CH1 Introduction to Group Theory

Symmetries of a Square

What is symmetry?

> "Symmetry is a vast subject, significant in art and nature. Mathematics lies at its root..." - Hermann Weyl

Our Goal: Describe all possible ways a square can be repositioned so that it occupies the same space.

Visual:

- Show a square with corners labeled P (pink), W (white), G (green), B (blue)
- Indicate that we want to find all motions that map the square onto itself

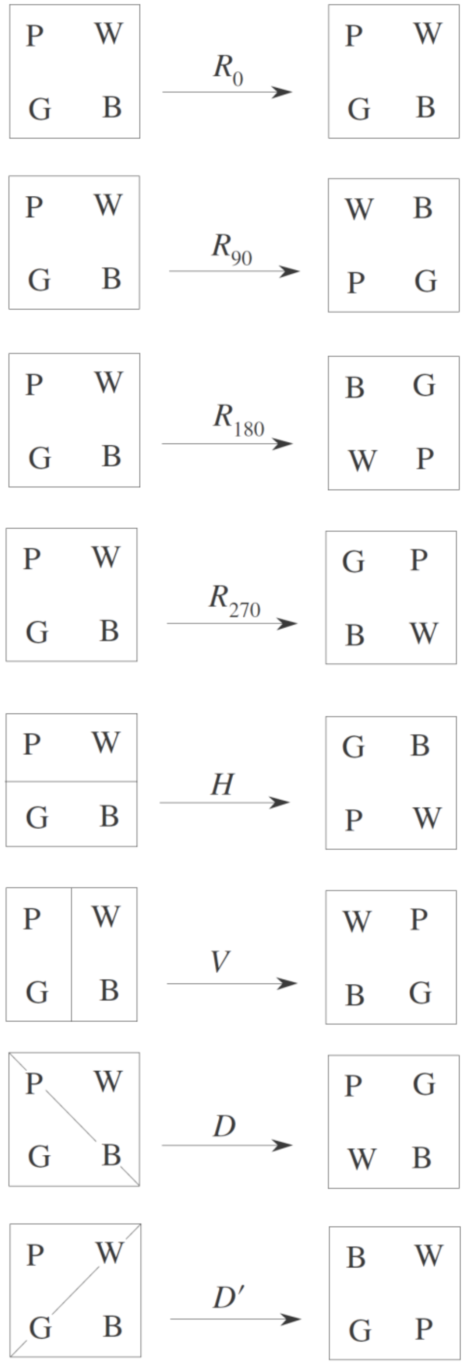
The Eight Symmetries of a Square

Rotations:

- $R_0 = 0^\circ$ rotation (identity)
- $R_{90} = 90^\circ$ counterclockwise rotation
- $R_{180} = 180^\circ$ rotation
- $R_{270} = 270^\circ$ counterclockwise rotation

Reflections:

- $H =$ Horizontal flip
- $V =$ Vertical flip
- $D =$ Main diagonal flip
- $D' =$ Other diagonal flip

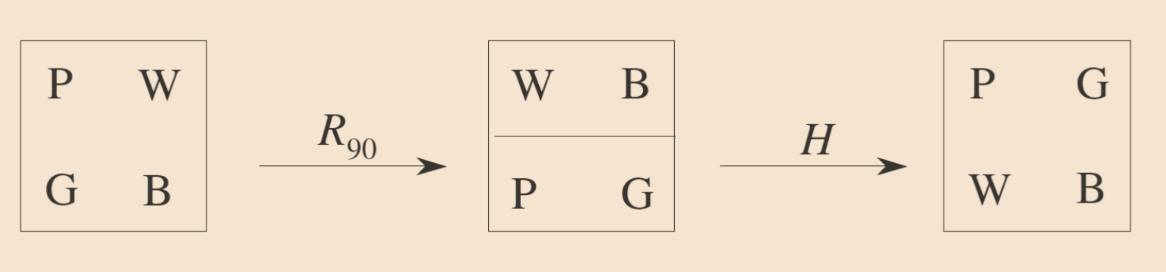


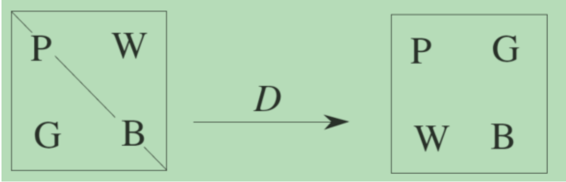
Key Observation: Composition

Example: What happens when we perform R_{90} followed by H?

