Chris Hayduk
Math B4900
Homework 1 Reflection
9/21/2020

## 1. Questions

1.

2.

## 2. Marked-up Homework

1. Recall that $\mathbb{Z}/n\mathbb{Z} = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z}\}$ is the set of congruence classes modulo $n$. Define $(\mathbb{Z}/n\mathbb{Z})^\times$ to be the subset of $\mathbb{Z}/n\mathbb{Z}$ that have multiplicative inverses, i.e.

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{ there is some } \bar{c} \in \mathbb{Z}/n\mathbb{Z} \text{ such that } \bar{c}\bar{a} = 1 \}.$$

(a) Compute $(\mathbb{Z}/n\mathbb{Z})^\times$ for $n = 1, 2, 3, 4, 5,$ and $6$.

*Answer*. **Case 1** $(\mathbb{Z}/1\mathbb{Z})$: note that every integer is divisible by 1. This is true because, for any integer $x \in \mathbb{Z}$, we have that $x = 1 \cdot x$. Hence, every integer belongs to $\overline{0}$ when $n = 1$.

By the definition of modular multiplication on p. 9 of the text, if we have $\overline{a}, \overline{b} \in (\mathbb{Z}/1\mathbb{Z})$, we can take $\overline{a} \cdot \overline{b} = \overline{ab}$.

Since we just showed that every integer in $(\mathbb{Z}/1\mathbb{Z})$ belongs to the congruence class $\overline{0}$, we have $\overline{0} \cdot \overline{0} = \overline{0 \cdot 0} = \overline{0} \; \forall \; z \in \mathbb{Z}$.

Hence, there are no elements $\overline{a} \in \mathbb{Z}/1\mathbb{Z}$ such that $\exists \overline{c} \in \mathbb{Z}/1\mathbb{Z}$ with the property that $\overline{ca} = 1$.

Thus, $(\mathbb{Z}/n\mathbb{Z})^\times = \varnothing$

**Case 2** $(\mathbb{Z}/2\mathbb{Z})$: note that there are two congruence classes, $\overline{0}$ and $\overline{1}$.

We have $\overline{0} \cdot \overline{0} = \overline{0} \cdot \overline{1} = \overline{1} \cdot \overline{0} = \overline{0}$.

However, we have $\overline{1} \cdot \overline{1} = \overline{1}$. Hence, for $\overline{1} \in (\mathbb{Z}/2\mathbb{Z})$, $\exists \overline{c} \in (\mathbb{Z}/2\mathbb{Z})$ such that $\overline{c} \cdot \overline{1} = \overline{1}$. In this case, $\overline{c} = \overline{1}$.

Hence, $(\mathbb{Z}/2\mathbb{Z})^\times = \{\overline{1}\}$

**Case 3** $(\mathbb{Z}/3\mathbb{Z})$: note that there are three congruence classes, $\overline{0}$, $\overline{1}$, $\overline{2}$.

We know that $\overline{0} \cdot \overline{c} = \overline{0} \; \forall \; \overline{c} \in (\mathbb{Z}/3\mathbb{Z})$, so we don't need to consider it.

For the other two congruence classes, we have $\overline{1} \cdot \overline{1} = \overline{1}$, $\overline{1} \cdot \overline{2} = \overline{2} = \overline{2} \cdot \overline{1}$, and $\overline{2} \cdot \overline{2} = \overline{4} = \overline{1}$.

So we have that $(\mathbb{Z}/3\mathbb{Z})^\times = \{\overline{1}, \overline{2}\}$

**Case 4** $(\mathbb{Z}/4\mathbb{Z})$: note that there are four congruence classes, $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$.

From here I will assume the commutativity of multiplication of congruence classes and as such will only show one direction.

Once again, we do not need to consider $\overline{0}$ since multiplying it by any other congruence class yields $\overline{0}$.

