MATH 417, HOMEWORK 1

CHARLES ANCEL

Exercise 1.1.3. Determine the rotational symmetries of a brick with three unequal sides.

---

1. Introduction

A brick is a rectangular prism with dimensions $a \times b \times c$, where $a \neq b \neq c$. We aim to determine the rotational symmetries of such a brick, i.e., all rotations that map the brick onto itself while preserving its geometric structure.

Proof. 2. Rotational Symmetries

To find the rotational symmetries, we consider rotations around the principal axes passing through the centers of the faces of the brick. These axes are:

– x-axis: through the centers of the faces of dimension $b \times c$

– y-axis: through the centers of the faces of dimension $a \times c$

– z-axis: through the centers of the faces of dimension $a \times b$

2.1. **Symmetries Catalog.**

Notation	**Angle**	**Axis**	**Effect on Brick**
e	0°	–	No change (Identity rotation)
r_x^2	180°	x-axis	Swaps front/back, reverses top/bottom
r_y^2	180°	y-axis	Swaps left/right, reverses top/bottom
r_z^2	180°	z-axis	Swaps top/bottom, reverses front/back
r_x	90°	x-axis	Rotates front to top, top to back, back to bottom, etc.
r_y	90°	y-axis	Rotates left to top, top to right, right to bottom, etc.
r_z	90°	z-axis	Rotates top to left, left to bottom, bottom to right, etc.
r_x^3	270°	x-axis	Rotates front to bottom, bottom to back, back to top, etc.
r_y^3	270°	y-axis	Rotates left to bottom, bottom to right, right to top, etc.
r_z^3	270°	z-axis	Rotates top to right, right to bottom, bottom to left, etc.

Table 1: Rotational symmetries of a brick with unequal sides.

3. Conclusion

Summarizing the distinct rotational symmetries, we have:

– Identity rotation: 1

– 180° rotations around principal axes: 3

– 90° and 270° rotations around principal axes: 6

Therefore, the total number of rotational symmetries of a brick with three unequal sides is:

$$1 + 3 + 6 = 10$$

Considering only rotational symmetries, the count is:

$$\boxed{10}$$

□

Exercise 1.3.3. Here is another way to list the symmetries of the square.

a. Verify that the four symmetries a, b, c, d that exchange the top and bottom faces of the card are a, ra, r^2a, r^3a, in some order. Thus, a complete list of symmetries is $\{e, r, r^2, r^3, a, ra, r^2a, r^3a\}$.

b. Verify that $ar = r^{-1}a = r^3a$.

c. Conclude that $ar^k = r^{-k}a$ for all $k \in \mathbb{Z}$.

d. Show that these relations suffice to compute every product.

a. Verify that the four symmetries a, b, c, d that exchange the top and bottom faces of the card are a, ra, r^2a, r^3a, in some order. Thus, a complete list of symmetries is:

$$\{e, r, r^2, r^3, a, ra, r^2a, r^3a\}.$$

Proof.

- e is the identity (no change).
- r represents a 90° rotation counterclockwise.
- r^2 represents a 180° rotation.
- r^3 represents a 270° rotation counterclockwise (or 90° clockwise).
- a is a reflection across the vertical axis.
- ra, r^2a, r^3a represent reflections after 90°, 180°, and 270° rotations respectively.
- By enumerating and verifying these operations on a square, all symmetries are included in the set $\{e, r, r^2, r^3, a, ra, r^2a, r^3a\}$.

□

b. Verify that $ar = r^{-1}a = r^3a$.

$$ar = r^{-1}a = r^3a.$$

Proof.

- Consider ar: Rotate by 90° counterclockwise (apply r) and then reflect across the vertical axis (apply a).
- This is equivalent to reflecting first (apply a) and then rotating by 90° clockwise (apply r^{-1}).
- Therefore, $ar = r^{-1}a$.
- Since $r^{-1} = r^3$ in a modulo 4 system (as $r^4 = e$), we have:

$$ar = r^{-1}a = r^3a.$$

□

c. Conclude that $ar^k = r^{-k}a$ for all $k \in \mathbb{Z}$.

$$ar^k = r^{-k}a.$$

Proof.