Step-by-step transformation:

1. Starting position: P-W-G-B
2. After R_{90}: B-P-W-G
3. After H: G-W-P-B
4. Final result equals D





Key Insight: The composition of two symmetries is another symmetry!

Notation: $H \circ R_{90} = D$ (we write $H R_{90} = D$)

The Cayley Table for D_4

	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}	D	D'	V	H
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

Circle the entry $HR_{90} = D$

Properties We Observe in D_4

1. Closure: Every entry in the table is one of our eight elements

2. Identity: R_0 acts like "do nothing" - $AR_0 = R_0A = A$ for all A

3. Inverses: Each element has a partner that gives R_0:

- R_{90} and R_{270} are inverses
- H is its own inverse: $H^2 = R_0$
- Every row and column contains R_0 exactly once

4. Associativity: $(AB)C = A(BC)$ (harder to check, but true)

5. Non-commutativity: $HD \neq DH$ ($R_{180} \neq R_0$)

The Dihedral Groups

Generalizing: From Squares to Regular Polygons

Definition: For a regular n-gon ($n \geq 3$), the dihedral group D_n consists of:

- n rotations: $R_0, R_{\frac{360^\circ}{n}}, R_{\frac{2\cdot 360^\circ}{n}}, \ldots, R_{\frac{(n-1)\cdot 360^\circ}{n}}$
- n reflections through axes of symmetry

Order: $|D_n| = 2n$

Examples:

- D_3: symmetries of equilateral triangle (6 elements)
- D_4: symmetries of square (8 elements)
- D_5: symmetries of regular pentagon (10 elements)

Algebraic Description of D_n

Let:

- $R =$ rotation by $\dfrac{360^\circ}{n}$
- $F =$ any reflection

Then: $D_n = \{R^0, R^1, R^2, \ldots, R^{n-1}, F, RF, R^2F, \ldots, R^{n-1}F\}$

Key Relations:

1. $R^n = R_0$ (identity)
2. $F^2 = R_0$ (reflections are self-inverse)
3. $RF = FR^{-1}$ (fundamental commutation relation)

Example in D_{10}:
$R^3FR^7F = R^3F \cdot FR^{-7} = R^3 \cdot R^{-7} = R^{-4} = R^6$

Applications of Dihedral Groups

Art & Design:

- Corporate logos (Mercedes-Benz: D_3, Chrysler: D_5)
- Architectural patterns
- Decorative designs

Chemistry:

- Molecular symmetry (NH_3 has D_3 symmetry)
- Crystal structures

Biology:

- Starfish and sea creatures (D_5 symmetry)
- Snowflakes (D_6 symmetry)

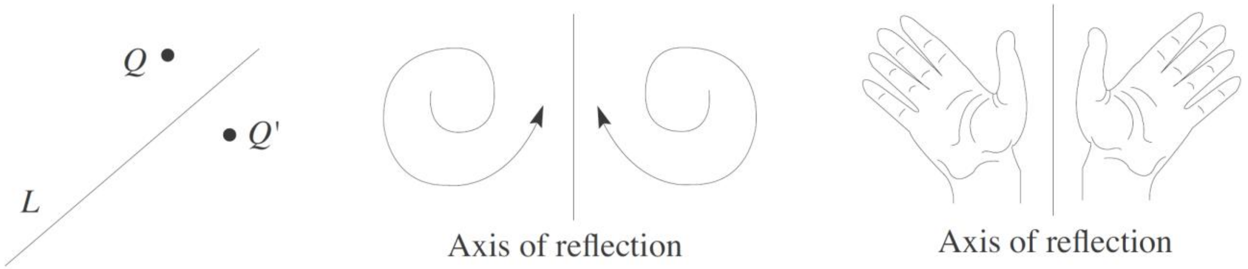


Figure 1.4 Reflected images.

