Lecture 04

Melissa Zhang

MAT 150A

Participation Slip

1. Take a slip from the front of the room.
2. Write your full name on the top left corner.
3. You will write down your answer to some clearly marked "Participation Slip" questions during lecture.
4. Hand in your slip at the end of class.

Reminder

- Participation slips won't be graded until Lecture 9.
- From Lecture 9 and onward, your participation slip will be graded for completion.
- A score of 15 (out of 20 lecture days) will receive full credit.

Notation Conventions

So far in this class we've used a couple different notations for the **composition law / group operation** in a group G:

1. An abstract symbol, such as $\circ$.
   - Permutations $p, q \in S_n$ are set maps $[n] \to [n]$. We can compose them in two ways: $p \circ q$ or $q \circ p$.
   - When $n \geq 3$, S_n is **nonabelian**, so in general $p \circ q \neq q \circ p$.
2. **Additive notation**, where $+$ is a **commutative** group operation:
   - e.g. $(\mathbb{Z}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$, $(n\mathbb{Z}, +)$
   - Use 0 to represent the **additive identity**.
3. **Multiplicative notation**, where $b \circ a = b \cdot a$ is written ba:
   - If $x, y \in \mathbb{R}^\times = (\mathbb{R} - \{0\}, \cdot)$, we write xy as their product.
   - If $p, q \in S_n$, we write pq or qp. In general, $pq \neq qp$.
   - Use 1 to represent the **multiplicative identity**.

Notation Conventions

Notation conventions summary

1. Abstract symbol: $x \circ y$, $x \circ x^{-1} = x^{-1} \circ x = e$
2. Additive notation when G is **abelian**: $x + y = y + x$, $x + (-x) = 0$
3. Multiplicative notation: xy, $xx^{-1} = x^{-1}x = 1$

The Integers $\mathbb{Z}$, the Prototypical **Ring**

Observe the following facts about the integers $\mathbb{Z}$:

1. $(\mathbb{Z}, +)$ is an abelian group.
2. There is a multiplication operation $\cdot$ and $1 \in \mathbb{Z}$ is the multiplicative identity.

Definition of a ring $(A, +, \cdot)$

A **ring** is a set A equipped with two *associative* binary operations, $+$ and $\cdot$, such that

- $(A, +)$ is an abelian group, with additive identity 0
- There is an element $1 \in A$ that is a multiplicative identity.

Note that

- $\cdot$ is **not** required to be commutative.
- Inverses under $\cdot$ are **not** required.

Examples of Rings

Definition of a ring $(A, +, \cdot)$

A **ring** is a set A equipped with two *associative* binary operations, $+$ and $\cdot$, such that

- $(A, +)$ is an abelian group, with additive identity 0
- There is an element $1 \in A$ that is a multiplicative identity.

Examples of rings

- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}/12\mathbb{Z}, +, \cdot)$
- $\mathbb{R}[x]$, polynomials in a variable x with coefficients in $\mathbb{R}$

Participation Slip

1. What is $5 \cdot 4$ in $\mathbb{Z}/12\mathbb{Z}$?
2. Find an element of $\mathbb{Z}/12\mathbb{Z} - \{0\}$ that is **not** invertible under $\cdot$.

Start with the ring $\mathbb{Z} = (\mathbb{Z}, +, \cdot)$.

- Only 1 and -1 are invertible in $\mathbb{Z}$. We say ± 1 are **units** in the ring $\mathbb{Z}$, because they are **invertible** (i.e. have an inverse) under $\cdot$.
- Note that $\cdot$ is commutative.

Participation Slip

What are the units (invertible elements under multiplication) in $\mathbb{Z}/12\mathbb{Z}$?

Start with the ring $\mathbb{Z} = (\mathbb{Z}, +, \cdot)$.

- Only 1 is invertible in $\mathbb{Z}$. We say 1 is a **unit** in the ring $\mathbb{Z}$, because it is invertible under $\cdot$.
- Note that $\cdot$ is commutative.

Now expand the set of elements by declaring that inverses exist, for all elements of $\mathbb{Z} - \{0\}$:

- For $b \neq 0$, b^{-1} now exists, and $bb^{-1} = b^{-1}b = 1$, the multiplicative identity in the ring $\mathbb{Z}$
- For $a, b \in \mathbb{Z}$, $b \neq 0$, we can write $\frac{a}{b} := ab^{-1} = b^{-1}a$ (a *fraction*).

Call this new larger set $\mathrm{Frac}(\mathbb{Z})$, the **fraction field** of $\mathbb{Z}$.
What is $\mathrm{Frac}(\mathbb{Z})$ better known as?

The Rational Numbers $\mathbb{Q}$, the Prototypical **Field**

The rational numbers are defined by $\mathbb{Q} := \mathrm{Frac}(\mathbb{Z})$.

Definition

A **field** is a ring $(\mathbb{F}, +, \cdot)$ where

- addition $(+)$ and multiplication $(\cdot)$ are **both associative and commutative**,
- and all nonzero elements $\mathbb{F}^\times := \mathbb{F} - \{0\}$ are all units.

We refer to $\mathbb{F}^\times$ as the *units* of $\mathbb{F}$.

- Less precisely, a field is a set where addition, subtraction, multiplication, and division are all well-defined.
- Alternatively, $(\mathbb{F}, +, \cdot)$ is a field if $(\mathbb{F}, +)$ and $(\mathbb{F}^\times, \cdot)$ are both *abelian* groups.

Examples of Fields

Definition

A **field** is a ring $(\mathbb{F}, +, \cdot)$ where

- addition $(+)$ and multiplication $(\cdot)$ are associative and commutative,
- and all nonzero elements $\mathbb{F}^{\times} := \mathbb{F} - \{0\}$ are all units.

Examples of Fields

1. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$
2. $(\mathbb{Z}/2\mathbb{Z}, +, \cdot)$
3. More generally, $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$, where p is prime

The Complex Numbers $\mathbb{C}$

Define a new symbol i, and let $i^2 = -1$. (Informally, "$i = \sqrt{-1}$.")

The Complex Numbers $\mathbb{C}$

The *complex numbers*, denoted $\mathbb{C}$, is the field

$$\mathbb{R} + \mathbb{R}i = \{a + bi \mid a, b \in \mathbb{R}\},$$

where $i^2 = -1$. Later: $\mathbb{C} = \mathbb{R}[i]/(i^2 + 1 = 0)$, or just $\mathbb{R}[i]$.

Q: How are $+$, $-$, $\times$, and $\div$ defined in $\mathbb{C}$?

- $(a + bi) \pm (c + di) = (a \pm c) + (b \pm d)i$
- $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$
- $\dfrac{1}{a + bi} = \dfrac{1}{a^2 + b^2}(a - bi)$