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`)

Definition: 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

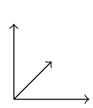
1. $S = \mathbb{R}^3$, define $f : S \times S \to S$ as $(\vec{x}, \vec{y}) \rightsquigarrow \vec{x} + \vec{y}$.

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 $a * b = e = b * a$.

Definition: 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.

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

Definition: 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 $\det(A)\det(A') = 1$.

Definition: 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 $(-m)g = -(mg)$.

Definition: 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 $m \geq 1$, $g^m = g \overset{m}{\cdots} g$.
$g^0 = 1$.
$g^{-m} = (g^m)^{-1}$.

Definition: 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 $g^m \neq 1,\ \forall m \in \mathbb{Z}^+$.

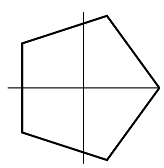
Examples

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)
$H \leq \mathrm{GL}_2(\mathbb{R})$.

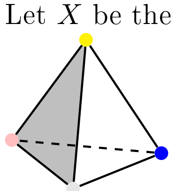
- Proof of closure. Suppose $T_1, T_2 \in H$. Then $T_1(P) = P$, $T_2(P) = P$ and $(T_1 \circ T_2)(P) = T_1(T_2(P)) = T_1(P) = P$.
  Therefore H is closed under $\circ$.

- 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

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

Definition: 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.

Propositions: 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

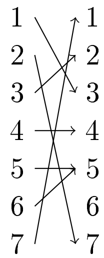
For the symmetric group on four letters $\{a, b, c, d\}$, $|\mathrm{Sym}(4)| = 4! = 24$

Definition: Cycles

Let $x = \{1, \ldots, n\}$, $m \geq 1$ be an integer and $a_1, a_2, \ldots, a_m$ distinct elements in X.
Then the m-cycle denoted by $(a_1\ a_2\ \cdots\ a_m)$ is the element of $\mathrm{Sym}(X)$ which maps a_1 to a_2, a_2 to a_3,..., a_{m-1} to a_m, and a_m to a_1.

Example

Let $n = 7$ and $m = 4$. Then $(2\ 7\ 1\ 3)$ is a bijection.



Degenerate Case

$m = 1$ gives Id_X.

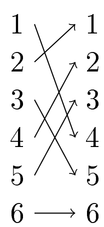
First Non-Degenerate Case

A transposition is, by definition a 2-cycle: $(a_1\ a_2)$.

Proposition: Symmetric Group as Cycle Composition

Every elenent in $\mathrm{Sym}(X)$ is the product (using $\circ$) of m-cycles, where m can vary.

- Proof Consider Sym(6).

  This gives a bijection $\pi = (1\ 4\ 2)(3\ 5)(6)$ which is the composition of cycles.
  We say that this π has cycle type $3 + 2 + 1$.

- Cycle Type If instead $\pi = (1\ 4\ 2)(3\ 5\ 6)$ then the cycle type is given as $3 + 3$.

Finite Symmetric Groups

For $n = 2$, $\mathrm{Sym}(X) = \{\mathrm{Id}, (1\ 2)\}$.
This gives cylce types $1 + 1$ and 2.
For $n = 3$, $\mathrm{Sym}(X) = \{\mathrm{Id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$.
This gives cycle types $1 + 1$, $2 + 1$ and 3.

Symmetric Group for Tetrahedron

For $n = 4$ let $X = \{B, P, W, Y\}$.
Partitions of $n = 4$ are

$$\begin{array}{llllllllll}
4 = 4 & 6 & (B\ P\ W\ Y) & \cdots & & & & & & \text{sign} = -1 \\
\ \ = 3+1 & 4 \cdot 2 = 8 & (P\ W\ Y) & \cdots & & & & & & \text{sign} = +1 \\
\ \ = 2+2 & \frac{\binom{4}{2}}{2} = 3 & (B\ P)(W\ Y) & (B\ W)(P\ Y) & (B\ Y)(P\ W) & & & & & \text{sign} = +1 \\
\ \ = 2+1+1 & \binom{4}{2} = 6 & (B\ P) & (B\ W) & (B\ Y) & (P\ W) & (P\ Y) & (W\ Y) & & \text{sign} = -1 \\
\ \ = 1+1+1+1 & 1 & \mathrm{Id}_X & & & & & & & \text{sign} = +1
\end{array}$$

Rotation Group for Tetrahedron

$$\begin{aligned} A &= \{\text{Rotational Symmetries}\} \\ &= \{\mathrm{Id}_X, 8 \text{ 3-cycles}, 3 \text{ of type } 2{+}2\} \end{aligned}$$

Note, from the sign, that $A \leq \mathrm{Sym}(4)$.

