Algebra I

September 28, 2023

Grade Weights

50% Homework + 50% Final
Participation matters for pass/fail.

Office Hours

Tuesday / Thursday 11:25 - 12:00
Or by appointment (jusuh@ucsc.edu)

Recommended Text

Abstract Algebra (3e) - Dummit and Foote
Finite Groups: An Introduction (2nd revised) - Jean-Pierre Serre
Robert Boltje's Lecture Notes - (`https://boltje.math.ucsc.edu/courses/f17/f17m200notes.pdf`)

Binary Operation

Let S be a set. A binary operation on S is a function $f : S \times S \to S$. We will almost never use f for the binary operation $(f(s,t))$.
The usual notation for binary operations is $s * t$.

Example

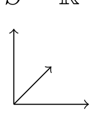
1. $S = \mathbb{R}^3$, define $f : S \times S \to S$ as $(\vec{x}, \vec{y}) \rightsquigarrow \vec{x} + \vec{y}$.

2. $S = \mathbb{R}^3$, define $S \times S \xrightarrow{f} S$ as $(\vec{x}, \vec{y}) \rightsquigarrow \vec{x} + \vec{y}$.

    - Note that $(\vec{x}, \vec{y}) \rightsquigarrow \vec{x} \cdot \vec{y}$ is not a binary operation.

3. $S = \mathbb{Z}$ as $(m, n) \mapsto m \cdot n$.

4. $S = \mathbb{R}^3$ as $(\vec{x}, \vec{y}) \rightsquigarrow \frac{\vec{x}+\vec{y}}{2}$

5. Let $n \geq 1$ be an interger and $S = M_{n \times n}(\mathbb{R}) = \{n \times n \text{ real matricies}\}$. Then $(A, B) \rightsquigarrow AB$.

Observations

Examples 1,3,5 are associative; examples 2,4 are not.
Examples 1-4 are commutative; example 5 commutes only when $n = 1$.
$\vec{0}$ for example 1, 1 for example 3, and I_n for example 5.

Q: What is a Group?

A group is a set equipped with a binary operation which satisfies three axioms.
Let $*$ be a binary operation on a set S.

1. Say $*$ is associative if $\forall a, b, c \in S$, $(a * b) * c = a * (b * c)$.

2. Say $*$ is commutative if $\forall a, b \in S$, $a * b = b * a$.

3. An element $e \in S$ is a neutral element (with respect to $*$) if $\forall a \in S$, $a * e = a = e * a$.

    - If there exists a neutral element, then it is unique.

4. Suppose $(S, *)$ has a neutral element e. Let $a \in S$. Then $b \in S$ is called an inverse of a (with respect to $*$) if $a * b = e = b * a$.

Group

A group is a set G equipped with a binary operation $*$ such that

1. $*$ is associative.

2. $*$ has a neutral element e.

3. Every $g \in G$ has an inverse.

If, in addition, $*$ is commutative, we say $(G, *)$ is an abelian or commutative group.

Examples

$(\mathbb{R}^3, +)$ is a commutative group.
$(\mathbb{R}^3, \times)$ has no neutral element.
$(\mathbb{Z}, \cdot)$ has no inverse (except ± 1).
$(\mathbb{R}^3, \text{mid})$ is not associative. (the midpoint)
$(M_{n\times n}(\mathbb{R}), \cdot)$ has no inverse of $0_{n\times n}$.
For $n \geq 1$, $(\mathbb{R}^n, +)$ and $(\mathbb{C}^n, +)$ are abelian groups.

Proof that the Neutral Element is unique.

Let e, e' be neutral eements. Then $e' = e * e' = e$. ■

Proof that the Inverse is unique.

Left to the reader.

Subgroup

Let G be a group, and let H be a subset of G. We say that H is a subgroup of G if

1. $\forall h_1, h_2 \in H$, $h_1 * h_2 \in H$.

2. $e \in H$.

3. $\forall h \in H$, $h^{-1} \in H$.

Examples

$\mathbb{Z}^n \subseteq \mathbb{R}^n$ is a subgroup $(* = +)$.
$G = \{A \in M_{n\times n} : \det(A) \neq 0\}$. Then $(G, \cdot)$ is a group.

- This is the General Linear Group on $\mathbb{R}$: $\mathrm{GL}_n(\mathbb{R})$.

- Recall $A^{-1} = \frac{1}{\det(A)}\left((-1)^{itj}\det(M_{\alpha_i})\right)$.