- We use induction on k.
- Base case: For $k = 1$:
$$ar = r^{-1}a.$$
- Assume $ar^k = r^{-k}a$ for some k.
- For $k + 1$:
$$\begin{aligned} ar^{k+1} &= ar^k \cdot r \\ &= r^{-k}a \cdot r \\ &= r^{-k} \cdot r \cdot a \\ &= r^{-(k+1)}a. \end{aligned}$$
- Similarly, for $k = -1$:
$$ar^{-1} = r \cdot a.$$
- Assume $ar^{-k} = r^k a$ for some k.
- For $k + 1$:
$$\begin{aligned} ar^{-(k+1)} &= ar^{-k-1} \\ &= ar^{-k} \cdot r^{-1} \\ &= r^k a \cdot r^{-1} \\ &= r^k \cdot r^{-1} \cdot a \\ &= r^{k-1}a. \end{aligned}$$
- Therefore, $ar^k = r^{-k}a$ holds for all $k \in \mathbb{Z}$.

□

d. Show that these relations suffice to compute every product.

Proof.

- Consider any product $x \cdot y$, where x and y are elements from the set $\{e, r, r^2, r^3, a, ra, r^2a, r^3a\}$.
- Using the relations:
$$\begin{aligned} ar^k &= r^{-k}a, \\ a^2 &= e, \end{aligned}$$
- We can compute any product:
  - For $x = r^i$ and $y = r^j$:
$$r^i \cdot r^j = r^{i+j \mod 4}.$$

  - For $x = r^i$ and $y = ar^j$:
$$r^i \cdot ar^j = ar^{-i}r^j = ar^{j-i}.$$
  - For $x = ar^i$ and $y = r^j$:
$$ar^i \cdot r^j = a \cdot r^{-i}r^j = ar^{j-i}.$$
  - For $x = ar^i$ and $y = ar^j$:
$$ar^i \cdot ar^j = a \cdot r^{-i} \cdot ar^j = a^2 \cdot r^{-i}r^j = r^{-i+j}.$$

- Using these relations, any product of the symmetries can be computed.

$\square$

Exercise 3. An **affine transformation** of $\mathbb{R}^n$ is a function $T : \mathbb{R}^n \to \mathbb{R}^n$ of the form $T(x) = Ax + b$, where $A \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ and $b \in \mathbb{R}^n$

a. Show that if $T, U : \mathbb{R}^n \to \mathbb{R}^n$ are affine transformations, so is the composite function $U \circ T$.

b. Show that $T(x) \stackrel{\text{def}}{=} Ax + b$ is a bijection if and only if A is an invertible matrix. We call such T an **invertible affine transformation.**

c. Show that if T is an invertible affine transformation, then its inverse function is also an invertible affine transformation.

---

a. **Composite of Affine Transformations:**

Proof. Let $T(x) = A_1x + b_1$ and $U(x) = A_2x + b_2$ be affine transformations. We need to show that the composite function $U \circ T$ is also an affine transformation.

$$\begin{aligned}(U \circ T)(x) &= U(T(x)) \\ &= U(A_1x + b_1) \\ &= A_2(A_1x + b_1) + b_2 \\ &= A_2A_1x + A_2b_1 + b_2\end{aligned}$$

Let $A = A_2A_1$ and $b = A_2b_1 + b_2$. Thus,

$$(U \circ T)(x) = Ax + b,$$

which is an affine transformation. Hence, the composite of two affine transformations is also an affine transformation.

□

b. **Bijection of Affine Transformation:**

Proof. Let $T(x) = Ax + b$.