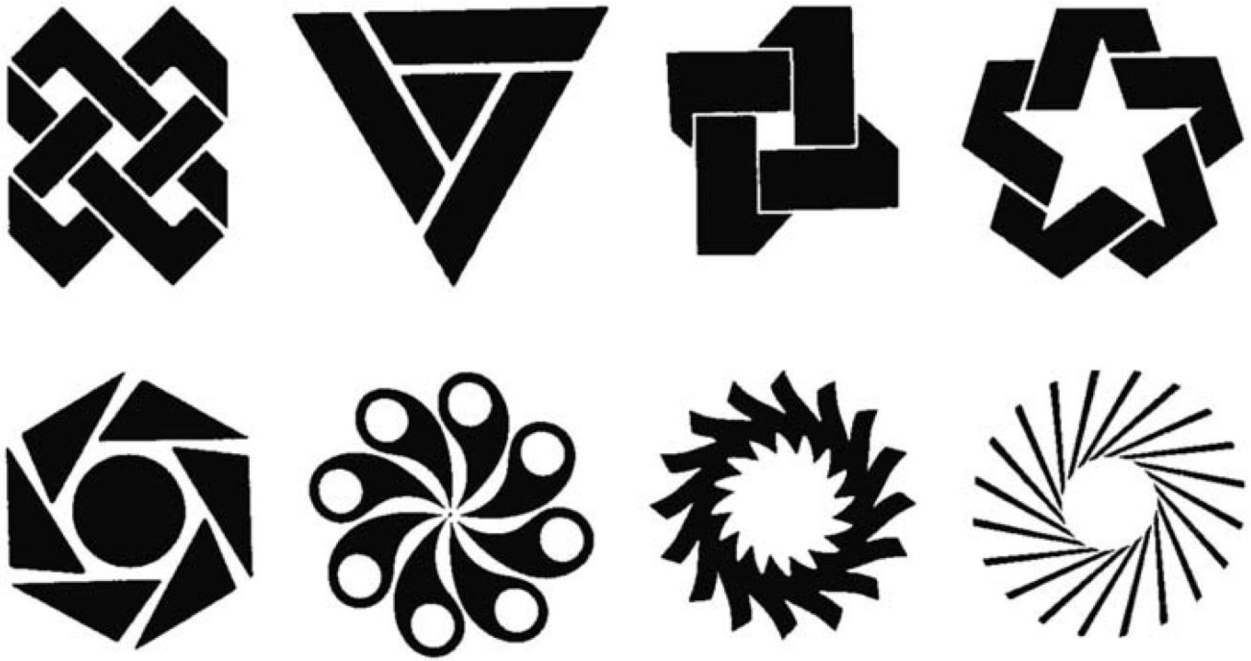


Figure 1.5 Logos with cyclic rotation symmetry groups.

CH 2 Groups

Formal Definition of Groups

What is a Binary Operation?

Definition: A binary operation on a set G is a function that assigns each ordered pair (a, b) of elements from G an element in G.

Examples:

- ✓ Addition on integers: $5 + 3 = 8 \in \mathbb{Z}$
- ✓ Matrix multiplication on 2×2 matrices
- ✗ Division on integers: $5 \div 3 \notin \mathbb{Z}$

Key Property: Closure - we never "leave" the set

Definition of a Group

Definition: A set G with binary operation $*$ is a **group** if:

G1. Associativity: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$

G2. Identity: $\exists e \in G$ such that $a * e = e * a = a$ for all $a \in G$

G3. Inverses: For each $a \in G$, $\exists b \in G$ such that $a * b = b * a = e$

Note: Closure is assumed in the definition of binary operation

Abelian vs Non-Abelian Groups

Definition: A group G is **Abelian** if $ab = ba$ for all $a, b \in G$

Examples:

- **Abelian:** $(\mathbb{Z}, +)$, $(\mathbb{Q}^*, \times)$, $(\mathbb{Z}_n, +)$
- **Non-Abelian:** D_4, $GL(2, \mathbb{R})$, matrix groups

Test for D_4:

- $HR_{90} = D$
- $R_{90}H = D'$
- Since $D \neq D'$, D_4 is non-Abelian

Examples of Groups

Number Systems as Groups

Example 1: $(\mathbb{Z}, +)$ - Integers under addition

- Identity: 0
- Inverse of k: $-k$
- Abelian: ✓

Example 2: $(\mathbb{Q}^*, \times)$ - Nonzero rationals under multiplication

- Identity: 1
- Inverse of a: $\frac{1}{a}$
- Abelian: ✓

Non-Example: $(\mathbb{Z}, \times)$ is NOT a group

- Why? 2 has no multiplicative inverse in $\mathbb{Z}$

Modular Arithmetic Groups

$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ under addition mod n

Example: $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

- Identity: 0
- Inverse of k: $n-k$ (e.g., inverse of 2 is 3)

Matrix Groups

$GL(2,\mathbb{R})$: 2×2 matrices with nonzero determinant

Matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ **has** $\det(A) = ad - bc$

Group Operation: Matrix multiplication

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}$$

Identity: $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Inverse of A: $A^{-1} = \dfrac{1}{\det(A)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

Why $\det(A) \neq 0$**?** So A^{-1} exists!