General Linear Subgroups

$S = \{A \in \mathrm{GL}_n(\mathbb{R}) : a_{ij} \in \mathbb{Z},\ \forall 1 \leq i, j \leq n\}$.
S is closed under $\cdot$ and $I_n \in S$, but for example

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{-1} = \frac{1}{1\cdot 4 - 2\cdot 3}\begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix}$$

so S is not a subgroup.
However, $T = \{A \in S : \det(A) = \pm 1\} \subseteq \mathrm{GL}_n(\mathbb{R})$.

- Note that if $AA' = I_n$ then $\det(A)\det(A') = 1$.

Additive Groups

For groups like $\mathbb{Z}^n$, $\mathbb{R}^n$ and $\mathbb{C}^n$, we will use $+$ for the binary operation and say that they are additive groups.
The Neutral Element is denoted as 0.
The inverse is denoted as $-g$.
For $m \geq 1$ and $g \in G$, $mg = g + \overset{m}{\cdots} + g$ and $(-m)g = -(mg)$.

Multiplicative Groups

For groups like $\mathrm{GL}_n(\mathbb{C})$ or $\mathrm{GL}_n(\mathbb{Z})$, we say that the group is multiplicative.
Denote the neutral element as 1.
Denote the inverse of g as g^{-1}.
For $m \geq 1$, $g^m = g \overset{m}{\cdots} g$.
$g^0 = 1$.
$g^{-m} = (g^m)^{-1}$.

Group Element Order

Let G be a group, $g \in G$, and $m \geq 1$.
Say g has order m if $g^m = 1$ and $g^k \neq 1,\ \forall k$ such that $1 \leq k \leq m$.
An element has infinite order if $g^m \neq 1,\ \forall m \in \mathbb{Z}^+$.

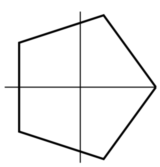
Examples

In D_{10}, I_2 has order 1, rotations have order 5 and reflections have order 2.

Groups from Geometry

Pentagon

Consider the regular pentagon P.



$H = \{T \in \mathrm{GL}_2(\mathbb{R}) : T(P) = P\}$.
This is the symmetry group of P or D_{10} (sometimes D_5)
$H \leq \mathrm{GL}_2(\mathbb{R})$.

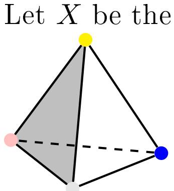
- Proof of closure. Suppose $T_1, T_2 \in H$. Then $T_1(P) = P$, $T_2(P) = P$ and $(T_1 \circ T_2)(P) = T_1(T_2(P)) = T_1(P) = P$.
  Therefore H is closed under $\circ$.

- Proof of identity. $\mathrm{Id}_{\mathrm{GL}_2} = I_2$ does satisfy $I_2(P)$.

- Proof of inverse. If $T \in H$ (i.e. $T \in \mathrm{GL}_2(\mathbb{R})$ and $T(P) = P$, apply T^{-1} and get $T^{-1}(T(P)) = T^{-1}(P)$. Therefore $P = T^{-1}(P)$.

Tetrahedron

Let X be the regular tetrahedron and $A = \{\text{rotational symmetries of } X\}$.



Then A contains

- The identity: 1.

- $2 \cdot 4 = 8$ rotations by 120°.

- 3 rotations of 180°.

So we have a bijection $r : \{B, P, W, Y\} \to \{B, P, W, Y\}$ where

$$\begin{tikzcd}[row sep=tiny]
B \arrow[r] & B \\
P \arrow[rddd] & P \\
W \arrow[ru] & W \\
Y \arrow[ru] & Y
\end{tikzcd}$$

Symmetric Group

Let S be a set (e.g. $E = \{B, P, W, Y\}$). The Symmetric Group $\mathrm{Sym}(E)$ is the set of bijections $f : E \to E$ equipped with the binary operation $\circ$ (composition).

October 3, 2023

Homework

First homework should be released this Thursday, October 5th.
Next lecture will be on group actions.

Symmetric Group

Let X be a set.
When $|X| = n$ denote the elements $\{1, 2, \ldots, n\}$.
$\mathrm{Sym}(X) = \{f : X \to X | f \text{ is bijective}\}$.
With $\circ$ (composition of functions) as a binary operation, $\mathrm{Sym}(X)$ is a group.

Symmetric Group Order

If $|X| = n$, then $|\mathrm{Sym}(X)| = n!$

- Proof Let $X = \{1, 2, \ldots, n\}$. A bijection f consists of $f(1), f(2), \ldots, f(n)$.
  For $f(1)$, we have n choices; for $f(2)$ we have $n - 1$ choices. This continues until only 1 choice remains for $f(n)$.
  Therefore the choices are $(n)(n-1)\cdots(1) = n!$

Example

For the symmetric group on four letters $\{a, b, c, d\}$, $|\mathrm{Sym}(4)| = 4! = 24$