We have,

$$\begin{aligned}
\overline{1} \cdot \overline{1} &= \overline{1} \\
\overline{1} \cdot \overline{2} &= \overline{2} \\
\overline{2} \cdot \overline{2} &= \overline{4} = \overline{0} \\
\overline{1} \cdot \overline{3} &= \overline{3} \\
\overline{2} \cdot \overline{3} &= \overline{6} = \overline{2} \\
\overline{3} \cdot \overline{3} &= \overline{9} = \overline{1}
\end{aligned}$$

So we have that $(\mathbb{Z}/4\mathbb{Z})^\times = \{\overline{1}, \overline{3}\}$

**Case 5** $(\mathbb{Z}/5\mathbb{Z})$: note that there are five congruence classes, $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$.

We have,

$$\begin{aligned}
\overline{1} \cdot \overline{1} &= \overline{1} \\
\overline{1} \cdot \overline{2} &= \overline{2} \\
\overline{1} \cdot \overline{3} &= \overline{3} \\
\overline{1} \cdot \overline{4} &= \overline{4} \\
\overline{2} \cdot \overline{2} &= \overline{4} \\
\overline{2} \cdot \overline{3} &= \overline{6} = \overline{1} \\
\overline{2} \cdot \overline{4} &= \overline{8} = \overline{3} \\
\overline{3} \cdot \overline{3} &= \overline{9} = \overline{4} \\
\overline{3} \cdot \overline{4} &= \overline{12} = \overline{2} \\
\overline{4} \cdot \overline{4} &= \overline{16} = \overline{1}
\end{aligned}$$

So we have that $(\mathbb{Z}/5\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

**Case 6** ($\mathbb{Z}/6\mathbb{Z}$): note that there are six congruence classes, $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$.

We have,

$$\begin{aligned}
\overline{1}\cdot\overline{1} &= \overline{1}\\
\overline{1}\cdot\overline{2} &= \overline{2}\\
\overline{1}\cdot\overline{3} &= \overline{3}\\
\overline{1}\cdot\overline{4} &= \overline{4}\\
\overline{1}\cdot\overline{5} &= \overline{5}\\
\overline{2}\cdot\overline{2} &= \overline{4}\\
\overline{2}\cdot\overline{3} &= \overline{6} = \overline{0}\\
\overline{2}\cdot\overline{4} &= \overline{8} = \overline{2}\\
\overline{2}\cdot\overline{5} &= \overline{10} = \overline{4}\\
\overline{3}\cdot\overline{3} &= \overline{9} = \overline{3}\\
\overline{3}\cdot\overline{4} &= \overline{12} = \overline{0}\\
\overline{3}\cdot\overline{5} &= \overline{15} = \overline{3}\\
\overline{4}\cdot\overline{4} &= \overline{16} = \overline{4}\\
\overline{4}\cdot\overline{5} &= \overline{20} = \overline{2}
\end{aligned}$$

So we have that $(\mathbb{Z}/6\mathbb{Z})^\times = \{\overline{1}\}$

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

(b) Prove that if $\bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\bar{a}\cdot\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

*Proof.* Suppose $\bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then $\exists \overline{c_1}, \overline{c_2} \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that

$$\begin{aligned}
\bar{a}\cdot\overline{c_1} &= \bar{1}\\
\bar{b}\cdot\overline{c_2} &= \bar{1}
\end{aligned}$$

Thus we have that,

$$\begin{aligned}
\overline{ab}\cdot\overline{c_1c_2} &= \overline{(a\cdot b)\cdot(c_1\cdot c_2)} \qquad (1)\\
&= \overline{a\cdot c_1\cdot b\cdot c_2}\\
&= (\bar{a}\cdot\overline{c_1})\cdot(\bar{b}\cdot\overline{c_2})\\
&= \bar{1}\cdot\bar{1}\\
&= \bar{1}
\end{aligned}$$

The first three equalities come from the properties of modular multiplication described on p. 9 in the text.