(⇒) Suppose T is a bijection:

- **Surjectivity**: For every $y \in \mathbb{R}^n$, there exists $x \in \mathbb{R}^n$ such that $T(x) = y$. Thus, $Ax + b = y$, or $Ax = y - b$. Since A maps to all y, A must cover all of $\mathbb{R}^n$, implying A is surjective and hence invertible.
- **Injectivity**: If $T(x_1) = T(x_2)$, then $Ax_1 + b = Ax_2 + b$, or $A(x_1 - x_2) = 0$. Since A is invertible, $x_1 - x_2 = 0$, hence $x_1 = x_2$, showing T is injective.

Therefore, T is bijective if A is invertible.

(⇐) Suppose A is invertible:

- Define A^{-1} such that $A^{-1}A = I$. Let $T(x_1) = T(x_2)$. Then $Ax_1 + b = Ax_2 + b$, which simplifies to $A(x_1 - x_2) = 0$. Since A is invertible, $x_1 - x_2 = 0$, so $x_1 = x_2$, proving injectivity.
- To show surjectivity, for any $y \in \mathbb{R}^n$, let $x = A^{-1}(y-b)$. Then $T(x) = A(A^{-1}(y-b)) + b = y$, proving surjectivity.

Therefore, $T(x)$ is a bijection if and only if A is invertible.

□

c. **Inverse of an Invertible Affine Transformation:**

Proof. Suppose $T(x) = Ax + b$ is an invertible affine transformation. We need to show that T^{-1} is also an affine transformation.

- Assume A is invertible. To find $T^{-1}(y)$ for $y \in \mathbb{R}^n$:

$$\begin{aligned} T(x) &= y \\ Ax + b &= y \\ Ax &= y - b \\ x &= A^{-1}(y - b) \end{aligned}$$

  Define $T^{-1}(y) = A^{-1}y - A^{-1}b$.
- Verify that T^{-1} is indeed the inverse:

$$\begin{aligned} T(T^{-1}(y)) &= A(A^{-1}y - A^{-1}b) + b \\ &= y - b + b \\ &= y \\ T^{-1}(T(x)) &= A^{-1}(Ax + b - b) \\ &= A^{-1}Ax \\ &= x \end{aligned}$$

- Therefore, $T^{-1}(y) = A^{-1}y - A^{-1}b$ is also an affine transformation, with A^{-1} as the linear part and $-A^{-1}b$ as the translation part.

□

Exercise 1.5.3. Work out the decomposition in disjoint cycles for the following:

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 6 & 3 & 7 & 4 & 1 \end{pmatrix}$

(b) $(1\ 2)(1\ 2\ 3\ 4\ 5)$

(c) $(1\ 4)(1\ 2\ 3\ 4\ 5)$

(d) $(1\ 2)(2\ 3\ 4\ 5)$

(e) $(1\ 3)(2\ 3\ 4\ 5)$

(f) $(1\ 2)(2\ 3)(3\ 4)$

(g) $(1\ 2)(1\ 3)(1\ 4)$

(h) $(1\ 3)(1\ 2\ 3\ 4)(1\ 3)$

SOLUTIONS

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 6 & 3 & 7 & 4 & 1 \end{pmatrix}$
Solution: We start with 1:

$$1 \to 2 \to 5 \to 7 \to 1$$

Cycle: $(1\ 2\ 5\ 7)$
Next, we start with 3:

$$3 \to 6 \to 4 \to 3$$

Cycle: $(3\ 6\ 4)$
Disjoint cycles:

$$(1\ 2\ 5\ 7)(3\ 6\ 4)$$

(b) $(1\ 2)(1\ 2\ 3\ 4\ 5)$
Solution: Apply the permutations in sequence:

$$(1\ 2) \circ (1\ 2\ 3\ 4\ 5)$$

Start with 1:

$$1 \to 2 \to 1 \to 3 \to 4 \to 5 \to 2$$

Cycle: $(1\ 2)$
Next:

$$1 \to 2 \to 3 \to 5 \to 4$$

Cycle: $(1\ 2\ 3\ 5\ 4)$

(c) $(1\ 4)(1\ 2\ 3\ 4\ 5)$
Solution: Apply the permutations in sequence:

$$(1\ 4) \circ (1\ 2\ 3\ 4\ 5)$$

Start with 1:

$$1 \to 4 \to 5 \to 1$$

Cycle: (1 4 5)
Continue with 2:

$$2 \to 3 \to 2$$

Cycle: (2 3)
Disjoint cycles:

$$(1\ 4\ 5)(2\ 3)$$

(d) (1 2)(2 3 4 5)
Solution: Apply the permutations in sequence:

$$(1\ 2) \circ (2\ 3\ 4\ 5)$$

Start with 1:

$$1 \to 2 \to 3 \to 4 \to 5$$

Cycle: (1 2 3 4 5)
Continue:

$$1 \to 2 \to 5 \to 4 \to 3$$

Simplifies to: (1 2 5)(3 4)

(e) (1 3)(2 3 4 5)
Solution: Apply the permutations in sequence:

$$(1\ 3) \circ (2\ 3\ 4\ 5)$$

Start with 1:

$$1 \to 3 \to 4 \to 5$$

Cycle: (1 3 5)
Continue:

$$2 \to 3 \to 4$$

Cycle: (2 4)
Disjoint cycles:

$$(1\ 3\ 5)(2\ 4)$$

(f) (1 2)(2 3)(3 4)
Solution: Apply the permutations in sequence:

$$(1\ 2) \circ (2\ 3) \circ (3\ 4)$$

Start with 1:

$$1 \to 2 \to 3 \to 4$$

Cycle: (1 2 3 4)
Since the rest only flips between 2 and 3, this simplifies to:

$$(1\ 4)(2\ 3)$$

(g) (1 2)(1 3)(1 4)
Solution: Apply the permutations in sequence:

$$(1\ 2) \circ (1\ 3) \circ (1\ 4)$$

Start with 1:

$$1 \to 4 \to 1 \to 3 \to 1 \to 2$$

Cycle: (1 4 3 2)

(h) (1 3)(1 2 3 4)(1 3)
Solution: Apply the permutations in sequence:

$$(1\ 3) \circ (1\ 2\ 3\ 4) \circ (1\ 3)$$

Start with 1:

$$1 \to 3 \to 1 \to 2 \to 3$$

Cycle: (1 2 4)
Disjoint cycles:

$$(1\ 2\ 4)(3)$$

Exercise 1.5.5.. Show that any k-cycle $(a_1 \dots a_k)$ can be written as a product of $(k-1)$ 2-cycles. Conclude that any permutation can be written as a product of some number of 2-cycles.

Proof.

Part 1: k-cycle as a Product of 2-cycles. Consider a k-cycle $\sigma = (a_1\, a_2\, \dots\, a_k)$, where σ maps a_i to a_{i+1} for $1 \leq i < k$, and σ maps a_k back to a_1. We will show that σ can be decomposed into $(k-1)$ 2-cycles.

$$\begin{aligned}\sigma &= (a_1\, a_2\, \dots\, a_k) \\ &= (a_1\, a_k)(a_1\, a_{k-1}) \cdots (a_1\, a_3)(a_1\, a_2)\end{aligned}$$

To verify this decomposition, consider the action of the product of 2-cycles on each element:

– For a_1:
$$(a_1\, a_k) \cdots (a_1\, a_2)(a_1) = a_2$$
Each 2-cycle swaps a_1 with the respective a_i it pairs with, ultimately resulting in a_1 being mapped to a_2.

– For a_2:
$$(a_1\, a_k) \cdots (a_1\, a_2)(a_2) = a_3$$
The first 2-cycle fixes a_2, and each subsequent 2-cycle swaps a_2 until it is mapped to a_3.