Symmetries Not in Rotation

Why, for example, is $(B\ P)$ not in the rotation group?
If it were, it should be possible to swap vertices and then undo the switch with only rotation.
However, the two tetrahedra are mirror images across a plane.
Observe that the right hand rule with respect to P, W and Y will give opposite, orthogonal vectors.

Rotation as a Subgroup of Symmetry

Q: Is A a subgroup of $\mathrm{Sym}(4)$?
Following the definition, it would be necessary to veryify

- $\mathrm{Id} \in A$
- A is closed under inverse.
- A is closed under composition.

Group Homomorphism

Let G and H be groups (whose binary operations are denoted by $g_1 \cdot g_2$).
A (group) homomorphism from G to H is a function $\phi : G \to H$ such that

- $\phi(g_1 \underset{G}{\cdot} g_2) = \phi(g_1) \underset{H}{\cdot} \phi(g_2)$

Properties of Group Homomorphism

1. $\phi(1_G) = 1_H$

2. $\phi(g^{-1}) = [\phi(g)]^{-1},\ \forall g \in G$

- Proof By definition, $\phi(1_G \cdot 1_G) = \phi(1_G) \cdot \phi(1_G)$.
  Letting $e = \phi(1_G)$, we get $e = e \cdot e$.
  By multiplying both sides by e^{-1}, we get $1_H = e$.
  Part two is left as an exercise.

Example 1

Let $n \geq 1$ and $G = \mathrm{GL}_n(\mathbb{R}) = \{A \in M_{n\times n}(\mathbb{R}) | \det(A) \neq 0\}$.
In particular, when $n = 1$, $\mathrm{GL}_1(\mathbb{R}) = \mathbb{R}^* = \{r \in \mathbb{R} | r \neq 0\}$ (with multiplication as the binary operation).
Then $\det : G \to H$ is a group homomorphism.
That is $\det(AB) = \det(A)\det(B)$ (as learned in MATH 21).

Example 2

Let $n \geq 1$, $G = \mathrm{Sym}(n)$, $H = \mathrm{GL}_n(\mathbb{R})$.
Construct a group homomorphism $\rho : G \to H$.

Recall that a linear transformation $A \in H$ is completely determined by $Ae_1,\ Ae_2,\ \ldots\ , Ae_n$ where $e_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \ldots, e_n = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$.
For $\pi \in G = \mathrm{Sym}(n)$, $\rho(\pi)$ is the linear transformation that maps e_i to e_j whenever π maps i to j.
This is a surjective linear transformation on a vector space and, therefore, invertible.

- Example For $n = 4$ and $\pi = (2\ 3\ 4)$

$$\begin{tikzcd}[row sep=tiny] 1 \arrow[r] & 1 \\ 2 \arrow[dr] & 2 \\ 3 \arrow[dr] & 3 \\ 4 \arrow[uur] & 4 \end{tikzcd} \quad \rho(\pi)$$

$$\begin{tikzcd}[row sep=tiny] e_1 \arrow[r] & e_1 \\ e_2 \arrow[dr] & e_2 \\ e_3 \arrow[dr] & e_3 \\ e_4 \arrow[uur] & e_4 \end{tikzcd} \quad \text{Therefore}$$

$$\rho(\pi) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

  – Is this a group homomorphism? Let $\pi_1, \pi_2 \in G$ be arbitrary elements.

Need to show: $\rho(\pi_1 \circ \pi_2) = \rho(\pi_1) \circ \rho(\pi_2)$.
Both sides are linear transformations and, hence, determined by their actions on e_i for $i = 1, \ldots, n$.

$$\begin{aligned} \rho(\pi_1 \circ \pi_2)e_i &= e_{\pi(i)} \\ &= e_{\pi_1(\pi_2(i))} \\ \rho(\pi_1)(\rho(\pi_2)e_i) &= \rho(\pi_1)(e_{\pi_2(i)}) \end{aligned}$$

Composition of Group Homomorphisms

Let G, H and K be groups and $G \xrightarrow{\phi} H$ and $H \xrightarrow{\psi} K$ be homomorphisms.
Then the composite $\psi \circ \phi : G \to K$ is a group homomorphism.

