then $x^{-1} \in F$ because F is a field.

Consequently, by multiplying both sides of $xy = 0$ by x^{-1}, we obtain

$$0 = x^{-1}(xy) = (x^{-1}x)y = y.$$

□

Subfields

Subfields

Definition.

A subset K of a field F is a **subfield** of F if K is itself a field with respect to the operations on F.

Example

- $\mathbb{Q}$ and $\mathbb{Z}$ are subsets of $\mathbb{R}$.
- However, $\mathbb{Q}$ is a field and $\mathbb{Z}$ is not.
- Thus, $\mathbb{Q}$ is a subfield of $\mathbb{R}$ but $\mathbb{Z}$ is not.

As for groups and rings, we have a quicker way of checking whether a subset is a subfield.

Quick Subfield Theorem

Let F be a field and K a subset of F. Then K is a subfield of F if and only if

1. K contains the zero and the unity of F,
2. if $a, b \in K$ then $a + b$ and ab belong to K,
3. if $a \in K$ then $-a \in K$,
4. if $a \in K$ and $a \neq 0$ then $a^{-1} \in K$.

Proof. It follows from similar arguments as for the Quick Sub**ring** theorem. You can find the proof in the Deep Dive Slides.

Example: Gaussian Integers

Let is use the QSF Theorem to show that

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

is **not** a subfield of $\mathbb{C}$. It suffices to show that **one** condition fails.

4. Multiplicative inverse: Given $a + ib \underline{\in \mathbb{C}}$, we have

$$(a + ib)^{-1} = \frac{1}{a^2 - b^2}(a - ib). \qquad \text{(Exercise!)}$$

For instance, $(1 + i) \in \mathbb{Z}[i]$ has inverse

$$(1 + i)^{-1} = \frac{1}{2}(1 - i) = \frac{1}{2} - \frac{i}{2} \notin \mathbb{Z}[i].$$

Thus, $\mathbb{Z}[i]$ **it is not a subfield** of $\mathbb{C}$.

Application of QST - $\mathbb{Q}[i]$

Example: $\mathbb{Q}[i]$

What about

$$\mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}?$$

Is this a subfield of $\mathbb{C}$? We have that if $a + ib \in \mathbb{Q}[i]$, then its inverse is

$$(a + ib)^{-1} = \frac{1}{a^2 - b^2}(a - ib) = \frac{a}{a^2 - b^2} - i\frac{b}{a^2 - b^2} \in \mathbb{Q}[i]$$

because $\frac{a}{a^2-b^2}$ and $-\frac{b}{a^2-b^2}$ are rational numbers.

Thus, $\mathbb{Q}[i]$ satisfy the property of the QST that $\mathbb{Z}[i]$ does not.

Let us check the other three.

Example: $\mathbb{Q}[i]$

1. $\mathbb{Q}[i]$ contains the zero and the unity of $\mathbb{C}$:

The zero of $\mathbb{C}$ is 0. Let us show that this is an element of $\mathbb{Q}[i]$:

$$0 = 0 + 0i \in \mathbb{Q}[i]. \qquad (0 \in \mathbb{Q})$$

The unity of $\mathbb{C}$ is 1. Let us show that this is an element of $\mathbb{Q}[i]$:

$$1 = 1 + 0i \in \mathbb{Q}[i]. \qquad (0, 1 \in \mathbb{Q})$$

Example: $\mathbb{Q}[i]$

2. if $a, b \in \mathbb{Q}[i]$ then $a + b$ and ab belong to $\mathbb{Q}[i]$:

Given $a + bi$ and $c + di$ in $\mathbb{Q}[i]$, we have

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

because $a + c$, $b + d$, $ac - bd$, and $ad + bc$ are rationals.

3. If $x \in \mathbb{Q}[i]$ then $-x \in \mathbb{Q}[i]$:
Given $a + bi \in \mathbb{Q}[i]$, we have

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

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

Finite integral domains are fields!

Theorem

Every finite integral domain is a field.

Proof.

Let D be an integral domain.

A field is an integral domain having inverses for all non-zero elements.

Thus, we must show that every non-zero $a \in D$ has an inverse.

Goal: Find $b \in D$ such that

$$a * b = e.$$

Proof of Theorem - Part 2

Proof.

Strategy: Define the map

$$\lambda : D \to D \text{ given by } \lambda(x) = a * x.$$

- If we show that there exists $b \in D$ such that $\lambda(b) = e$, then we are done.
  - In fact, $\lambda(b) = e$ means $a * b = e$.
  - That is equivalent to b being the inverse of a, as required.
- By definition, if λ is surjective, then there exists $b \in D$ such that $\lambda(b) = e$.
- It then suffices to show that λ is surjective.

Fact.

