# MATH403: Homework 2

James Zhang*

September 10, 2024

**12.** Suppose that an element $X$ of a dihedral group is the product of $m$ rotations and $n$ reflections. Complete the following statement: $X$ is a rotation if and only if ________________.

$X$ is a rotation if and only if $n$ **is even**

*Solution.* Observe the Cayley table for $D_4$ from the textbook as reference, but we will generalize for all dihedral groups.

| | $R_0$ | $R_{90}$ | $R_{180}$ | $R_{270}$ | $H$ | $V$ | $D$ | $D'$ |
|---|---|---|---|---|---|---|---|---|
| $R_0$ | $R_0$ | $R_{90}$ | $R_{180}$ | $R_{270}$ | $H$ | $V$ | $D$ | $D'$ |
| $R_{90}$ | $R_{90}$ | $R_{180}$ | $R_{270}$ | $R_0$ | $D'$ | $D$ | $H$ | $V$ |
| $R_{180}$ | $R_{180}$ | $R_{270}$ | $R_0$ | $R_{90}$ | $V$ | $H$ | $D'$ | $D$ |
| $R_{270}$ | $R_{270}$ | $R_0$ | $R_{90}$ | $R_{180}$ | $D$ | $D'$ | $V$ | $H$ |
| $H$ | $H$ | $D$ | $V$ | $D'$ | $R_0$ | $R_{180}$ | $R_{90}$ | $R_{270}$ |
| $V$ | $V$ | $D'$ | $H$ | $D$ | $R_{180}$ | $R_0$ | $R_{270}$ | $R_{90}$ |
| $D$ | $D$ | $V$ | $D'$ | $H$ | $R_{270}$ | $R_{90}$ | $R_0$ | $R_{180}$ |
| $D'$ | $D'$ | $H$ | $D$ | $V$ | $R_{90}$ | $R_{270}$ | $R_{180}$ | $R_0$ |

Let's first consider the value $m$, the number of rotations. Trivially, 1 rotation is a rotation. From the table, we see that 2 rotations is still a rotation, and this holds for all dihedral groups, so if $n = 0$, then $X$ is a rotation for all $m$. Now let's consider nonzero $n$. If $n$ is odd, either a singular reflection or a sequence of reflections and rotations, then $X$ will be a reflection. However, an even number of reflections results in a rotation. Therefore, $X$ is a rotation if and only if $n$ is even. ☐

*Email: jzhang72@terpmail.umd.edu

**18.** Consider an infinitely long strip of equally spaced H's:

$$\cdots \text{H H H H} \cdots$$

Describe the symmetries of this strip. Is the group of symmetries of the strip Abelian?

*Proof.* Recall that a group is Abelian (or commutative) if $ab = ba$ for all choices of group elements $a, b$. Let us enumerate the infinite strip of $H$'s for the sake of determining if the strip is Abelian.

$$\cdots \quad H_{-2} \quad H_{-1} \quad H_0 \quad H_1 \quad H_2 \quad \cdots \tag{1}$$

Visually, ignoring the enumerations, if you translate the strip left or right $n$ units or even reflect the strip horizontally, the strip will still appear the same, but let's take a closer look with the aid of our enumerations. Let us define two transformations: $T(n)$, which is a translation $n$ units such that positive is to the right and negative is to the left (analagous to a real number line), and $R$, a horizontal reflection. We will show that $T(1)\ R$ and $R\ T(1)$ do not result in the same final state, and thus the strip is not Abelian.

Case 1: $T(1)\ R$. The reflection $R$ turns (1) into

$$\cdots \quad H_2 \quad H_1 \quad H_0 \quad H_{-1} \quad H_{-2} \quad \cdots$$

and then the translation turns this into

$$\cdots \quad H_3 \quad H_2 \quad H_1 \quad H_0 \quad H_{-1} \quad \cdots \tag{2}$$

Case 2: $R\ T(1)$. The translation turns (1) into

$$\cdots \quad H_{-3} \quad H_{-2} \quad H_{-1} \quad H_0 \quad H_1 \quad \cdots$$

and then the reflection would result in

$$\cdots \quad H_1 \quad H_0 \quad H_{-1} \quad H_{-2} \quad H_{-3} \quad \cdots \tag{3}$$

and clearly, (2) and (3) are not the same final state, and so the strip is not Abelian. □

**24.** If $F$ is a reflection in the dihedral group $D_n$ find all elements $X$ in $D_n$ such that $X^2 = F$ and all elements $X$ in $D_n$ such that $X^3 = F$.

*Proof.* For the following, let $F$ be a *reflection* in $D_n$.

(i) First, let us find all elements $X$ in $D_n$ such that $X^2 = F$. Note that any rotation followed by the same rotation results a new rotation, so there are no rotations in the set $X$. Furthermore, given any reflection, applying that same reflection twice over results in $R_0$, which cannot be the reflection $F$. Therefore, $X = \emptyset$, the empty set.

(ii) For all elements $X$ in $D_n$ such that $X^3 = F$, we apply similar logic. Any rotation applied three times successively will result in an new rotation, so there are no rotations in $X$. Now onto reflections. Equipped with the fact that applying the same reflection twice back to back results in $R_0$, applying the same reflection the third time would be equivalent to have only applying the reflection once. Therefore, for any given $F$, $X$ only contains one element: $F$. $X = \{F\}$.