Proof

Let $g_1, g_2 \in G$ be arbitrary.

$$\begin{aligned} (\psi \circ \phi)(g_1 g_2) &= \psi(\phi(g_1 g_2)) && \text{by definition of } \circ \\ &= \psi(\phi(g_1 \phi(g_2)) && \text{since } \phi \text{ is a group homomorphism} \\ &= \psi(\phi(g_1))\psi(\phi(g_2)) && \text{since } \psi \text{ is a group homomorphism} \\ &= (\psi \circ \phi)(g_1) \circ (\psi \circ \phi)(g_2) && \text{by definition of } \circ \end{aligned}$$

Definition: Sign Homomorphism

Let $n \geq 1$ and $G = \mathrm{Sym}(n)$.
Ths sign homomorphism is the composition sign: $G \xrightarrow{\rho} \mathrm{GL}_n(\mathbb{R}) \xrightarrow{\det} \mathbb{R}^*$

Sign of Symmetric Group

$\mathrm{sign}(\mathrm{sym}(n)) \subseteq \{1, -1\} \leq \mathbb{R}^*$

- Lemma Let $a_1, \ldots, a_m$ be distinct numbers between 1 and n.
  Then $(a_1 \cdots a_m)$ is equal to $(a_1 \cdots a_{m-1})(a_{m-1}\ a_m)$.
  This will be proven on homework.

- Corollary Any m cycle is the composition of $m - 1$ transpositions.
  Namely, $(a_1, \ldots, a_m) = (a_1\ a_2)(a_2\ a_3)\cdots(a_{m-1}\ a_m)$.
  Easily check: $\mathrm{sign}((a_i\ a_{i+1})) = -1$.
  Now any $g \in \mathrm{Sym}(n)$ allows a cycle decomposition.

Definition: Kernel of a Homomorphism

Let $G \xrightarrow{\phi} H$ be a group homomorphism.
The kernel of ϕ is $\ker(\phi) := \{g \in G | \phi(g) = 1_H\}$.

The Kernel is a Subgroup

Let $g_1, g_2 \in \ker(\phi)$. Then

$$\begin{aligned} \phi(g_1 g_2) &= \phi(g_1)\phi(g_2) && \phi \text{ is a homomorphism} \\ &= 1_H 1_H && g_1, g_2 \in \ker(\phi) \\ &= 1_H && g_1, g_2 \in \ker(\phi) \end{aligned}$$

Similarly, $1_G \in \ker(\phi)$ and $g^{-1} \in \ker(\phi)$ if $g \in \ker(\phi)$. ■

Definition: Alternating Group

Let X be a set, $|X| = n \leq \infty$.
The alternating group on X is the $\mathrm{Alt}(X) = \ker(\mathrm{sign} : \mathrm{Sym}(X) \to \{\pm 1\})$.

October 5, 2023

Definition: Group Action

Let G be a group and X a set.
A (left) action of G on X is a function $\alpha : G \times X \to X$ which satisfies two conditions:

1. $\alpha(1_G, x) = x$ for all $x \in X$.

2. $\alpha(g_1, \alpha(g_2, x)) = \alpha(g_1 g_2, x)$ for all $g_1, g_2 \in G$ and $x \in X$.

Notation

Write $\alpha(g, x) = g * x = g \cdot x = gx$.

Example A

Let X be any set, and let $G = \mathrm{Sym}(X) = \{f : X \to X \text{ bijections}\}$ where the group operation $\circ$ is the composition of functions.
Then G acts (on the left) on X by $f * x \underset{\text{def}}{=} f(x)$.
Then the features

1. $\mathrm{Id}_X(x) = x,\ \forall x \in X$

2. $g_1 * (g_2 * x) = (g_1 \circ g_2) * x,\ \forall g_1, g_2 \in G,\ \forall x \in X$

    - Or $g_1(g_2(x)) = (g_1 \circ g_2)(x)$

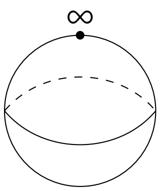
are satisfied.

Example B

Let $G = \mathrm{Sym}(\{B,\ P,\ W,\ Y\})$ which acts on $X = \{B,\ P,\ W,\ Y\}$.
If $H \leq G$, then H acts on X as well, define $h * x = \dot{h} * x$ (where $\dot{h}$ is regarded as in the alternating group of G).
In particular, $\mathrm{Alt}(\{B,\ P,\ W,\ Y\})$ acts on X by rotations.

