Problem Set 2 solutions

Problem 1. (a) Show that every $\alpha \in S_n$ and every k-cycle $(i_1\ \ i_2\ \cdots\ i_k) \in S_n$ satisfy

$$\alpha\,(i_1\ \ i_2\ \cdots\ i_k)\,\alpha^{-1} = (\alpha(i_1)\quad \alpha(i_2)\quad \cdots\quad \alpha(i_k)).$$

Hint: when writing your solution, you might find it helpful to consider $\alpha^{-1}(j)$ for each $j \in [n]$.

Proof. First, consider the element $\alpha(i_t)$ for some $t \in \{1,\ldots,k\}$. We have

$$\begin{aligned}(\alpha(i_1\ \ i_2\ \cdots\ i_k)\alpha^{-1})(\alpha(i_t)) &= (\alpha(i_1\ \ i_2\ \cdots\ i_k))(\alpha^{-1}\alpha(i_t))\\ &= \alpha(i_1\ \ i_2\ \cdots\ i_k)(i_t)\\ &= \alpha(i_{t+1 \pmod k}).\end{aligned}$$

Now consider any element j such that $j \notin \{\alpha(i_1),\ldots,\alpha(i_k)\}$. Equivalently, this means that $\alpha^{-1}(j) \notin \{i_1,\ldots,i_k\}$. Then

$$(i_1\ \ i_2\ \cdots\ i_k)\,(\alpha^{-1}(j)) = \alpha^{-1}(j),$$

so

$$\left(\alpha\,(i_1\ \ i_2\ \cdots\ i_k)\,\alpha^{-1}\right)(j) = \alpha\alpha^{-1}(j) = j.$$

Thus the left hand side of our proposed equality sends $\alpha(i_t)$ to $\alpha(i_{t \pmod k})$ and fixes all other elements, and this is precisely what the cycle $(\alpha(i_1)\quad \alpha(i_2)\quad \cdots\quad \alpha(i_k))$ does. □

(b) Prove that the center of S_n is trivial.

Proof. We will use a special case of part (a):

$$\alpha\,(i\quad j) = (\alpha(i)\quad \alpha(j))\,\alpha$$

for any $\alpha \in S_n$ and any 2-cycle $(i\quad j)$. Assume that α is in the center of S_n. Then the above equation gives us

$$(i\quad j) = (\alpha(i)\quad \alpha(j))$$

and hence for all $i \neq j$ one of the following must hold:

- $\alpha(i) = i$ and $\alpha(j) = j$, or
- $\alpha(i) = j$ and $\alpha(j) = i$.

We will show that $\alpha(i) = i$ for all i. To do that, pick any i. If $\alpha(i) \neq i$, then by what we just proved, $\alpha(j) = i$ for all $j \neq i$. Since $n \geqslant 3$, we can find $1 \leqslant j, k \leqslant n$ so that i, j, k are all distinct, and hence $\alpha(j) = i = \alpha(k)$, which is not possible. We conclude that $\alpha(i) = i$, and α must be the identity. Thus the center of S_n is trivial. □

Problem 2. Find $\mathrm{Z}(D_n)$ for $n \geqslant 3$.
Hint: your answer will depend on whether n is even or odd.

To prove this, we will use the following lemma:

Lemma. *For all integers i,*

$$(*) \qquad sr^i = r^{-i}s.$$

Proof. We will prove this lemma by induction on i. We showed the case $i = 1$ in class: $sr = r^{-1}s$. Now suppose $sr^i = r^{-i}s$ for some $i \geqslant 1$. Then

$$\begin{aligned} sr^{i+1} &= (sr^i)r \\ &= (r^{-i}s)r && \text{by Induction Hypothesis} \\ &= r^{-i}(sr) \\ &= r^{-i}(r^{-1}s) && \text{by the case } i = 1 \\ &= r^{-(i+1)}s. && \square \end{aligned}$$

Proof. We claim that

$$\mathrm{Z}(D_n) = \begin{cases} \{e\} & \text{if } n \text{ is odd} \\ \{e, r^{n/2}\} & \text{if } n \text{ is even.} \end{cases}$$

We will use lemma $(*)$ above, and the fact that all the elements of D_{2n} can be written as r^i or $r^i s$ for some integer $0 \leqslant i < n$, and no two such expressions represent the same element of D_{2n}.