Units Modulo n: $U(n)$

$U(n) = \{k : 1 \leq k < n, \gcd(k, n) = 1\}$ under multiplication mod n

Example: $U(10) = \{1, 3, 7, 9\}$

$\times$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Key Fact: If p is prime, then $U(p) = \{1, 2, \ldots, p-1\}$

Complex Numbers and Roots of Unity

$\mathbb{C}^*$ under multiplication:

- $(a+bi)(c+di) = (ac-bd) + (ad+bc)i$
- Identity: 1
- Inverse of $a+bi$: $\dfrac{a-bi}{a^2+b^2}$

nth Roots of Unity: $\left\{\cos\left(\dfrac{2\pi k}{n}\right) + i\sin\left(\dfrac{2\pi k}{n}\right) : k = 0, 1, \ldots, n-1\right\}$

Example: 4th roots of unity: $\{1, i, -1, -i\}$

Visual: Unit circle with 6th roots of unity marked at 60° intervals

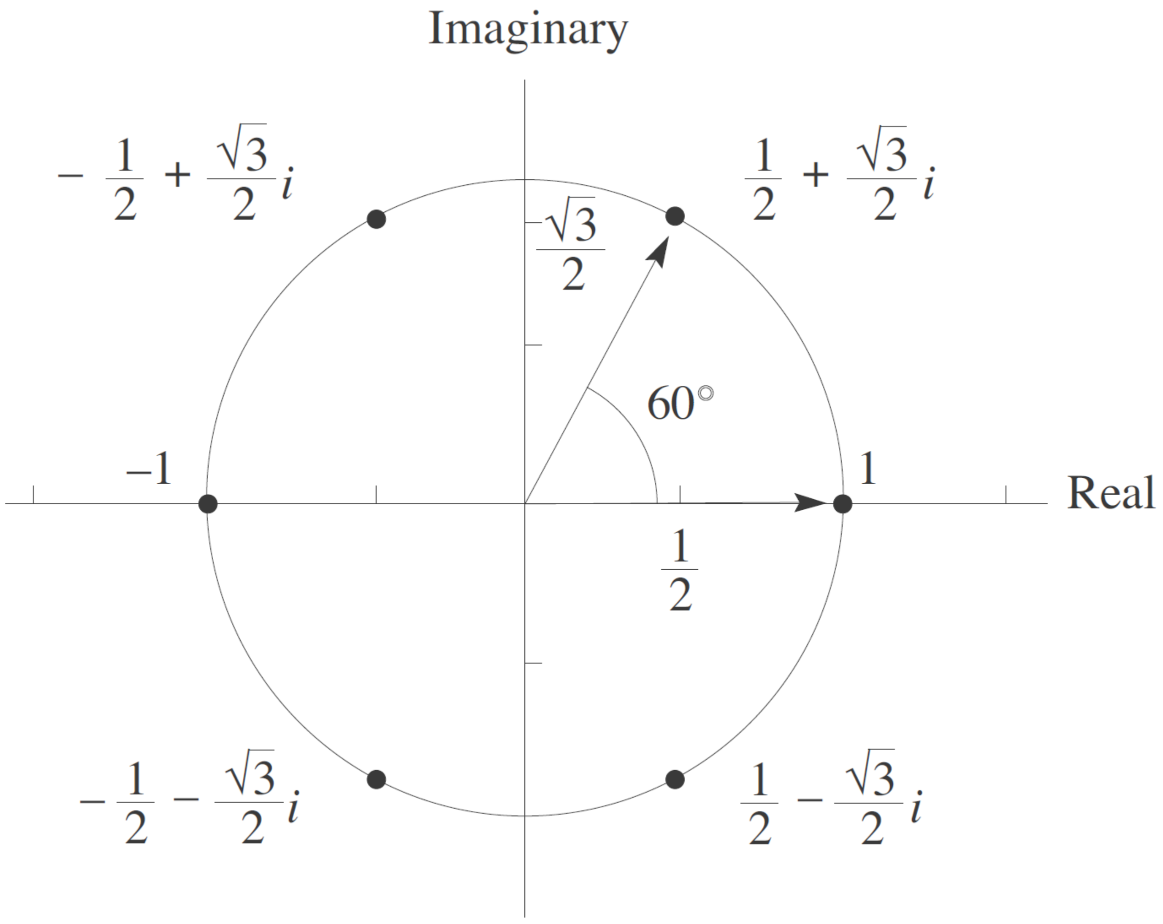


Figure 2.1 Zeros of $x^6 = 1$ on the unit circle.