Since multiplication in $(\mathbb{Z}/n\mathbb{Z})^\times$ is well-defined and both $\overline{c_1}, \overline{c_2} \in (\mathbb{Z}/n\mathbb{Z})^\times$, we have that $\overline{c_3} = \overline{c_1 c_2} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Similarly, $\overline{ab} \in (\mathbb{Z}/n\mathbb{Z})^\times$

Hence by (1) and the above statements, we have that $\bar{a} \cdot \bar{b} = \overline{ab} \in (\mathbb{Z}/n\mathbb{Z})^\times$. $\square$

(c) Let $a \in \mathbb{Z}$. Show that if $(a, n) \neq 1$, then there is some $1 \leqslant b \leqslant n-1$ for which $n \big| ab$. Conclude that if $(a, n) \neq 1$, there is some $1 \leqslant b \leqslant n-1$ for which $\bar{a} \cdot \bar{b} = \bar{0}$.

*Proof.* Let $a \in \mathbb{Z}$ and suppose $(a, n) \neq 1$. Since the gcd is a positive integer, we know that $(a, n) > 1$.

Hence, $\exists d \in \mathbb{Z}$ such that $d > 1$, $d|a$, and $d|n$.

Let $b = n/d$ and $c = a/d$. We know that $d|n$ and $d|a$, so $b, c \in \mathbb{Z}$.

Then we have,

$$\begin{aligned} ab &= a \cdot \frac{n}{d} \\ &= \frac{a}{d} \cdot n \\ &= cn \end{aligned} \tag{2}$$

Thus, we clearly have that $n|ab$.

We know that $d > 1$ and also that $n \geqslant 1$. Hence, it is clear that $b \geqslant 1$.

Now suppose that $b \geqslant n$. Since $d > 1$, it is clear that,

$$bd > n$$

However, we defined $b = n/d$. Hence, the above statement is a contradiction and thus $b < n$.

We already established that $b \geqslant 1$, so we have $1 \leqslant b < n$, or equivalently since $b, n \in \mathbb{Z}$, $1 \leqslant b \leqslant n-1$.

Now note that $\overline{0} = \{0 + kn | k \in \mathbb{Z}\}$. We have from (2) that $ab = cn$.

Since $c \in \mathbb{Z}$, $cn$ satisfies the condition defined for the set $\bar{0}$ and so $cn = ab \in \bar{0}$.

Hence, we have

$$\overline{ab} = \bar{0} = \bar{a} \cdot \bar{b}$$

$\square$

(d) Let $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. Show that if there is some non-zero $\bar{b} \in \mathbb{Z}/n\mathbb{Z}$ such that $\bar{a} \cdot \bar{b} = \bar{0}$, then $\bar{a} \notin (\mathbb{Z}/n\mathbb{Z})^\times$.

*Proof.* Let $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ and suppose there is some non-zero $\bar{b} \in \mathbb{Z}/n\mathbb{Z}$ such that $\bar{a} \cdot \bar{b} = \bar{0}$.

We have that,

$$\bar{a} \cdot \bar{b} = \bar{0} \implies ab = 0 + kn$$

for some $k \in \mathbb{Z}$

Now assume $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Then there exists $\bar{c} \in \mathbb{Z}/n\mathbb{Z}$ such that $\bar{a} \cdot \bar{c} = \bar{1}$. That is,

$$ac = 1 + mn$$

for some $m \in \mathbb{Z}$. □

(e) Prove that if $a$ and $n$ are relatively prime then there is an integer $c$ such that $ac \equiv_n 1$. [Hint: use the fact that the g.c.d. of two integers is a $\mathbb{Z}$-linear combination of the integers]

(f) Conclude from the previous exercises that $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of elements $\bar{a}$ of $\mathbb{Z}/n\mathbb{Z}$ with $(a, n) = 1$ and hence prove Proposition 0.3.4. Verify this directly in the case $n = 6$.

2. Determine (prove positive, or give a reason why not) which of the following sets are groups under addition:

(a) the set of polynomials $\mathbb{Z}[x]$;

*Answer.* Yes, this is a group. Firstly, we have the identity element 0. For any polynomial $p \in \mathbb{Z}[x]$, we have that $p + 0 = p = 0 + p$.