□

**6.** In each case, perform the indicated operation.

**a.** In **C***, $(7 + 5i)(-3 + 2i)$

**b.** In $GL(2, Z_{13})$, det$\begin{bmatrix} 7 & 4 \\ 1 & 5 \end{bmatrix}$

**c.** In $GL(2, \mathbf{R})$, $\begin{bmatrix} 6 & 3 \\ 8 & 2 \end{bmatrix}^{-1}$

**d.** In $GL(2, Z_7)$, $\begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix}^{-1}$

*Proof.*

a. $(7 + 5i)(-3 + 2i) = -21 + 14i - 15i + 10i^2 = -31 - i$

b. $35 - 4 = 31$ but we need this in $Z_{13}$ so $31 \bmod 13 = 5$ and so the determinant in $GL(2, Z_{13})$ is 5.

c. Using the formula for inverse of a $2 \times 2$ matrix,

$$\begin{bmatrix} 6 & 3 \\ 8 & 2 \end{bmatrix}^{-1} = \begin{bmatrix} -\frac{1}{6} & \frac{1}{4} \\ \frac{2}{3} & -\frac{1}{2} \end{bmatrix}$$

whcih is already in $GL(2, \mathbb{R})$ and so we are done.

d. We have to be more careful with this example. Recall that the inverse of a $2 \times 2$ matrix $M$ is given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{\det M} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

The determinant of our matrix is $2(3) - 1(1) = 5$. The modular mutliplicative inverse of $t$ in $Z_7$ is 3. Therefore, we now compute

$$3 \begin{bmatrix} 3 & -1 \\ -1 & 2 \end{bmatrix} = \begin{bmatrix} 9 & -3 \\ -3 & 6 \end{bmatrix} \implies \begin{bmatrix} 2 & 4 \\ 4 & 6 \end{bmatrix} \in Z_7$$

and we are done.

$\square$

**10.** List the elements of $U(20)$ and find the inverse of each one.

*Proof.* Recall that $U(n)$ is the set of all positive integers less than $n$ and relatively prime to $n$. Thus, $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$. For inverses, note that

- $1 * 1 \equiv 1 (\text{mod } 20)$, so 1 is its own inverse
- $3 * 7 \equiv 21 \equiv 1 (\text{mod} 20)$, so 3 and 7 are inverses of each other
- $9 * 9 \equiv 81 \equiv 1 (\text{mod } 20)$, so 9 is its own inverse
- $11 * 11 \equiv 121 \equiv 1 (\text{mod } 20)$, so 11 is its own inverse
- $13 * 17 \equiv 221 \equiv 1 (\text{mod } 20)$, so 13 and 17 are inverses of each other
- $19 * 19 \equiv 361 \equiv 1 (\text{mod } 20)$, so 19 is its own inverse.

$\square$

**36.** Prove that in a group, $(ab)^2 = a^2b^2$ if and only if $ab = ba$.
Prove that in a group, $(ab)^{-2} = b^{-2}a^{-2}$ if and only if $ab = ba$.

*Proof.*

(i) First let us prove that $(ab)^2 = a^2b^2$ if and only if $ab = ba$.

$\Longrightarrow$ Assume $(ab)^2 = a^2b^2$. We want to show that $ab = ba$. Taking our given statement and expanding, we obtain

$$(ab)(ab) = aabb$$

Now by associativity of groups,

$$a(ba)b = a(ab)b$$

By the inverses of groups, we apply

$$a^{-1}a(ba)bb^{-1} = a^{-1}a(ab)bb^{-1} \implies e(ba)e = e(ab)a \implies ba = ab$$

Therefore, any group with this property must be Abelian.

$\Longleftarrow$ Now assume the group is Abelian, so $ab = ba$. We want to show that $(ab)^2 = a^2b^2$.

$$ba = ab \implies aba = aab \implies abab = aabb$$

By associativity of groups,

$$abab = aabb \implies (ab)(ab) = (aa)(bb) \implies (ab)^2 = a^2b^2$$

(ii) Now let us prove that $(ab)^{-2} = b^{-2}a^{-2}$ if and only if $ab = ba$.

$\Longrightarrow$ Assume that $(ab)^{-2} = b^{-2}a^{-2}$. We want to show that $ab = ba$. Multiply both sides by $(ab)^2$ on the left

$$(ab)^2(ab)^{-2} = (ab)^2b^{-2}a^{-2} \implies e = (ab)^2b^{-2}a^{-2}$$

Multiply both sides by $a^2$ on the right to get

$$a^2 = (ab)^2b^{-2}a^{-2}a^2 \implies a^2 = (ab)^2b^{-2}e \implies a^2 = (ab)^2b^{-2}$$

Multiply both sides on the right by $b^2$ and this yields

$$a^2b^2 = (ab)^2e \implies a^2b^2 = (ab)^2$$

From here, we apply the same proof in part $i$, and we have shown that $ab = ba$.

$\Longleftarrow$ Assume $ab = ba$, we want to show that $(ab)^{-2} = b^{-2}a^{-2}$. Furthermore, note the property $(ab)^{-1} = b^{-1}a^{-1}$ and we can quickly show this because $(ab)b^{-1}a^{-1} = a(bb^{-1})a^{-1} = e$. Now observe that

$$(ab)^{-2} = ((ab^{-1}))^2 = (b^{-1}a^{-1})^2 = (b^{-1}a^{-1})(b^{-1}a^{-1})$$

Since we have commutativivity, we can rearrange such that

$$(ab)^{-2} = (b^{-1}b^{-1})(a^{-1}a^{-1}) = b^{-2}a^{-2}$$

and so $(ab)^{-2} = b^{-2}a^{-2}$ as desired.

$\square$