Example C*

This example is not required for this class.
From complex Analysis we have the Riemann sphere $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$.



Let $G = \mathrm{SL}_2(\mathbb{C})$.
Define G-action on $X = \mathbb{P}^1(\mathbb{C})$ by

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} z := \frac{\alpha z + \beta}{\gamma z + \delta} \qquad (\infty \text{ if } \gamma z + \delta = 0)$$

This is called the Möbius group action on $\mathbb{P}^1(\mathbb{C})$.
Exercise: show that 1. and 2. are satisfied.

Definitions

Let G act on X. (Say X is a (left) G-set)

Stabilizer

Let $x \in X$. The stabilizer of x in G is $\mathrm{Stab}_G(x) = \{g \in G | g * x = x\} \subseteq G$.

- Example 1 Let G be any group and X a G-set.
  Then for any $x \in X$, $\mathrm{Stab}_G(x) \leq G$.

  - Proof
    1. $1_G \in \mathrm{Stab}_G(x)$ since, by definition, $1_G * x = x$.
       Therefore the identity is present.
    2. If $g_1, g_2 \in \mathrm{Stab}_G(x)$ are such that $g_1 * x = x$ and $g_2 * x = x$, then $(g_1 g_2) * x \underset{\text{2nd Axiom}}{=} g_1 * (g_2 * x) = g_1 * x = x$.
       Therefore the stabilizer is closed under composition.
    3. Say $g \in \mathrm{Stab}_G(x)$ and $g * x = x$. Apply g^{-1} to both sdies to get

    $$x \underset{\text{1st Axiom}}{=} 1_G * x = (g^{-1} g) * x \underset{\text{2nd Axiom}}{=} g^{-1} * (g * x) = g^{-1} * x$$

    Therefore the stabilizer is closed under inverse.

- Example 2 Let $G = \mathrm{Alt}(\{B,\ P,\ W,\ Y\})$ and consider $H = \mathrm{Stab}_G(W) = \{\mathrm{Id}, (B\ P\ Y), (B\ Y\ P)$.
  Fact: H does not act transitively on X, since W is fixed and no element $g \in H$ satisfies $g * W = B$.

Orbit

Let $x \in X$. The G-orbit of x in X is $G \cdot x = \{g * x | g \in G\} \subseteq X$.
Let G act on X and $x, y \in X$. Either $G \cdot x = G \cdot Y$ or $G \cdot x \cap G \cdot y = \varnothing$.
So X is the disjoint union of G-orbits.
e.g. $\{B,\ P,\ W,\ Y\} = \{W\} \coprod \{B,\ P,\ Y\}$ gives the $\mathrm{Stab}_G(W)$-orbits.

- Example 1 When $G = \mathrm{Alt}(X)$, for $X = \{B,\ P,\ W,\ Y\}$, there is only one orbit since $\forall x \in X$, $G \cdot x = X$.

- Example 2 When $G = \mathrm{Stab}_G(W)$, for $X = \{B,\ P,\ W,\ Y\}$, then $G \cdot W = \{W\}$ while

$$\begin{aligned} G \cdot B &= \{\mathrm{Id}(B),\ (B\ P\ Y)(B),\ (B\ Y\ P)(B)\} = \{B,\ P,\ Y\} \\ &= G \cdot P = \{\mathrm{Id}(P),\ (B\ P\ Y)(P),\ (B\ Y\ P)(P)\} = \{P,\ Y,\ B\} \\ &= G \cdot Y \end{aligned}$$

Transitivity

Say G acts transitively on X (or the action is transitive) if, for any pair $x, y \in X$, there exists $g \in G$ (depending on x and y) such that $g * x = y$.

- Example $G = \mathrm{Alt}(\{B,\ P,\ W,\ Y\}) \circlearrowright \{B,\ P,\ W,\ Y\}$ is transitive.

  - Proof Let $x, y \in X$ be arbitrary.
    If $x = y$, then take $g = \mathrm{Id}_X$ and we have $g * x = y$.
    Suppose $x \neq y$, then write $X = \{x,\ y,\ z,\ w\}$ and take $g = (x\ y)(z\ w)$. We have $g * x = y$.
    e.g. $x = P$, $y = Y$, $z = B$ and $w = W$ gives $g = (P\ Y)(B\ W)$.