If F is a **finite** set, then every mapping $F \to F$ is surjective if and only if it is injective.

Proof of Theorem - Part 3

- Thus, it suffices to show that λ is **injective**.

Assume $\lambda(x) = \lambda(y)$. We must show $x = y$.

In fact, $\lambda(x) = \lambda(y)$ is equivalent to $a * x = a * y$.

Since **multiplicative cancellation** holds for integral domains, we have $x = y$ as desired. □

$m * n = m * p \Longrightarrow n = p$

Corollary

$\frac{\mathbb{Z}}{n\mathbb{Z}}$ is a field if and only if n is prime.

Proof.

We know that $\frac{\mathbb{Z}}{n\mathbb{Z}}$ is an integral domain if n is prime, and it is not an integral domain otherwise.

Since $\frac{\mathbb{Z}}{n\mathbb{Z}}$ is finite, by the previous theorem, if n is prime, then $\frac{\mathbb{Z}}{n\mathbb{Z}}$ is a field. $\square$

Homomorphism of rings, ID and fields

Ring homomorphism

Definition

Let R and S be rings. A **ring homomorphism** from R to S is a mapping

$$\theta : R \to S$$

that satisfies:

- $\theta(a+b) = \theta(a) + \theta(b)$, and
- $\theta(ab) = \theta(a)\theta(b)$,

for all $a, b \in R$.

Ring, Integral Domain and field homomorphisms

Remark

Recall that

$$\text{Fields} \subset \text{Integral Domains} \subset \text{Rings}.$$

Thus

- an **integral domain homomorphism** is just a **ring homomorphisms** between two integral domains.
- Similarly, a **field homomorphism** is just a **ring homomorphisms** between two fields.

Which of the following maps are ring homomorphisms?

1. $f : \mathbb{R} \to \mathbb{R}$ given by

$$f(x) = 4x, \text{ for all } x \in \mathbb{R},$$

2. $g : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ given by

$$g(x) = \overline{4}x, \text{ for all } x \in \mathbb{Z}/6\mathbb{Z}.$$

Solutions

1. $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 4x,$ for all $x \in \mathbb{R}$.

$$\begin{aligned} f(x+y) &= 4(x+y) = 4x + 4y = f(x) + f(y). \quad \checkmark \\ f(xy) &= 4(xy) = 4xy, \\ f(x)f(y) &= 4x4y = 16xy. \quad \chi \end{aligned}$$

Thus, this is **not a ring homomorphism!**

2. $g : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ given by $g(x) = \overline{4}x,$ for all $x \in \mathbb{Z}/6\mathbb{Z}$.

$$\begin{aligned} g(x+y) &= \overline{4}(x+y) = \overline{4}x + \overline{4}y = g(x) + g(y). \checkmark \\ g(xy) &= \overline{4}(xy) = \overline{4}xy, \\ g(x)g(y) &= \overline{4}x\overline{4}y = \overline{16}xy = \overline{4}xy. \quad \checkmark \end{aligned}$$

Thus, this is a **ring homomorphism!**

Example of ring homomorphisms

Example.

The map $\theta : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by

$$\theta(a) = \overline{a} \quad (\text{i.e. } a \mod n)$$

is a ring homomorphism.

In fact:

- $\theta(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \theta(a) + \theta(b)$. ✓
- $\theta(ab) = \overline{ab} = \overline{a} \cdot \overline{b} = \theta(a)\theta(b)$, ✓

for all $a, b \in \mathbb{Z}$.

Remark.

In the previous example, we showed that the map $\theta : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by

$$\theta(a) = \overline{a} \quad (\text{i.e. } a \mod n)$$

is a ring homomorphism.

Now,

- $\mathbb{Z}$ is an integral domain.
- If n is prime, $\mathbb{Z}/n\mathbb{Z}$ is an integral domain.
- We can conclude: If n is prime, then this map $\theta : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is an **integral domain homomorphism**.

Example of ring homomorphism: $\mathbb{R} \to M(2,\mathbb{R})$

Recall $M(2,\mathbb{R})$

Recall that

$$M(2,\mathbb{R}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \middle| a, b, c, d \in \mathbb{R} \right\}$$

is a ring with usual addition and multiplication of matrices.

Example of ring homomorphism $\mathbb{R} \to M(2,\mathbb{R})$

The map $\phi : \mathbb{R} \to M(2,\mathbb{R})$ given by

$$\phi(x) = \left(\begin{smallmatrix} 0 & 0 \\ x & x \end{smallmatrix} \right)$$

is a ring homomorphism.

