Modern Algebra 1

Grant Talbert

September 5, 2024

College of Arts and Sciences
Department of Mathematics and Statistics
CAS MA 541

Contents

1 Introduction to Groups **2**
1.1 Applications 2
1.2 Symmetries 2
1.3 Integers Mod n 4

2 Groups **6**

Lecture 1: Syllabus Day

Tue 03 Sep 2024 09:30

Chapter 1

Introduction to Groups

1.1 Applications

Applied

- Physics & chemistry
- Comp sci - cryptography (Particularly RSA, ECC)
- Robotics??? Modelinng movements
- Economics??? Symmetries in games, game theory

Pure

- Symmetries of roots of polynomials, Galois
- Representation theory, relates groups to lin alg
- Symmetries in geometry & topology

1.2 Symmetries

Definition 1.1: Symmetry

A symmetry of a geometric object is a rearrangement of the figure preserving all properties (the arrangements of sides, vertices, distances, and angles).

For example, a 60/60/60 triangle can be rotated by 120 degrees without changing the shape, or it can be flipped directly about one of its vertices. Both preserve all geometric properties. These transformations are rotation and reflection, respectively. Translation technically works but they don't count cuz boring lol. However doing nothing to the triangle (identity transformation), it's symmetric about that transformation. Oh and flipping about a line (equiv to 180 deg rotation) isn't symmetric. However, we can then rotateit another 180 degrees to obtain a symmetry.

Claim. The only symmetries of a triangle are the identity, 2 rotations and 3 reflections.

Proof. Each symmetry is determined by the different possible locations of each *specific* vertex, and they can have 2 orientations (face up or down), and 3 locations per orientation. $3 \cdot 2 = 6$. ■

Remark

This group of symmetries, as we will learn later, is the dihedral group D_3.

We can compose symmetric transformations, giving rise to another symmetry. wow its almost as if its a group...

Call the rotation by 60 degrees transformation R, and call the reflection transformation S. Then we can compose functions:

$$SR \text{ is a symmetry..}$$

$$RR \text{ is a symmetry.}$$

$$SS \text{ is a symmetry..}$$

etc

Definition 1.2: Cayley Table

The Cayley Table of a group (of symmetries) is a table indexed by symmetries as rows and columns, whose entries in the row A and column B is the symmetry BA.

Cayley Table for D_3

R	R	S	RR	I	RS	RRS
S	1	2	3	4	5	6
RR	1	2	3	4	5	6
I	1	2	3	4	5	6
RS	1	2	3	4	5	6
RRS	1	2	3	4	5	6

To standardize the definition of a rotation and reflection, let's look at the symmetries of a square. We should find 8 symmetries (2 orientations, 4 vertices, $4 * 82 = 8$).

- Rotate 90 degrees R_{90}
- Rotate 180 degrees R_{180}
- Rotate 270 degrees R_{270}
- Rotate 0 degrees 1
- Reflect and rotate 0 degrees S
- Reflect and rotate 90 degrees $R_{90}S$
- Reflect and rotate 180 degrees $R_{180}S$
- Reflect and rotate 270 degrees $R_{270}S$

Cayley Table for the group D_4, represented with unconventional notation.

	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D'	D	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	D'	D
R_{270}	R_{270}	R_0	R_{90}	R_{180}	idk	idk	idk	idk
H	H	D	V	D'	R_0	R_{180}	R_{90}	R_{270}
V	V	D'	H	D	R_{180}	R_0	R_{270}	R_{90}
D	D	V	D'	H	R_{270}	R_{90}	R_0	R_{180}
D'	D'	H	D	V	R_{90}	R_{270}	R_{180}	R_0

This table has a few specfic properties:

- This table is filled in without introducing new properties (closure).
- Each symmetry can be represented as a composition of a standard 90 degree rotation r and a standard reflection s (basis of dihedral group).
- Everything times R_0 stays the same; $AR_0 = R_0A = A$ (itentity element).

Remark

The elements do not necessarily commute.