– Continuing similarly:
$$(a_1\, a_k) \cdots (a_1\, a_2)(a_i) = a_{i+1} \quad \text{for } 2 \leq i < k$$

– For a_k:
$$(a_1\, a_k) \cdots (a_1\, a_2)(a_k) = a_1$$
Each 2-cycle moves a_k back to a_1.

Thus, $\sigma = (a_1\, a_k)(a_1\, a_{k-1}) \cdots (a_1\, a_3)(a_1\, a_2)$, confirming the decomposition into $(k-1)$ 2-cycles.

Part 2: Any Permutation as a Product of 2-cycles. Any permutation π in S_n can be written as a product of disjoint cycles. Let $\pi = \tau_1 \tau_2 \cdots \tau_m$, where τ_i are disjoint cycles. Each τ_i can be expressed as a product of 2-cycles as shown in Part 1. Therefore, π can be written as a product of 2-cycles. $\square$

Exercise 1.5.9.. Let σ_n denote the perfect shuffle of a deck of $2n$ cards. Regard σ_n as a bijective function of the set $\{1, 2, \ldots, 2n\}$. Find a formula for $\sigma_n(j)$ when $1 \leq j \leq n$, and another formula for $\sigma_n(j)$ when $n+1 \leq j \leq 2n$. (The "perfect shuffle" is described in Example 1.5.2.)

Solution

A **perfect shuffle** interleaves the two halves of a deck of $2n$ cards. Assume the deck is represented by the sequence $\{1, 2, \ldots, 2n\}$. The perfect shuffle operation, denoted by σ_n, interleaves the two halves as follows:

Proof.

Formulas for σ_n. Case 1: $1 \leq j \leq n$

For the first half of the deck:

$$\sigma_n(j) = 2j - 1$$

Derivation:

– Consider the original position j in the first half $\{1, 2, \ldots, n\}$.

– In the shuffled deck, the position is odd, and each element from the first half goes to the positions $1, 3, 5, \ldots, 2n - 1$.

– Hence, j is mapped to $2j - 1$.

Case 2: $n + 1 \leq j \leq 2n$

For the second half of the deck:

$$\sigma_n(j) = 2(j - n)$$

Derivation:

– Consider the original position j in the second half $\{n + 1, n + 2, \ldots, 2n\}$.

– In the shuffled deck, the position is even, and each element from the second half goes to the positions $2, 4, 6, \ldots, 2n$.

– Hence, j is mapped to $2(j - n)$, which simplifies to $2j - 2n$.

Verification. To verify these formulas, consider the following example with $n = 3$:

– Original deck: $\{1, 2, 3, 4, 5, 6\}$

– First half: $\{1, 2, 3\}$

– Second half: $\{4, 5, 6\}$

– Shuffled deck: $\{1, 4, 2, 5, 3, 6\}$

Applying the formulas:

– For $1 \leq j \leq 3$: $\sigma_3(j) = 2j - 1$

$$\sigma_3(1) = 2(1) - 1 = 1$$
$$\sigma_3(2) = 2(2) - 1 = 3$$
$$\sigma_3(3) = 2(3) - 1 = 5$$

– For $4 \leq j \leq 6$: $\sigma_3(j) = 2(j - 3)$

$$\sigma_3(4) = 2(4 - 3) = 2$$
$$\sigma_3(5) = 2(5 - 3) = 4$$
$$\sigma_3(6) = 2(6 - 3) = 6$$

Therefore, the shuffled deck is $\{1, 4, 2, 5, 3, 6\}$, which matches our calculation.

Conclusion

We have derived the formulas for the perfect shuffle σ_n:

$$\sigma_n(j) = \begin{cases} 2j - 1 & \text{if } 1 \leq j \leq n \\ 2(j - n) & \text{if } n + 1 \leq j \leq 2n \end{cases}$$

These formulas correctly map each position j in the original deck to its new position in the shuffled deck.

$\square$