Now for the additive inverse of $p$, we must take $-p$. That is, for

$$p = p_0 + p_1X + p_2X^2 + \cdots + p_{m-1}X^{m-1} + p_mX^m$$

with $p_k \in \mathbb{Z}$, we will take $-p$ to be:

$$\begin{aligned} -p &= -(p_0 + p_1X + p_2X^2 + \cdots + p_{m-1}X^{m-1} + p_mX^m) \\ &= -p_0 - p_1X - p_2X^2 - \cdots - p_{m-1}X^{m-1} - p_mX^m \end{aligned}$$

Note that if we take $p + (-p)$, we get,

$$\begin{aligned} p + (-p) &= p_0 + p_1X + p_2X^2 + \cdots + p_{m-1}X^{m-1} + p_mX^m + (-p_0 - p_1X - p_2X^2 - \cdots - p_{m-1}X^{m-1} - p_mX^m) \\ &= (p_0 - p_0) + (p_1X - p_1X) + (p_2X^2 - p_2X^2) + \cdots + (p_{m-1}X^{m-1} - p_{m-1}X^{m-1}) + (p_mX^m - p_mX^m) \\ &= 0 + 0 + 0 + \cdots + 0 + 0 \\ &= 0 \end{aligned}$$

The same is true for $(-p) + p$.

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

(b) the set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are even;

*Answer.* Yes, this is a group. Firstly, we have the identity element $0 = \frac{0}{2}$. For any rational number $q$ in the described set, we have that

$$q + \frac{0}{2} = q + 0 = q$$
$$\frac{0}{2} + q = 0 + q = q$$

Now let $q$ in this set. Then $\exists n, m \in \mathbb{Z}$ such that $q = n/m$. Note that $m$ is even and $n$ is odd, since if $n$ were even this fraction would not be in lowest terms.

Now consider the fraction $-q = -n/m$. Observe that, since $n$ is odd, we can take $n = 2k+1$ for some $k \in \mathbb{Z}$. When we take $-n$, we have $-n = -2k - 1$. Since $-2k$ is even, we have that $-n$ is still odd. Hence, even if we needed to reduce $-q$ to lowest terms, it would still be in the described set since $m$ would still be even.

Now that we have established that $-q$ is in our set, we can show that $q + -q = 0$.

Observe that

$$\begin{aligned} q + -q &= \frac{n}{m} + \frac{-n}{m} \\ &= \frac{n + -n}{m} \\ &= \frac{0}{m} = 0 \end{aligned}$$

The same is true for $-q + q$.

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

(c) the set of rational numbers of absolute value $< 1$;

*Answer.* Yes, this is a group.

We have that $0 \in \mathbb{Q}$ and $|0| < 1$, so 0 is in our set. For any $q \in \mathbb{Q}$ with $|q| < 1$, we have that

$$0 + q = 0 = q + 0$$

So 0 is the identity element.

Now observe that if $q \in \mathbb{Q}$, then $-q \in \mathbb{Q}$. In addition, note that if $|q| < 1$, then we have that $|-q| = |-1| \cdot |q| = |q| < 1$. Hence, $-q$ is in our set as well. Thus, we have that,

$$q + (-q) = 0 = (-q) + q$$

Hence, every element in our set has an additive inverse within the set, as required.

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

3. Let $x, y \in G$. Prove that $xy = yx$ if and only if $y^{-1}xy = x$ if and only if $x^{-1}y^{-1}xy = 1$.

*Proof.* Suppose that $x = yx$. Then we have that,

$$\begin{aligned} & xy = yx \\ \implies & y^{-1}(xy) = y^{-1}(yx) \\ \implies & y^{-1}xy = (y^{-1}y)x \\ \implies & y^{-1}xy = x \end{aligned}$$

Now suppose that $y^{-1}xy = x$. Then we have that,

$$\begin{aligned} & y^{-1}xy = x \\ \implies & y(y^{-1}xy) = yx \\ \implies & (yy^{-1})xy = yx \\ \implies & xy = yx \end{aligned}$$

In addition, we have that

$$\begin{aligned} & y^{-1}xy = x \\ \implies & x^{-1}(y^{-1}xy) = x^{-1}x \\ \implies & x^{-1}y^{-1}xy = 1 \end{aligned}$$

Now suppose that $x^{-1}y^{-1}xy = 1$. Then we have that

$$\begin{aligned} & x^{-1}y^{-1}xy = 1 \\ \implies & x(x^{-1}y^{-1}xy) = x \cdot 1 \\ \implies & (xx^{-1})y^{-1}xy = x \\ \implies & y^{-1}xy = x \end{aligned}$$

Hence we have that $xy = yx \iff y^{-1}xy = x \iff x^{-1}y^{-1}xy = 1$ □

4. Let $G$ be a group and let $x \in G$.

   (a) If $g \in G$, show $|g^{-1}xg| = |x|$.

