Lecture 05

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.

Recall: Rings and Fields

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.

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.

(Write summary on board.)

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 $\mathbb{C}$?

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

The Complex Numbers $\mathbb{C}$

$\mathbb{C} = \mathbb{R} + \mathbb{R}i = \{a + bi \mid a, b \in \mathbb{R}\} = \mathbb{R}[i]/(i^2 + 1)$

- $\pm, \cdot$ are defined analogously to polynomial operations
- $\dfrac{1}{a+bi} = \dfrac{1}{a^2+b^2}(a - bi)$

Definition

Let $z = a + bi \in \mathbb{C}$.

- $\bar{z} = a - bi$ is the **complex conjugate** of z.
  - Compare with the conjugate relationship between $1 + \sqrt{2}$ and $1 - \sqrt{2}$.
- $|z| = \sqrt{a^2 + b^2} \in \mathbb{R}$ is the **absolute value** or **modulus** of $z \in \mathbb{C}$.
  - $|z|$ is also the length of the vector z in the complex plane.
  - Check that $z\bar{z} = |z|^2$.

The Circle Group S^1

Circle group

Recall that $\mathbb{C}^\times = (\mathbb{C} - \{0\}, \cdot)$. The **circle group** S^1 is the subgroup of $\mathbb{C}^\times$ given by the unit circle:

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\}.$$

We can view $\mathbb{Z}/4\mathbb{Z}$ as a subgroup of S^1 by representing it as the cyclic subgroup $\langle i \rangle$.

The Hamiltonian Quaternions $\mathbb{H}$

There is an extension of the complex numbers called the *Hamiltonians*, denoted $\mathbb{H}$.
Inside $\mathbb{H}$, there are three distinguished elements, $\mathbf{i}, \mathbf{j}, \mathbf{k}$, that behave similarly to $i \in \mathbb{C}$:

- $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$
- $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \mathbf{jk} = -\mathbf{kj} = i, \mathbf{ki} = -\mathbf{ik} = \mathbf{j}$.

As a set $\mathbb{H} = \mathbb{R} + \mathbf{i}\mathbb{R} + \mathbf{j}\mathbb{R} + \mathbf{k}\mathbb{R}$.

Q: Is $\mathbb{H}$ a field?

A: No, because $\cdot$ is not commutative!
However, we can still define multiplicative inverses for $\mathbb{H}^\times$. This makes $\mathbb{H}$ into a *division ring*, which we will not talk about again.

The Hamiltonian Quaternions $\mathbb{H}$

$\mathbb{H} = \mathbb{R} + \mathbf{i}\mathbb{R} + \mathbf{j}\mathbb{R} + \mathbf{k}\mathbb{R}$.

- $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$
- $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \mathbf{jk} = -\mathbf{kj} = i, \mathbf{ki} = -\mathbf{ik} = \mathbf{j}$.

Quaternion group

The **quaternion group** H is the subgroup of $\mathbb{H}^\times$ generated by $\mathbf{i}$ and $\mathbf{j}$, subject to the relations above.

$$H = \{\pm \mathbf{1}, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}.$$

The Quaternion Group

Quaternion group

The **quaternion group** H is the subgroup of $\mathbb{H}^\times$ generated by $\mathbf{i}$ and $\mathbf{j}$, subject to the relations above.

$$H = \{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}.$$

We can represent H using 2×2 complex matrices:

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$$

$$\mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Vector Spaces

Definition

Let $\mathbb{F}$ be a *field.* A **vector space** V over $\mathbb{F}$ is a set together with two laws of composition:

1. **addition**: $V \times V \to V$, written $(v, w) \mapsto v + w$ for $v, w \in V$
2. **scalar multiplication** by elements of the *ground field*: $\mathbb{F} \times V \to V$, written $(c, v) \mapsto cv$, for $c \in \mathbb{F}$ and $v \in V$.

These laws are required to satisfy the following axioms:

- $(V, +)$ is an abelian group, with identity denoted $\mathbf{0}$.
  - Note that this 0 is technically different from the 0 in $\mathbb{F}$.
- $1v = v$ for all $v \in V$
- *associative law*: $(ab)v = a(bv)$ for all $a, b, \in \mathbb{F}$, $v \in V$
- *distributive laws*: $(a + b)v = av + bv$ and $a(v + w) = av + aw$, for all $a, b \in \mathbb{F}$, $v, w \in V$.

Vector Spaces

A **vector space** V over $\mathbb{F}$ is a set with addition $(v + w)$ and scalar multiplication (cv).

Examples of vector spaces

1. $V = \mathbb{F}$ over $\mathbb{F}$
   - e.g. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$...
2. $V = M_{n \times n}(\mathbb{F})$, the set of $n \times n$ matrices with coefficients in $\mathbb{F}$
   - While V was not a group under *matrix multiplication*, it certainly is a group under addition!
3. The set $\mathbb{F}^n = \underbrace{\mathbb{F} \times \mathbb{F} \times \ldots \times \mathbb{F}}_{n}$ over $\mathbb{F}$
4. $\mathbb{R}[x]$, the set of polynomials in x with coefficients in $\mathbb{R}$
5. The set of continuous functions $\mathbb{R} \to \mathbb{R}$, over $\mathbb{R}$

Definition

- A **subspace** W of a vector space V over a field $\mathbb{F}$ is a *nonempty* subset closed on the operations of addition and scalar multiplication.
- A subspace W is **proper** if it is not $\{0\} \subset V$ nor $V \subset V$.

Participation Slip

Consider the field $\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$.

- Recall that $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ is a field if and only if $p \in \mathbb{N}$ is prime.

1. How many elements are there in $\mathbb{F}_p^2$?
2. How many different *proper* subspaces of $\mathbb{F}_p^2$ are there?