Problem Set 2

Due Wednesday, September 10

Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand. You cannot use any resources besides me, your classmates, and our course notes.

I will post the .tex code for these problems for you to use if you wish to type your homework. If you prefer not to type, please *write neatly.* As a matter of good proof writing style, please use complete sentences and correct grammar. You may use any result stated or proven in class or in a homework problem, provided you reference it appropriately by either stating the result or stating its name (e.g. the definition of ring or Lagrange's Theorem). Please do not refer to theorems by their number in the course notes, as that can change.

Problem 1. Find $\mathbb{Z}(D_n)$ for $n \geqslant 3$.
Hint: your answer will depend on whether n is even or odd.

To prove this, we will use following Lemma stated in the notes.

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

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

□

We can now complete the proof.

Proof. We claim that

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

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

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

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 $r^{n/2} \in \mathbb{Z}(S_n)$ 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 $\mathbb{Z}(D_{2n})$ 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. □

Problem 2. List all of the orders of elements of S_5 and how many elements have each such order. Justify your answer.

Proof. Recall that the order of permutation with cycle type $l_1, \ldots, l_m$ (that is, theproduct of m disjoint cycles of lengths $l_1, \ldots, l_m$) is $lcm(l_1, \ldots, l_m)$. When $n = 5$, the possible cycles types are: the identity, a j cycle for $2 \leq j \leq 5$, the product of two disjoint 2 cycles, and the product of a 2 cycle and a disjiont 3 cycle.

- There is just one element of order 1 in any group, the identity.
- There are $\binom{5}{2} = 10$ two cycles and $\frac{1}{2}\binom{5}{2}\binom{3}{2} = 15$ permutations that are products of two disjoint 2 cycles, giving a total of 25 elements of order 2.
- There are $2 \cdot \binom{5}{3} = 20$ three cycles, and these are all the elements of order 3.
- There are $3! \cdot \binom{5}{4} = 30$ four cycles and these are all the elements of order 4.
- There are $4! = 24$ five cycles, and these are all the elements of order 5.
- There are $2\binom{5}{3} = 20$ products of a disjoint 2 cycle and a 3 cycle, and these give all the elements of order 6.

Note that $1 + 25 + 20 + 30 + 24 + 20 = 120$. □

Problem 3. Let G be a group.

(3.1) Show that if $g^n = e$ for some $n \geq 1$, then $|g|$ divides n.

Proof. First note that the fact that $g^n = e$ implies that g has finite order, so let $|g| = d$. By the Division Algorithm, we can find integers q, r with $0 \leqslant r < d$ such that $n = qd + r$. Moreover,

$$e = g^n = g^{qd+r} = (g^d)^q g^r = e^q g^r = g^r.$$

Thus $g^r = e$, but by minimality of d, we conclude that $r = 0$. Thus $d = |g|$ divides n. □

(3.2) Let $g \in G$ be an element of finite order. Show that g^m has finite order for any integer $m \geq 0$, and in fact

$$|g^m| = \frac{\operatorname{lcm}(m, |g|)}{m} = \frac{|g|}{\gcd(m, |g|))}.$$

Proof. Set $\ell = \operatorname{lcm}(m, |g|)$ and note that $\ell = d|g|$ for some integer d. Then we have

$$(g^m)^{\frac{\ell}{m}} = g^\ell = g^{d|g|} = \left(g^{|g|}\right)^d = e^d = e,$$

which implies

$$|g^m| \leq \frac{\ell}{m} = \frac{\operatorname{lcm}(m, |g|)}{m}.$$

Moreover, if $n > 0$ is an integer so that $(g^m)^n = e$ then $g^{mn} = e$. Write according to the division theorem $mn = |g|q + r$ with $0 \leq r < |g|$. Then $g^{mn} = e$ and $g^{|g|} = e$ imply $g^r = e$ and since $r < |g|$ we must have $r = 0$ by the definition of order. So $mn = |g|q$ for some integer q. Set $t = \gcd(m, |g|)$ so that $m = ta$ and $|g| = tb$ with a, b non-negative integers with $\gcd(a, b) = 1$. Then we have

$$mn = |g|q \iff tan = tbq \iff an = bq \Rightarrow b \mid n,$$

where the last implication is due to $\gcd(a, b) = 1$. The above shows $n \geq b$, so

$$|g^m| \geq b = \frac{|g|}{\gcd(m, |g|)}.$$

Finally, since

$$\frac{\operatorname{lcm}(m, |g|)}{m} = \frac{|g|}{\gcd(m, |g|)}$$

holds by elementary arithmetic, the above inequalities prove the claim. □

(3.3) Prove that for all g, h in G, $|gh| = |hg|$ holds.

Proof. First we show that $|x| = |yxy^{-1}|$ for all $x, y \in G$. Indeed, recall that $x^n = (yxy^{-1})^n$ and thus $x^n = e$ if and only if $(yxy^{-1})^n = e$. This establishes the claim.

Next set $x = gh$ and $y = g^{-1}$ in the above claim to deduce that

$$|gh| = |g^{-1}(gh)g| = |hg|.$$

□

Problem 4. Let C denote the unit circle in the plane $\mathbb{R}^2$. One can show, along similar lines to our analysis of D_n, that the group G symmetries of C consists exactly of the following elements:

$r_\alpha =$	rotation counterclockwise by $2\pi\alpha$	for $0 \leq \alpha < 1$
$s_\alpha =$	reflection over the line through the center with angle $\pi\alpha$	for $0 \leq \alpha < 1$

You do not have to prove this.

(4.1) Determine the order of each element of G.

Proof. Each reflection has order 2. For a rotation r_α, if α is rational and $\alpha = \frac{m}{n}$ in lowest terms, the order of r_α is n; if α is irrational, the order of r_α is infinite. □

(4.2) Find two elements $g, h \in G$ of finite order with product gh of infinite order.

Proof. Let $\alpha \in [0, 1)$ be irrational and consider the elements s_0 and s_α. We claim that $s_\alpha s_0 = r_{2\alpha}$. Indeed, let $x \in C$ and let $2\pi t$ be the angle from $(1, 0)$ to x. Then $s_\alpha s_0(x)$ is the point y with angle $2\pi(t + 2\alpha)$ from $(1, 0)$ to y. Since this is true for all points on the unit circle, $s_\alpha s_0 = r_{2\alpha}$. □

Problem 5. Show that for every integer $n \geqslant 2$, there is no nontrivial group homomorphism $\mathbb{Z}/n \longrightarrow \mathbb{Z}$.

Proof. Suppose that $f : \mathbb{Z}/n \longrightarrow \mathbb{Z}$ is a group homomorphism. Denote the class of $i \in \mathbb{Z}$ by $[i]$. Then

$$\begin{aligned} 0 &= f([0]) && \text{since } f \text{ is a group homomorphism} \\ &= f([n]) && \text{since } [n] = [0] \\ &= f(n[1]) && \text{since } n[1] = [n] \\ &= nf([1]) && \text{since } f \text{ is a homomorphism} \end{aligned}$$

Thus $nf([1]) = 0$, which implies that $f([1]) = 0$. But $[1]$ generates $\mathbb{Z}/n$, and we conclude that f must be the trivial map, since for any $[a] \in \mathbb{Z}/n$, we have

$$f([a]) = af([1]) = 0. \quad \square$$