   *Proof.* We know that $|x| \in \mathbb{Z}$ and $|x| \geqslant 1$. Suppose $|x| = 1$. Then $x = e$. Hence we have that,

$$\begin{aligned} |g^{-1}xg| &= |g^{-1}eg| \\ &= |g^{-1}g| \\ &= |e| = 1 \end{aligned}$$

   So we have $|g^{-1}xg| = |x|$ in this case.

Now suppose $|x| = n > 1$. Then we can show that,

$$\begin{aligned}(g^{-1}xg)^n &= g^{-1}xg \cdot g^{-1}xg \cdots g^{-1}xg \cdot g^{-1}xg \\ &= g^{-1}x(gg^{-1})x(gg^{-1}) \cdots (gg^{-1})x(gg^{-1})xg \\ &= g^{-1}x \cdot x \cdots x \cdot x \cdot g \\ &= g^{-1}x^n g \\ &= g^{-1}eg \\ &= g^{-1}g = e\end{aligned}$$

So $(g^{-1}xg)^n = e$.

Now suppose we select an $m$ such that $1 \leqslant m < n$. Then we have that,

$$(g^{-1}xg)^m = g^{-1}x^m g$$

Since $|x| = n$ and $1 \leqslant m < n$, we have that $x^m \neq e$, and thus $(g^{-1}xg)^m \neq e$.

Hence, $n$ is the least positive integer $k$ such that $(g^{-1}xg)^k = e$ and we have that $|g^{-1}xg| = n$

□

(b) Prove that if $|x| \leqslant 2$ for all $x \in G$ then $G$ is abelian.

*Proof.* Suppose that $|x| \leqslant 2$ for all $x \in G$. Now let $x, y \in G$.

Note that, since the order of an element is a positive integer, the only two possibilities for $|x|$ are $1, 2$.

If $|x| = 1$, then $x = e$ and we have,

$$xy = ey = y = ye = yx$$

for any $y \in G$.

Now suppose $|x| = 2$. If $|y| = 1$, $y$ is the identity and is commutative (as shown above), so we will assume $|y| = 2$ as well.

Since $x^2 = xx = e$ and $y^2 = yy = e$, we have that $x = x^{-1}$ and $y = y^{-1}$. If $|xy| = 1$ or $|xy| = 2$, then $xy = (xy)^{-1}$ and

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$

as required

□

(c) If $|x| = n < \infty$, prove that the elements $e, x, x^2, \ldots, x^{n-1}$ are all distinct. Deduce that $|x| \leqslant |G|$.

*Proof.* Let $|x| = n < \infty$. Now suppose that there are numbers $m, k \in \mathbb{Z}$ with $0 \leqslant m, k \leqslant n-1$ and $k < m$ such that $x^m = x^k$.

Then we clearly have that,

$$\begin{aligned} x^k \cdot x &= x^m \cdot x \\ x^k \cdot x^2 &= x^m \cdot x^2 \\ x^k \cdot x^3 &= x^m \cdot x^3 \\ &\vdots \\ x^k \cdot x^{n-m} &= x^m \cdot x^{n-m} \end{aligned}$$

However, on the right side of the equality, we have

$$\begin{aligned} x^m \cdot x^{n-m} &= x^{m+n-m} \\ &= x^n \\ &= e \end{aligned}$$

This implies that,

$$\begin{aligned} x^k \cdot x^{n-m} &= x^{k+n-m} \\ &= e \end{aligned}$$

where $k + n - m \in \mathbb{Z}$ and $0 < k + n - m < m + n - m = n$.

However, we know that the order of $x$ is $n$, which is defined to be the smallest positive integer of $x$ that yields the identity element. Hence, $e, x, x^2, \ldots, x^{n-1}$ are all distinct.

