Math 2070 Week 1

Topics: Groups

Motivation

- How many ways are there to color a cube, such that each face is either red or green?

  Answer: 10. Why?

- How many ways are there to form a triangle with three sticks of equal lengths, colored red, green and blue, respectively?

- What are the symmetries of an equilateral triangle?

  Dihedral Group D_3

Cayley Table

$*$	a	b	c
a	a^2	ab	ac
b	ba	b^2	bc
c	ca	cb	c^2

Cayley Table for D_3

$*$	r_0	r_1	r_2	s_0	s_1	s_2
r_0	r_0	r_1	r_2	s_0	s_1	s_2
r_1	r_1	r_2	r_0	s_1	s_2	s_0
r_2	r_2	r_0	r_1	s_2	s_0	s_1
s_0	s_0	s_2	s_1	r_0	r_2	r_1
s_1	s_1	s_0	s_2	r_1	r_0	r_2
s_2	s_2	s_1	s_0	r_2	r_1	r_0

Groups

Definition 1.1. *A group G is a set equipped with a binary operation $* : G \times G \longrightarrow G$ (typically called* **group operation** *or "* **multiplication** *"), such that:*

- **Associativity**

  $$(a * b) * c = a * (b * c),$$

  for all $a, b, c \in G$. In other words, the group operation is **associative** *.*

- **Existence of an Identity Element**

  There is an element $e \in G$, called an **identity element** *, such that:*

  $$g * e = e * g = g,$$

  for all $g \in G$.

- **Invertibility**

  Each element $g \in G$ has an **inverse** *$g^{-1} \in G$, such that:*

  $$g^{-1} * g = g * g^{-1} = e.$$

- Note that we do not require that $a * b = b * a$.

- We often write ab to denote $a * b$.

Definition 1.2. *If $ab = ba$ for all $a, b \in G$. We say that the group operation is* **commutative** *, and that G is an* **abelian group** *.*

Example 1.3. *The following sets are groups, with respect to the specified group operations:*

- $G = \mathbb{Q}\backslash\{0\}$, *where the group operation is the usual multiplication for rational numbers. The identity is $e = 1$, and the inverse of $a \in \mathbb{Q}\backslash\{0\}$ is $a^{-1} = \frac{1}{a}$. The group G is abelian.*
- $G = \mathbb{Q}$, *where the group operation is the usual addition $+$ for rational numbers. The identity is $e = 0$. The inverse of $a \in \mathbb{Q}$ with respect to $+$ is $-a$. Note that $\mathbb{Q}$ is* **NOT** *a group with respect to multiplication. For in that case, we have $e = 1$, but $0 \in \mathbb{Q}$ has no inverse $0^{-1} \in \mathbb{Q}$ such that $0 \cdot 0^{-1} = 1$.*

Exercise 1.4. *Verify that the following sets are groups under the specified binary operation:*

- $(\mathbb{Z}, +)$
- $(\mathbb{R}, +)$
- $(\mathbb{R}^{\times}, \cdot)$
- $(U_m, \cdot)$, *where $m \in \mathbb{N}$,*

$$U_m = \{1, \xi_m, \xi_m^2, \ldots, \xi_m^{m-1}\},$$

and $\xi_m = e^{2\pi i/m} = \cos(2\pi/m) + i\sin(2\pi/m) \in \mathbb{C}$.

- *The set of bijective functions $f : \mathbb{R} \longrightarrow \mathbb{R}$, where $f * g := f \circ g$ (i.e. composition of functions).*

Exercise 1.5. *1.* **WeBWork**

2. **WeBWork**

3. **WeBWork**

4. **WeBWork**

5. **WeBWork**

6. **WeBWork**

7. **WeBWork**

8. **WeBWork**

9. **WeBWork**

Example 1.6. *The set $G = \mathrm{GL}(2, \mathbb{R})$ of real 2×2 matrices with nonzero determinants is a group under matrix multiplication, with identity element:*

$$e = \begin{pmatrix} 1 & amp; 0 \\ 0 & amp; 1 \end{pmatrix}.$$

In the group G, we have:

$$\begin{pmatrix} a & amp; b \\ c & amp; d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & amp; -b \\ -c & amp; a \end{pmatrix}$$

Note that there are matrices $A, B \in \mathrm{GL}(2, \mathbb{R})$ such that $AB \neq BA$. Hence $\mathrm{GL}(2, \mathbb{R})$ is not abelian.

Exercise 1.7. *The set $\mathrm{SL}(2, \mathbb{R})$ (* **Special Linear Group** *) of real 2×2 matrices with determinant 1 is a group under matrix multiplication.*

Claim 1.8. *The identity element e of a group G is unique.*

Proof. Suppose there is an element $e' \in G$ such that $e'g = ge' = g$ for all $g \in G$. Then, in particular, we have:

$$e'e = e$$

But since e is an identity element, we also have $e'e = e'$. Hence, $e' = e$. □

Claim 1.9. *Let G be a group. For all $g \in G$, its inverse g^{-1} is unique.*

Proof. Suppose there exists $g' \in G$ such that $g'g = gg' = e$. By the associativity of the group operation, we have:

$$g' = g'e = g'(gg^{-1}) = (g'g)g^{-1} = eg^{-1} = g^{-1}.$$

Hence, g^{-1} is unique. $\square$

Let G be a group with identity element e. For $g \in G$, $n \in \mathbb{N}$, let:

$$g^n amp; := \underbrace{g \cdot g \cdots g}_{n \text{ times}}.$$

$$g^{-n} amp; := \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{n \text{ times}}$$

$$g^0 amp; := e.$$

Claim 1.10. *Let G be a group.*

1. *For all $g \in G$, we have:*
$$(g^{-1})^{-1} = g.$$

2. *For all $a, b \in G$, we have:*
$$(ab)^{-1} = b^{-1}a^{-1}.$$

3. *For all $g \in G$, $n, m \in \mathbb{Z}$, we have:*
$$g^n \cdot g^m = g^{n+m}.$$

Proof. **Exercise.** $\square$

Definition 1.11. *Let G be a group, with identity element e. The* **order** *of G is the number of elements in G. The* **order** $\operatorname{ord} g$ *of an $g \in G$ is the smallest $n \in \mathbb{N}$ such that $g^n = e$. If no such n exists, we say that g has* **infinite order** *.*

Theorem 1.12. *Let G be a group with identity element e. Let g be an element of G. If $g^n = e$ for some $n \in \mathbb{N}$, then* $\operatorname{ord} g$ *divides n.*

Proof. Shown in class. $\square$