Elementary Properties

Uniqueness of Identity

Theorem 2.1: In a group G, there is only one identity element.

Proof:
Suppose e and e' are both identities. Then:

1. $ae = a$ for all $a \in G$ (e is identity)
2. $e'a = a$ for all $a \in G$ (e' is identity)

Choose $a = e'$ in (1): $e'e = e'$
Choose $a = e$ in (2): $e'e = e$

Therefore: $e' = e'e = e$ ∎

Conclusion: We can speak of "the" identity e

Cancellation Laws

Theorem 2.2: In a group G, if $ba = ca$ then $b = c$, and if $ab = ac$ then $b = c$.

Proof of Left Cancellation:

Given: $ba = ca$

Let a' be the inverse of a

Multiply both sides on the right by a':

$(ba)a' = (ca)a'$

$b(aa') = c(aa')$ (associativity)

$be = ce$ (definition of inverse)

$b = c$ (definition of identity) ∎

Consequence: In a Cayley table, each element appears exactly once in each row and column.

Uniqueness of Inverses

Theorem 2.3: For each element a in a group G, there is a unique element b such that $ab = ba = e$.

Proof:

Suppose b and c are both inverses of a.

Then: $ab = e$ and $ac = e$

So: $ab = ac$

By cancellation: $b = c$ ∎

Notation: We write a^{-1} for the unique inverse of a

Examples:

- In $(\mathbb{Z}, +)$: $(-5)^{-1} = -(-5) = 5$
- In $(\mathbb{Q}^*, \times)$: $(2/3)^{-1} = 3/2$

The Socks-Shoes Property

Theorem 2.4: For group elements a and b, $(ab)^{-1} = b^{-1}a^{-1}$

Intuition: To undo "put on socks, then shoes," you must "take off shoes, then socks"

Proof:

We need to show $(ab)(b^{-1}a^{-1}) = e$

$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$ (associativity)
$= a(e)a^{-1}$ (definition of inverse)
$= aa^{-1}$ (definition of identity)
$= e$ (definition of inverse) ∎

Exponent Notation

For positive integer n: $a^n = a \cdot a \cdots a$ (n factors)

Special cases:

- $a^0 = e$ (by definition)
- $a^{-n} = (a^{-1})^n$ for $n > 0$

Laws of Exponents:

- $a^m a^n = a^{m+n}$
- $(a^m)^n = a^{mn}$

WARNING: In general, $(ab)^n \neq a^n b^n$

Example in D_4: $(HR_{90})^2 = D^2 = e$, but $H^2 R_{90}^2 = eR_{180} = R_{180}$

Additive vs Multiplicative Notation

Multiplicative Groups:

- Operation: ab
- Identity: e or 1
- Inverse: a^{-1}
- Powers: a^n

Additive Groups:

- Operation: $a + b$
- Identity: 0
- Inverse: $-a$
- Multiples: na (where n is an integer)

Example: In $(\mathbb{Z}_5, +)$:

- 3^{-1} means "inverse of 3" $= 2$ (since $3 + 2 = 0$)
- $3 \cdot 4$ means "4 added to itself 3 times" $= 12 \equiv 2 \pmod 5$

Our Growing Library of Groups

Finite Groups:

- D_n (dihedral groups)
- $\mathbb{Z}_n$ (integers mod n)
- $U(n)$ (units mod n)
- Symmetric groups S_n (to come!)

Infinite Groups:

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$
- $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$
- $GL(n, \mathbb{R})$ (matrix groups)

Looking Ahead

Next Topics:

- **Subgroups:** Groups within groups
- **Cyclic Groups:** Generated by a single element
- **Permutation Groups:** Rearrangements and Cayley's theorem
- **Quotient Groups:** Factoring out symmetry
- **Homomorphisms:** Maps between groups
- **Group Actions:** Groups acting on sets