Suppose $x \in G$ where $G$ is a group. Then, $\{e, x, x^2, \ldots, x^{n-1}\} \subset G$. Thus $|x| = n$ and there are at least $n$ elements in $G$. Hence, we have that $|x| \leqslant |G|$. □

5. **The dihedral group.** The dihedral group $D_{2n}$ has the usual presentation

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle.$$

(a) Compute the order of each of the elements in $D_8$.

*Answer.* Suppose $|r| = k < 4$. Then, since $r^4 = 1$, we must have that $4 = mk$ for some $m \in \mathbb{Z}^+$.

Since $k > 1$ and $k$ must be a factor of 4, we also have that $k = 2$.

However, if $|r| = 2$, then $r = r^{-1}$. Thus, the second relation becomes

$$rs = sr$$

This implies one of two cases: either $r = s^{-1}$ or $r = 1$. We know that $r \neq 1$ by the geometric properties of rotation of a square, so we can ignore this case.

Thus, we will only consider the case where $r = s^{-1}$. Note that $s^{-1} = s$ since $s^2 = 1$, so we have that $r = s$. However, by the geometric properties of clockwise rotation (which $r$ represents) and reflection over the line $y = x$ (which $s$ represents) of the square, we know that $r \neq s$.

Hence, $|r|$ cannot be less than 4. Since we know that $r^4 = 1$ from the list of generators, we have that $|r| = 4$.

From the list of generators we also have that $s^2 = 1$. If $s^1 = 1$, then we have that $s = 1$. However, by the properties of reflection over the line $y = x$ of the square, we know that $s \neq 1$.

Thus, $|s| = 2$.

Now take $rs$. We have that

$$\begin{aligned}(rs)^2 &= rsrs \\ &= rssr^{-1} \\ &= rs^2r{-}1 \\ &= rr^{-1} \\ &= 1\end{aligned}$$

Hence $|rs| = 2$

Similarly, for $sr^{-1}$, we have

$$\begin{aligned}(sr^{-1})^2 &= sr^{-1}sr^{-1} \\ &= rssr^{-1} \\ &= rs^2r^{-1} \\ &= rr^{-1} \\ &= 1\end{aligned}$$

so $|sr^{-1}| = 2$ as well.

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

(b) Use the generators and relations above to show that if $x$ is any element of $D_{2n}$ which is not a power of $r$, then

$$rx = xr^{-1} \qquad \text{and} \qquad |x| = 2.$$

*Proof.* Suppose $x \in D_{2n}$ and $x \neq r^k$ for any $k \in \mathbb{Z}^+$.

Hence $x$ must be some product of $r$ and $s$.

Note that, since $s^2 = 1$, we have that $s^{2m+1} = s^2m \cdot s^1 = s$ for any $m \in \mathbb{Z}^+$. So the $s$ term in $x$ must be $s^1$.

Thus, we have

$$x = sr^k \tag{3}$$

or

$$x = r^k s \tag{4}$$

So for the case of (3) we get,

$$\begin{aligned} rx &= r(sr^k) \\ &= (rs)r^k \\ &= (sr^{-1})r^k \\ &= sr^{k-1} \\ &= sr^k(r^{-1}) \\ &= xr^{-1} \end{aligned}$$

and for (4) we get

$$\begin{aligned} rx &= r(r^k s) \\ &= r^k(rs) \\ &= r^k(sr^{-1}) \\ &= (r^k s)r^{-1} \\ &= xr^{-1} \end{aligned}$$

as required.

Now we will compute the order of (3):

$$\begin{aligned} x^2 &= sr^k sr^k \\ &= sr^k r^{-k} s \\ &= s(r^k r^{-k})s \\ &= ss \\ &= 1 \end{aligned}$$

and of (4):

$$\begin{aligned} x^2 &= r^k sr^k s \\ &= r^k r^{-k} ss \\ &= (r^k r^{-k})(ss) \\ &= 1 \end{aligned}$$

So in either case, $|x| = 2$.