Example of ring homomorphism: $\mathbb{R} \to M(2, \mathbb{R})$ - Part 2

Sum

$$\begin{aligned}\phi(x) + \phi(y) &= \begin{pmatrix} 0 & 0 \\ x & x \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ y & y \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ x+y & x+y \end{pmatrix} \\ &= \phi(x+y). \quad \checkmark\end{aligned}$$

Mutiplication

$$\begin{aligned}\phi(x)\phi(y) &= \begin{pmatrix} 0 & 0 \\ x & x \end{pmatrix}\begin{pmatrix} 0 & 0 \\ y & y \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ xy & xy \end{pmatrix} \\ &= \phi(xy). \quad \checkmark\end{aligned}$$

More Examples

Are the following maps ring homomorphisms?

1. $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x + 2$. Let us check:

$$f(x + y) = (x + y) + 2 = x + y + 2, \text{ whereas}$$
$$f(x) + f(y) = (x + 2) + (y + 2) = x + y + 4.$$

Not a ring homomorphism.

2. $\mathbf{0} : \mathbb{R} \to \mathbb{R}$ given by $\mathbf{0}(x) = 0$, for all $x \in \mathbb{R}$. Let us check:

$$\mathbf{0}(x + y) = 0 = 0 + 0 = \mathbf{0}(x) + \mathbf{0}(y), \checkmark$$
$$\mathbf{0}(xy) = 0 = 0 \cdot 0 = \mathbf{0}(x)\mathbf{0}(y)\checkmark.$$

This is a ring homomorphism. (Also an **integral domain homomorphism** and a **field homomorphism**.)

Let us practice!

Which of the following maps are ring homomorphisms?

1. $f : \mathbb{R} \to \mathbb{R}$ given by

$$f(x) = x^2, \text{ for all } x \in \mathbb{R},$$

2. $\mathbf{1} : \mathbb{R} \to \mathbb{R}$ given by

$$\mathbf{1}(x) = 1, \text{ for all } x \in \mathbb{R}.$$

3. $g : M(2, \mathbb{R}) \to M(2, \mathbb{R})$ given by

$$g\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right) = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right).$$

Solution

1. $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$, for all $x \in \mathbb{R}$.

f can only be a ring homomorphism if

$$f(x+y) = f(x) + f(y)$$
$$f(xy) = f(x)f(y).$$

We have

$$f(x+y) = (x+y)^2 = x^2 + 2xy + y^2,$$

$$f(x) + f(y) = x^2 + y^2 \neq (x+y)^2.$$

Thus, f is **not** a ring homomorphism.

Solution

2. The map $\mathbf{1} : \mathbb{R} \to \mathbb{R}$ can only be a ring homomorphism if

$$\mathbf{1}(a+b) = \mathbf{1}(a) + \mathbf{1}(b)$$
$$\mathbf{1}(ab) = \mathbf{1}(a)\mathbf{1}(b).$$

We have

$$\mathbf{1}(a+b) = 1 \quad \text{and} \quad \mathbf{1}(a) + \mathbf{1}(b) = 1 + 1 \neq 1.$$

Thus, $\mathbf{1}$ is **not** a ring homomorphism.

Solution of 3

Solution

3. $g : M(2, \mathbb{R}) \to M(2, \mathbb{R})$ given by $g\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right) = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$.

$$\begin{aligned} g\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) + \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)\right) &= g\begin{pmatrix} a+x & b+y \\ c+z & d+w \end{pmatrix} = \begin{pmatrix} a+x & 0 \\ 0 & a+x \end{pmatrix} \\ &= \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) + \left(\begin{smallmatrix} x & 0 \\ 0 & x \end{smallmatrix}\right) = g\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) + g\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right). \checkmark \end{aligned}$$

$$g\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)\right) = g\begin{pmatrix} ax+bz & ay+wz \\ cx+dz & cy+dw \end{pmatrix} = \begin{pmatrix} ax+bz & 0 \\ 0 & ax+bz \end{pmatrix},$$

$$g\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right) \cdot g\left(\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)\right) = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} x & 0 \\ 0 & x \end{smallmatrix}\right) = \begin{pmatrix} ax & 0 \\ 0 & ax \end{pmatrix} . \chi$$

Not a ring homomorphism.

Properties of ring homomorphisms

If $\theta : R \to S$ is a ring homomorphism, then

- $\theta(0_R) = 0_S$,
- $\theta(-a) = -\theta(a)$ for all $a \in R$.

Proof.

1. Notice that

$$\theta(0_R) = \theta(0_R + 0_R) = \theta(0_R) + \theta(0_R).$$

Subtracting $\theta(0_R)$ from both sides gives

$$\theta(0_R) = 0_S.$$

2. Exercise!

Exercises before next lecture

Solve the following exercises before next lecture:

- Practical 7: Question 7.1.

You can also attempt the following, for extra practice:

- Practice question: Question 7.5.

Next time...

- Isomorphism of rings, ID and fields
- Isomorphic rings.