Lecture 03

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. Answer the following question. You are encouraged to discuss your answer with those around you.

Exercise (write solution on participation slip)

Prove the following proposition.
Proposition 2.2.3 (Cancellation Law) Let G be a group, and let $a, b, c \in G$.

1. If $ab = ac$ or if $ba = ca$, then $b = c$.
2. If $ab = a$ or if $ba = a$, then $b = 1$.

More examples and non-examples of groups

Definition

- An **abelian group** is a group whose law of composition is commutative.
- The **order** of a group G is the number of elements that it contains, and is denoted $|G|$.
  - If $|G|$ is finite, then G is a *finite group*.
  - If $|G|$ is infinite, then G is an *infinite group*.

Some familiar infinite abelian groups

Your book's notation is on the left.

- $\mathbb{Z}^+ := (\mathbb{Z}, +)$
- $\mathbb{R}^+ := (\mathbb{R}, +)$
- $\mathbb{R}^\times := (\mathbb{R} - \{0\}, \cdot)$ Why do we need to remove 0?
- $\mathbb{C}^+, \mathbb{C}^\times$, defined analogously

Some properties of groups

Definition

- An **abelian group** is a group whose law of composition is commutative.
- The **order** of a group G is the number of elements that it contains, and is denoted $|G|$.
  - If $|G|$ is finite, then G is a *finite group*.
  - If $|G|$ is infinite, then G is an *infinite group*.

Some familiar infinite abelian groups

Your book's notation is on the left.

- $\mathbb{Z}^+ := (\mathbb{Z}, +)$
- $\mathbb{R}^+ := (\mathbb{R}, +)$
- $\mathbb{R}^\times := (\mathbb{R} - \{0\}, \cdot)$ Why do we need to remove 0?
- $\mathbb{C}^+, \mathbb{C}^\times$, defined analogously

Subgroups

Definition (copy to board)

A subset H of a group G is a **subgroup** (written $H \leq G$) if it has the following properties:

- *Closure*: If $a, b \in H$, then $ab \in H$ as well.
- *Identity*: $e \in H$.
- *Inverses*: If $a \in H$, then $a^{-1} \in H$ as well.

Examples of subgroups

1. $(2\mathbb{Z}, +) \leq (\mathbb{Z}, +)$
   - $2\mathbb{Z}$ denotes the even integers, $\{\ldots, -2, 0, 2, 4, \ldots\}$
2. $G \leq G$ and $\langle e \rangle \leq G$ for any group G
   - $\langle e \rangle$, also sometimes written $\langle 1 \rangle$, is the **trivial group**.
3. $S_m \leq S_n$ for $m, n \in \mathbb{N}$, $m < n$

Subgroups of $(\mathbb{Z}, +)$

Theorem 2.3.3 (write on board)

Let S be a subgroup of $(\mathbb{Z}, +)$. Then S is either

- the trivial subgroup $\{0\}$ or
- of the form $n\mathbb{Z}$, where n is the smallest positive integer in the set S.

The book uses the notation $\mathbb{Z}n$ instead of $n\mathbb{Z}$. We will use the notation $n\mathbb{Z}$ to be consistent with the notation $\mathbb{Z}/n\mathbb{Z}$.

We will now sketch the proof of the Theorem. See the book for the full proof.

Proof of Theorem 2.3.3

- Since 0 is the additive identity, $0 \in S$. If $S \neq \{0\}$, then there exist integers $n, -n \neq 0$ in S. So S contains a positive integer.
- Let a be the smallest positive integer in S. We want to show that $a\mathbb{Z} = S$, so we need to show that $a\mathbb{Z} \leq S$ and $S \leq a\mathbb{Z}$.
- To check that $a\mathbb{Z} \leq S$, observe that (1) closure and induction imply $ka \in S$, (2) $0 = 0a \in S$, and (3) S contains inverses, so $-ka \in S$.
- To show $S \subseteq a\mathbb{Z}$, pick any $n \in S$. Use division with remainder to write $n = qa + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < a$.
  - Since S is a *subgroup*, $r = n - qa \in S$.
  - Since a is the smallest positive integer in S, r must $= 0$.
  - Therefore $n = qa \in a\mathbb{Z}$.

$\square$

Order of an element

Definition

Let G be a group, and let x be a particular element (or *member*).