Note that the second line of both of the above equations was derived by repeatedly applying the relation $sr = r^{-1}s$ $\square$

(c) Show that if $s_1 = s$ and $s_2 = sr$, then those together with the relations

$$s_1^2 = s_2^2 = (s_1 s_2)^n = 1$$

forms and alternative presentation of $D_{2n}$ (you have to show that $S = \{s_1, s_2\}$ generates the whole group and that you can derive these relations from the old ones and vice versa).

*Proof.* By the relations given above we have that,

$$s_1^2 = 1 = s^2$$

Moreover, we have that

$$s_2^2 = 1 = srsr$$

This implies that $sr = (sr)^{-1} = r^{-1}s^{-1}$.

However, we know that $s^{-1} = s$ since $s^2 = 1$, so we have

$$\begin{aligned} sr = (sr)^{-1} &= r^{-1}s^{-1} \\ &= r^{-1}s \end{aligned}$$

We are also given that $(s_1 s_2)^n = 1$. That is,

$$\begin{aligned} (s_1 s_2)^n &= (ssr)^n \\ &= r^n \\ &= 1 \end{aligned}$$

Hence, the elements $s_1$ and $s_2$ together with the relations shown above fully describe the initial presentation of $D_{2n}$. □

6. **The symmetric group.**

(a) Let

$$\alpha = (1\ 2\ 3\ 4\ 5\ 6\ 7), \quad \beta = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12), \quad \text{and} \quad \gamma = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8).$$

(i) Compute $\alpha^2$, $\beta^2$, and $\gamma^2$.

*Answer.* We have,

$$\begin{aligned} \alpha^2 &= (1\ 2\ 3\ 4\ 5\ 6\ 7) \circ (1\ 2\ 3\ 4\ 5\ 6\ 7) \\ &= (1\ 3\ 5\ 7\ 2\ 4\ 6) \end{aligned}$$

and,

$$\begin{aligned} \beta^2 &= (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12) \circ (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12) \\ &= (1\ 3\ 5\ 7\ 9\ 11)(2\ 4\ 6\ 8\ 10\ 12) \end{aligned}$$

finally,

$$\begin{aligned} \gamma^2 &= (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8) \circ (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8) \\ &= (1\ 3\ 5\ 7)(2\ 4\ 6\ 8) \end{aligned}$$

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

(ii) For which $i$ between 1 and 7 is $\alpha^i$ still a 7-cycle? …between 1 and 12 is $\beta^i$ still a 12-cycle? …between 1 and 8 is $\gamma^i$ still an 8-cycle?

*Answer*. For the case of $\alpha$:

We already have that $\alpha$ and $\alpha^2$ are 7-cycles. We will now check the other powers.

$$\begin{aligned}\alpha^3 &= \alpha \circ \alpha^2 \\ &= (1\ 2\ 3\ 4\ 5\ 6\ 7) \circ (1\ 3\ 5\ 7\ 2\ 4\ 6) \\ &= (1\ 4\ 7\ 3\ 6\ 2\ 5)\end{aligned}$$

$$\begin{aligned}\alpha^4 &= \alpha \circ \alpha^3 \\ &= (1\ 2\ 3\ 4\ 5\ 6\ 7) \circ (1\ 4\ 7\ 3\ 6\ 2\ 5) \\ &= (1\ 5\ 2\ 6\ 3\ 7\ 4)\end{aligned}$$

$$\begin{aligned}\alpha^5 &= \alpha \circ \alpha^4 \\ &= (1\ 2\ 3\ 4\ 5\ 6\ 7) \circ (1\ 5\ 2\ 6\ 3\ 7\ 4) \\ &= (1\ 6\ 4\ 2\ 7\ 5\ 3)\end{aligned}$$

$$\begin{aligned}\alpha^6 &= \alpha \circ \alpha^5 \\ &= (1\ 2\ 3\ 4\ 5\ 6\ 7) \circ (1\ 6\ 4\ 2\ 7\ 5\ 3) \\ &= (1\ 7\ 6\ 5\ 4\ 3\ 2)\end{aligned}$$

$$\begin{aligned}\alpha^7 &= \alpha \circ \alpha^6 \\ &= (1\ 2\ 3\ 4\ 5\ 6\ 7) \circ (1\ 7\ 6\ 5\ 4\ 3\ 2) \\ &= 1\end{aligned}$$

So we have that $\alpha^i$ is a 7-cycle if $i \in \{1, 2, 3, 4, 5, 6\}$.