Lecture 2: Review of Proofs

Thu 05 Sep 2024 09:30

No discussion tomorrow - and they will all be canceled until the grad students get tf off strike

Notation. For $a, b \in \mathbb{Z}$, if a divides b, that is $b/a \in \mathbb{Z}$, then we weite $a|b$ to mean a divides b.

1.3 Integers Mod n

Definition 1.3: Integer Equivalence mod n

Integers $a, b \in \mathbb{Z}$ are equivalent mod n if n divides $a - b$ (the remainders are the same), and we write

$$a \equiv b \, (mod \, n).$$

For example, $7 + 4 \equiv 1 \, (mod \, 5)$, since $5|(11 - 1)$.

Definition 1.4: Integers modulo n

The set of integers modulo n is the set $\{0, \ldots, n-1\}$, and is denoted $\mathbb{Z}_n$. In $\mathbb{Z}_n$, addition and multiplication are done modulo n.

The Cayley Table for $\mathbb{Z}_6$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Proposition 1.1

Let $\mathbb{Z}_n$ be the set of integers modulo n, and let $a, b, c \in \mathbb{Z}_n$. We have

- $a + (b + c) = (a + b) + c \mod n$.
- There exists an additive identity 0 such that for all $a \in \mathbb{Z}_n$, $a + 0 = a \mod n$.
- For every $a \in \mathbb{Z}_n$, there exists an additive inverse $-a \in \mathbb{Z}_n$ such that $a + (-a) = -a + a = 0 \mod n$.
- $a + b = b + a \mod n$ for all $a, b \in \mathbb{Z}$.

Proof. (1) Since $(a + b) + c = a + (b + c)$ in the integers, then the remainders mod n are also equal. The rest of the proof is left as an exercise ■

Chapter 2

Groups

Definition 2.1: Binary Operation

Let G be a set. A binary operation on G is a function that assigns each ordered pair of elements of G to an element of G.

$$\cdot : G \times G \to G.$$

For example, in the case of $G = D_4$, then function composition $\circ(A, B) = BA$ is a binary operation on G. If $G = \mathbb{Z}_n$, then the binary operation is addition $+(a, b) = a + b \mod n$.

Definition 2.2: Group

Let G be a set together with a binary operation under which G is closed:

$$\cdot : G \times G \to G$$

$$\cdot : (a, b) \mapsto ab.$$

We say that G is a group under this operation if the following properties are satisfied:

1. Associativity - for any $a, b, c \in G$, $a(bc) = (ab)c$.
2. Identity - there exists some $e \in G$ such that for all $g \in G$, $ge = eg = g$.
3. Inverses - for all $a \in G$, there exists a corresponding $b \in G$ such that $ab = ba = e$. This is usually denoted a^{-1}.

Definition 2.3: Abelian Group

Let G be a group. We call G an **abelian** group if $ab = ba$ for all $a, b \in G$ (commutative property). Otherwise, the group is non-abelian.

For example, D_4 under function composition is called the Dihedral group of order 8, and $\mathbb{Z}_n$ under addition mod n is the group of integers mod n. D_4 is non-abelian, while $\mathbb{Z}_n$ is abelian. More examples:

- $\mathbb{Z}$ under addition is a group.
- $\mathbb{Z}$ under division is **not** a group.
- $\mathbb{Z}$ under multiplication is **not** a group.
- $\mathbb{R}^*$ (the set of nonzero reals) is a group under multiplication.
- $M_2(\mathbb{R})$ (set of 2×2 matrices with real entries) is a group under addition.

- $\mathrm{GL}_2(\mathbb{R}) \subseteq M_2(\mathbb{R})$ the general linear is a group under multiplication.

QUATERNIONS!

Let 1 be the identity matrix,

$$I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

where $i^2 = -1$. Then

$$I^2 = J^2 = K^2 = -1, \quad IJ = K, \quad JK = -I, \quad KI = J, \quad JI = -K,$$

$$KJ = -I, \quad IK = -J.$$

The group $\{\pm 1, \pm I, \pm J, \pm K\}$ is knpwn as the quaternion group under multipliaction.