- The set of all elements of the form x^k, where $k \in \mathbb{Z}$, forms a subgroup of G:

$$\langle x \rangle := \{g \in G \mid g = x^k \text{ for some } k \in \mathbb{Z}\}.$$

- $\langle x \rangle \leq G$ is called the **cyclic subgroup generated by** x.
- We say that x **has order** n in the group G if $|\langle x \rangle| = n$.

Order of an element

Let's practice proving some propositions.

Proposition (write on board)

Let $\langle x \rangle$ be the cyclic subgroup of a group G generated by an element x, and let S denote the set of integers k such that $x^k = 1$.

(a) The set S is a subgroup of $(\mathbb{Z}, +)$.

(b) Two powers $x^r = x^s$, $r \geq s$, if and only if $x^{r-s} = 1$, i.e. if and only if $r - s \in S$.

(c) Suppose S is not the trivial subgroup $\{0\} \leq (\mathbb{Z}, +)$. Then $S = n\mathbb{Z}$ for some positive integer n. The powers $\{1, x, x^2, \ldots, x^{n-1}\}$ are the distinct elements of the subgroup $\langle x \rangle$, and the order of $\langle x \rangle$ is n.

Claim (a) The set S is a subgroup of $(\mathbb{Z}, +)$.

Proof.

We check the three defining properties of subgroups.

1. (Closure) If $x^k = 1$ and $x^l = 1$, then $x^{k+l} = x^k x^l = 1$. In other words, if k and l are both in S, then $k + l \in S$ as well.
2. (Identity) Since $e = x^0$, we have $e \in \langle x \rangle$.
3. (Inverses) Suppose $k \in S$, i.e. $x^k = 1$. Then $x^{-k} = (x^k)^{-1} = 1$ too, so $-k \in S$ as well.

□

Claim (b) Two powers $x^r = x^s$, $r \geq s$, if and only if $x^{r-s} = 1$, i.e. if and only if $r - s \in S$.

Proof.

The "i.e." part is just restating the definition of S, so below we prove the first "if and only if".
First assume $x^r = x^s$. Then

$$x^{r-s} = x^r x^{-s} = x^s x^{-s} = 1,$$

i.e. $r - s \in S$.
Conversely, assume $x^{r-s} = 1$, i.e. $r - s \in S$. In other words, $x^r x^{-s} = 1 = x^s x^{-s}$. The Cancellation Law then implies that $x^r = x^s$. □

Order of an element

Claim (c) Suppose S is not the trivial subgroup $\{0\} \leq (\mathbb{Z}, +)$. Then $S = n\mathbb{Z}$ for some positive integer n. The powers $\{1, x, x^2, \ldots, x^{n-1}\}$ are the distinct elements of the subgroup $\langle x \rangle$, and the order of $\langle x \rangle$ is n.

Proof.

- Suppose $S \neq \{0\}$. By Theorem 2.3.3, $S = n\mathbb{Z}$, where n is the smallest positive integer in S.
  - Therefore $1, x, x^2, \ldots, x^{n-1}$ are all distinct.
- For any power x^k of x, use division with remainder to write $k = nq + r$ (where $q, r \in \mathbb{Z}$, $0 \leq r < n$). Then $x^{nq} = 1^q = 1$, so $x^k = x^{nq}x^r = x^r$.
- Therefore x^k is equal to *exactly one* of the powers $1, x, x^2, \ldots, x^{n-1}$.

□

Matrix Groups

Notation / Definition

1. $M_{n\times n}(\mathbb{R}) = \{n \times n \text{ matrices with entries in } \mathbb{R}\}$
   - This is not a group! Why not?
2. **General linear group:**
   $GL_n(\mathbb{R}) = \{A \in M_{n\times n}(\mathbb{R}) \mid \det(A) \neq 0\}$.
3. **Special linear group:**
   $SL_n(\mathbb{R}) = \{A \in M_{n\times n}(\mathbb{R}) \mid \det(A) = 1\}$.
4. $M_{n\times n}(\mathbb{C}), GL_n(\mathbb{C}), SL_n(\mathbb{C})$ are defined analogously.

By definition, $SL_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$.

Matrix Groups

Definition

A group G is a **matrix group** (over a field $\mathbb{F}$) if it is a subgroup of $GL_n(\mathbb{F})$.

- For us $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$, most of the time. We'll talk about *fields* later.
- Note that all elements of matrix groups are necessarily square matrices. Why?

Example: Klein four group ♫

$$V = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

Exercise

Prove that V is *not* cyclic.