Now for the case of $\gamma$:

We already have that $\gamma$ is an 8-cycle and $\gamma^2$ is not. We will now check the other powers.

$$\begin{aligned}\gamma^3 &= \gamma \circ \gamma^2 \\ &= (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8) \circ (1\ 3\ 5\ 7)(2\ 4\ 6\ 8) \\ &= (1\ 4\ 7\ 2\ 5\ 8\ 3\ 6)\end{aligned}$$

$$\begin{aligned}\gamma^4 &= \gamma \circ \gamma^3 \\ &= (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8) \circ (1\ 4\ 7\ 2\ 5\ 8\ 3\ 6) \\ &= (1\ 5)(4\ 8)(7\ 3)(2\ 6)\end{aligned}$$

$$\begin{aligned}\gamma^5 &= \gamma \circ \gamma^4 \\ &= (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8) \circ (1\ 5)(4\ 8)(7\ 3)(2\ 6) \\ &= (1\ 6\ 3\ 8\ 5\ 2\ 7\ 4)\end{aligned}$$

$$\begin{aligned}\gamma^6 &= \gamma \circ \gamma^5 \\ &= (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8) \circ (1\ 6\ 3\ 8\ 5\ 2\ 7\ 4) \\ &= (1\ 7\ 5\ 3)(2\ 8\ 6\ 4)\end{aligned}$$

$$\begin{aligned}\gamma^7 &= \gamma \circ \gamma^6 \\ &= (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8) \circ (1\ 7\ 5\ 3)(2\ 8\ 6\ 4) \\ &= (1\ 8\ 7\ 6\ 5\ 4\ 3\ 2\ 1)\end{aligned}$$

$$\begin{aligned}\gamma^8 &= \gamma \circ \gamma^7 \\ &= (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8) \circ (1\ 8\ 7\ 6\ 5\ 4\ 3\ 2\ 1) \\ &= 1\end{aligned}$$

So we have that $\gamma^i$ is an 8-cycle if $i \in \{1, 3, 5, 7\}$.

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

(iii) What's the theorem in general?

*If $\sigma$ is an $m$-cycle, then $\sigma^i$ is also an $m$-cycle if and only if ...*

(Just state, don't prove it.)

*Answer.* If $\sigma$ is an m-cycle, then $\sigma^i$ is also an m-cycle if and only if $i \equiv r \mod m$ with $r$ and $m$ relatively prime.

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

(b) Prove that if $\sigma$ is the $m$-cycle $(a_1\ a_2\ \dots\ a_m)$, then for all $i = 1, \dots, m$,

$$\sigma^i(a_k) = a_{\overline{k+i}} \qquad \text{where } \overline{k+i} \text{ is the least residue mod } m.$$

Deduce that $|\sigma| = m$.

*Proof.* Fix $i, k \in \{1, \cdots, m\}$.

Now consider $\sigma^i(a_k)$. Then we have,

$$\sigma^i(a_k) = (\sigma \circ \sigma \circ \cdots \circ \sigma)(a_k)$$

Note that we have,

$$\begin{aligned} \sigma(a_k) &= a_{k+1} \\ \sigma^2(a_k) &= a_{k+2} \\ &\vdots \end{aligned}$$

If for some $j$ we have $k + j = m + 1$, then $a_{k+j} = a_1$

$\square$

(c) Use the last part to prove that the order of an element in $S_n$ equals the least common multiple of the lengths of the cycles in its cycle decomposition (*cycle decomposition* means writing it as the product of disjoint cycles; you may assume such a decomposition exists, and that disjoint cycles commute).
[You may use previous problems in your solution.]

*Proof.* $\square$

(d) Which values appear as orders of elements of $S_5$ (for which $i$ is there some element of $S_5$ that has order $i$)? For each value, give an example of an element that has that order.