- Exercise * This exercise is not required for the course.
  Prove that $\mathrm{SL}_2(\mathbb{C})$ acts transitively on $\mathbb{P}^1(\mathbb{C})$.
  Say $\mathbb{P}^1(\mathbb{C})$ is a homogeneous space under $\mathrm{SL}_2(\mathbb{C})$.

Proposition: Group Action Gives Group Homomorphisms

($\longrightarrow$) Let G act on X. Then

1. For any $g \in G$, the function $\pi_g : X \to X$ defined by $\pi_g(x) = g * x$ is a bijection of X, hence $\pi_G \in \mathrm{Sym}(X)$.

2. The function $G \xrightarrow{\phi} \mathrm{Sym}(X)$ given by $\phi(g) = \pi_g$ is a group homomorphism.

Proof of 1

Need to show that π_g is injective and surjective.
(Inj) Let $x, y \in X$ and assume $\pi_g(x) = \pi_g(y)$ (i.e. $g * x = g * y$).
Apply $g^{-1}*$ on both sides, such that $x = g^{-1} * (g * x) = g^{-1} * (g * y) = y$.
(Sur) Let $x \in X$ be arbitrary. Need to find $y \in X$ such that $\pi_g(y) = x$.
Take $y = g^{-1} * x$, and $\pi_g(y) = g * (g^{-1} * x) = x$.

Proof of 2

Need to show that $\forall g_1, g_2 \in G$, $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$.
$\phi(g_1 g_2) \in \mathrm{Sym}(X)$ is characterized by $[\phi(g_1 g_2)](x) = \pi_{g_1 g_2}(x) = (g_1 g_2) * x$.
On the other hand, $\phi(g_1)\phi(g_2) \in \mathrm{Sym}(X)$ is characterized by $[\phi(g_1)\phi(g_2)](x) = \phi(g_1)[\phi(g_2)(x)] = g_1 * (g_2 * x)$.
By the second group action axiom, these must be the same.

Proposition: Group Homomorphism Admits Group Action

($\longleftarrow$) Let $G \xrightarrow{\rho} \mathrm{Sym}(X)$ be a group homomorphism.
Then, by letting $g * x = \rho(g)(x) \in X$ we get a left G-action on X.

Proof

1. $1_G * x = \rho(1_G)(x) = \mathrm{Id}_X(x) = x$.

2. Let $g_1, g_2 \in G$ and $x \in X$. Then $(g_1 g_2) * x = [\rho(g_1 g_2)](x) = [\rho(g_1) \circ \rho(g_2)](x) = \rho(g_1)[\rho(g_2)(x)] = g_1 * (g_2 * x)$.

Definition: Right Group Actions

Let G be a group and X be a set. A right G-action on X is a function $\beta : X \times G \to X$ such that

1. $\beta(x, 1_G) = x, \ \forall x \in X$.

2. $\beta(x, g_1 g_2) = \beta(\beta(x, g_1), g_2), \ \forall g_1, g_2 \in G, \ \forall x \in X$.

Notation

$\beta(x, g) = x * g = x \cdot g = xg$

Remark

If $\alpha : G \times X \to X$ is a left action, we get a right action $\beta : X \times G \to X$ by $\beta(x, g) = \alpha(g^{-1}, x)$ and vice versa.
That is $x * g = g^{-1} * x$.
Proof recommended as an exercise.

Analogues

Stability, orbit and transitivty all have analogues which can be demonstrated by converting to left actions.

Definition: Cosets

Let $H \leq G$, and let $X = G$.
We have left action $H \times X \to X$ and $h * x = hx$ (taken in G).
As well as right action $X \times H \to X$ where $x * h = xh$.
A (left) H-coset is an orbit xH for some $x \in X$.
A (right) H-coset is an orbit Hx for some $x \in X$.

Example

Let $G = \mathrm{Alt}(4)$, $H = \mathrm{Stab}_G(W) = \{\mathrm{Id},\ (B\ P\ Y),\ (B\ Y\ P)\}$.

1. Take any $x \in H$, $xH = H$.

2. Take $x = (B\ P)(W\ Y)$, and $xH = \{(B\ P)(W\ Y), (B\ P)(W\ Y)(B\ P\ Y) = (P\ W\ Y),\ (B\ P)(W\ Y)(B\ Y\ P) = (B\ W\ Y)\}$.

3. There are two more; what are they?

October 10, 2023

Cosets Revisited

Let G be a group, $H \leq G$. Then a (left) H-coset in G is a set of the form

$$gH = \{gh | h \in H\}$$

, where $g \in G$

Coset Space

G/H is the set of H-cosets.