Suppose r^i is central. Then

$$\begin{aligned} r^{-i}s &= sr^i && \text{by } (*) \\ &= r^i s && \text{since } r^i \text{ is central.} \end{aligned}$$

Multiplying by the inverse of s gives us $r^{-i} = r^i$. But the equality $r^{-i} = r^i$ holds if and only if i and $-i$ are congruent modulo n. When n is odd, $i \equiv -i \pmod{n}$ can only occur if $i = 0$. When n is even, $i \equiv -i \pmod{n}$ can only happen when $i = 0$ or $i = \frac{n}{2}$. This gives us $r^{n/2} \in \mathrm{Z}(S_n)$ when n is even, and it shows that no other power of r besides the identity can be in the center.

Now suppose $r^i s$ is central. Then

$$\begin{aligned} r^i(rs) &= r(r^i s) && \text{by associativity} \\ &= (r^i s)rs && \text{since } r^i s \text{ is central.} \end{aligned}$$

By cancellation (meaning, by multiplying by the inverse of r^i on the left), we conclude that $rs = sr$. Since we also proved in class that $srs = r^{-1}$, then it would follow that $r^2 = e$, which does not hold since $n \geqslant 3$.

We have proven that $\mathrm{Z}(D_{2n})$ consists of at most e if n is odd and at most e and $r^{\frac{n}{2}}$ if n is even. The element e belongs the center of any group. It remains to check that $r^{\frac{n}{2}}$ commutes with every element of D_{2n} for n odd.

First, note that for $r^{\frac{n}{2}}$ commutes with any r^i since they are both powers of r. Moreover, using $(*)$ and the fact that $r^{-\frac{n}{2}} = r^{\frac{n}{2}}$, we conclude that

$$sr^{\frac{n}{2}} = r^{-\frac{n}{2}}s = r^{-\frac{n}{2}}s.$$

Since $r^{\frac{n}{2}}$ commutes with s and r^i, it also commutes with $r^i s$, and thus it commutes with all elements of D_n. $\square$

Problem 3. Prove or disprove: if x and y have finite order in a group G, then xy has finite order.

Solution. *(Many correct answers are possible) The given statement is false. We illustrate this with a counterexample.*

Consider the following two elements of $\mathrm{GL}_2(\mathbb{R})$, *both of order* 2*:*

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \textit{and} \qquad \begin{pmatrix} 0 & 2 \\ \frac{1}{2} & 0 \end{pmatrix}.$$

Note that

$$AB = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ \frac{1}{2} & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{pmatrix}.$$

and so

$$(AB)^n = \begin{pmatrix} 2^n & 0 \\ 0 & \frac{1}{2^n} \end{pmatrix}.$$

In particular, note that $(AB)^n \neq I$ *for all* $n \geqslant 1$, *and thus* $|AB| = \infty$, *while* A *and* B *both have finite order.*

Problem 4. Let G be a group. Consider the map $f \colon G \longrightarrow G$ given by $f(a) = a^{-1}$ for all $a \in G$. Show that f is an automorphism if and only if G is abelian.

Proof. Suppose G is abelian. Then for all $a, b \in G$ we have

$$\begin{aligned} f(ab) &= (ab)^{-1} && \text{by definition of } f \\ &= b^{-1}a^{-1} \\ &= a^{-1}b^{-1} && \text{since } G \text{ is abelian} \\ &= f(a)f(b) && \text{by definition of } f \end{aligned}$$

Therefore, f is a homomorphism. Now note that

$$(f \circ f)(a) = f(f(a)) = f(a^{-1}) = (a^{-1})^{-1} = a$$

for all $a \in G$. Hence, $f \circ f = \mathrm{id}_G$, and thus $f = f^{-1}$. In particular, f is bijective, and thus f is an automorphism of G.

Conversely, suppose f is an automorphism. Then for any $a, b \in G$ we have

$$\begin{aligned} ab &= (a^{-1})^{-1}(b^{-1})^{-1} && \text{since } (x^{-1})^{-1} = x \text{ for all } x \in G \\ &= f(a^{-1})f(b^{-1}) && \text{by definition of } f \\ &= f(a^{-1}b^{-1}) && \text{since } f \text{ is a homomorphism} \\ &= (a^{-1}b^{-1})^{-1} && \text{by definition of } f \\ &= (b^{-1})^{-1}(a^{-1})^{-1} && \text{since } (xy)^{-1} = y^{-1}x^{-1}. \\ &= ba. \end{aligned}$$

We conclude that G is abelian. □