- Example For $G = \mathrm{Alt}(4)$, given $C_1 = H = \mathrm{Stab}_G(B) = \{1, (P\ W\ Y), (P\ Y\ W)\}$, we have
  $C_2 = (B\ P\ W)H = \{(B\ P\ W), (B\ P\ )(W\ Y), (B\ P\ Y)\}$
  $(B\ P\ W) \circ (P\ W\ Y) = (B\ P)(W\ Y)$

  P ⟵ B ⟵ B
  B ⟵ W ⟵ P
  Y ⟵ Y ⟵ W
  W ⟵ P ⟵ Y

  $(B\ P\ W) \circ (P\ Y\ W) = (B\ P\ Y)$

$$\begin{aligned} &\mathrm{P} \longleftarrow \mathrm{B} \longleftarrow \mathrm{B} \\ &\mathrm{Y} \longleftarrow \mathrm{Y} \longleftarrow \mathrm{P} \\ &\mathrm{W} \longleftarrow \mathrm{P} \longleftarrow \mathrm{W} \\ &\mathrm{B} \longleftarrow \mathrm{W} \longleftarrow \mathrm{Y} \end{aligned}$$

$C_3 = (B\ W\ P)H = \{(B\ W\ P), (B\ W\ Y), (B\ W)(P\ Y)\}$
$C_4 = (B\ Y\ P)H = \{(B\ Y\ P), (B\ Y\ )(P\ W), (B\ Y\ W)\}$
Then $G/H = \{C_1, C_2, C_3, C_4\}$.

- Q: What do the 3 elements in C3 have in common in geometric terms? C_3 sends B to W. Similarly, the cosets send B to all other vertices (including to itself).

Definition: Transporter

Let G be a group and X a G-set.
For two points, $x, y \in X$, the transporter $\mathrm{Trsp}_G(x, y) = \{g \in G | gx = y\}$.

Example

$G/H = \{\mathrm{Trsp}_G(B, B), \mathrm{Trsp}_G(B, P), \mathrm{Trsp}_G(B, W), \mathrm{Trsp}_G(B, Y)\}$

Note

When $x = y$, we recover $\mathrm{Trsp}_G(x, x) = \mathrm{Stab}_G(x)$.
For general G and H, there may not be a nice geometric action associated with it.
But G/H is still a G-set since $g^{'}(gH) = (g^{'}g)H$.

Proposition (B)

Let $H \leq G$ be a subgroup and let $g \in G$.
Then the map $H \xrightarrow{f} gH$ defined by $h \mapsto f(h) = gh$ is a bijection.

Proof

(Surjective) Any element x in gH is, by definition, of the form gh for some $h \in H$. So $x = f(h)$.
(Injective) Say $h_1, h_2 \in H$ satisfy $f(h_1) = f(h_2)$. That is $gh_1 = gh_2$. Multiplying g^{-1} on the left, we get $h_1 = h_2$.

Proposition (C)

Let G act on X, $x \in X$, and $g \in G$.
Take $y := gx$ and $H = \mathrm{Stab}_G(x)$. Then $gH = \mathrm{Trsp}_G(x, y)$.

Proof

$(\subseteq)$ Let $gh \in gH$ be arbitrary. Then

$$(gh) * x \underset{\text{Axiom 2}}{=} g * (h * x) \underset{h \in \mathrm{Stab}_G(x)}{=} g * x \underset{y = g * x}{=} y$$

Therefore $gh \in \mathrm{Trsp}_G(x,y)$.
($\supseteq$) Suppose $g' \in \mathrm{Trsp}_G(x,y)$. Consider $g^{-1}g'$. Then

$$(g^{-1}g') * x = g^{-1} * (g' * x) \underset{g' \in \mathrm{Trsp}_G(x,y)}{=} g^{-1}(y) = x$$

Therefore $(g^{-1}g') \in \mathrm{Stab}_G(x)$. Setting $g^{-1}g' := h$, so $g' = gh \in gH$.

Theorem: Orbit-Stabilizer Theorem

Let G act transitively on a set X (so that there is only one orbit in X, namely X itself). If $|G| < \infty$, then for any $x \in X$ we have

$$|X| \cdot |\mathrm{Stab}_G(x)| = |G|$$

Proof

Let us count $|G|$ by partitioning G into transporters.

$$G = \coprod_{y \in X} \mathrm{Trsp}_G(x,y)$$

Therefore

$$|G| = \sum_{y \in X} |\mathrm{Trsp}_G(x,y)| \underset{B+C}{=} \sum_{y \in X} |\mathrm{Stab}_G(x)| = |X||\mathrm{Stab}_G(x)| \quad \blacksquare$$

Theorem: Lagrange

If G is a finite group and $H \leq G$, then $|G| = |H| \cdot |G/H|$.

Proof (Sketch)

Apply the Orbit-Stabilizer Theorem to $X = G/H$.
This action is transitive as $g(1H) = gH$.
Note $gH = H \iff g \in H$ and $g1 \in H$.
Therefore $\mathrm{Stab}_G(1H) = \{g \in G \mid g(1H) = 1H\} = H$.

Corollary

If $H \leq G$ and $|G| < \infty$, then $|H| \mid |G|$.
The converse is not true. No subgroup of order 6 in $\mathrm{Alt}(4)$ (where $|\mathrm{Alt}(4)| = 12$).

Definition: Conjugate

Let G be a group, $H \leq G$, $g \in G$.

1. For $x \in G$ the g-conjugate of x is $gxg^{-1} = {}^g x$.

2. The g-conjugate of H is $gHg^{-1} = {}^g H = \{gxg^{-1} \mid x \in H\}$.

Example

Let $G = \mathrm{Alt}(4)$ and $H = \mathrm{Stab}_G(B) = \{1, (P\ W\ Y), (P\ Y\ W)\}$. Then, for $g = (B\ Y\ P)$

$$gHg^{-1} = \{1, (B\ W\ P), (B\ P\ W)\} = \mathrm{Stab}_G(Y)$$

$(B\ Y\ P)1(B\ P\ Y) = 1$
$(B\ Y\ P)(P\ W\ Y)(B\ P\ Y) = (B\ W\ P)$

$$\begin{array}{c}
\mathrm{W} \leftarrow \mathrm{W} \longleftarrow \mathrm{P} \longleftarrow \mathrm{B} \\
\mathrm{B} \longleftarrow \mathrm{P} \longleftarrow \mathrm{Y} \longleftarrow \mathrm{P} \\
\mathrm{P} \longleftarrow \mathrm{Y} \leftarrow \mathrm{W} \leftarrow \mathrm{W} \\
\mathrm{Y} \longleftarrow \mathrm{B} \longleftarrow \mathrm{B} \longleftarrow \mathrm{Y}
\end{array}$$

- Note: Shortcut $(gxg^{-1})^{-1} = (g^{-1})^{-1}x^{-1}g^{-1} = gx^{-1}g^{-1}$.
  Applying this to $g = (B\ Y\ P)$ with $x = (P\ W\ Y)$
  Therefore, from the previous calculation, $gx^{-1}g^{-1} = (gxg^{-1})^{-1} = (B\ P\ W)$.

Proposition: Geometric Meaning of Conjugate

Let G act on a set X, $x \in X$, $g \in G$, and define $y := g * x$.
Then for $H = \mathrm{Stab}_G(x)$, we have

$$gHg^{-1} = \mathrm{Stab}_G(y)$$

That is, the conjugate of a a stabilizer is a stabilizer.

Proof

$(\subseteq)$ Let $ghg^{-1} \in gHg^{-1}$ be arbitrary.
Then .

$$(ghg^{-1}) * y = g * (h * (g^{-1} * y))g * (h * x) = g * x = y$$

Therefore $ghg^{-1} \subseteq \mathrm{Stab}_G(y)$.
$(\supseteq)$ Let $g' \in \mathrm{Stab}_G(y)$ be arbitrary.
Consider $g^{-1}g'g$. Then

$$(g^{-1}g'g) * x = g^{-1} * (g' * (g * x)) = g^{-1} * (g' * y) = g^{-1} * y = x$$

Therefore $h := g^{-1}g'g \in H$. Then by multiplying g on the left and g^{-1} on the right, we get

$$g' = ghg^{-1} \in gHg^{-1}$$

Orbit-Stablizer Theorem and Lagrange

1. If G acts transitively on X, then all the stabilizers have the same cardinality because they are all conjugates. So the Orbit-Stabilizer Theorem is consistent.

2. If $X = G/H$, then $\mathrm{Stab}_G(1H) = H$. What about $\mathrm{Stab}_G(gH) = gHg^{-1}$?