# Math 1530: Homework 2

Milan Capoor

26 September 2023

## 2.26

*Let $G$ be a group and let $g \in G$ be an element of order $n$, and let $k \geq 1$.*

(a) *Prove that $g^k$ has order $n/\gcd(n,k)$*

Because $G$ has an element of order $n$, we know that

$$(g^k)^{\frac{n}{\gcd(n,k)}} = (g^n)^{\frac{k}{\gcd(n,k)}} = e$$

so

$$o(g^k) \left| \frac{n}{\gcd(n,k)} \right.$$

Now to show that this quantity is the order of $g^k$, we just need to show that it is the smallest value for which the above is true,

We choose an $m$ that satisfies

$$(g^k)^m = g^{km} = e$$

So

$$n | km \implies \frac{n}{\gcd(k,n)} \left| \frac{km}{\gcd(k,n)} \right.$$

However,

$$\gcd\left(\frac{n}{\gcd(k,n)}, \frac{k}{\gcd(k,n)}\right) = 1$$

(Because if they were not relatively prime, there would be a bigger $\gcd(k,n)$)
So

$$\frac{n}{\gcd(k,n)} \left| m \implies \frac{n}{\gcd(k,n)} \leq m \right.$$

Which shows that for any $m$ which satisfies the equation, it is still greater than or equal to $\frac{n}{\gcd(k,n)}$. Hence, $o(g^k) = \frac{n}{\gcd(k,n)}$ ■

(b) *Use (a) to give a quick proof that if* $G = \langle g \rangle$ *is a cyclic group of order* $n$*, then* $g^k$ *generates* $G$ *iff* $\gcd(n, k) = 1$

Since $G$ is a group of order $n$, $g^k$ can only be a generator if

$$o(g^k) = o(G) = n$$

But from (a),

$$o(g^k) = \frac{n}{\gcd(k,n)} \implies \frac{n}{\gcd(k,n)} = n \implies \gcd(k,n) = 1 \quad ■$$

## 2.28

*Let $G$ be a group and let $H \subset G$ be a subset of $G$. Prove that $H$ is a subgroup iff it has the following two properties:*

1. $H \neq \emptyset$
2. *For every $h_1, h_2 \in H$, the product $h_1 \cdot h_2^{-1}$ is in $H$.*

To be a subgroup, $H$ must satisfy the properties of a group. Namely, it must have an identity and inverse element. Clearly, if $H = \emptyset$ it has neither so it would not be a subgroup.

Then, if with $h_1 = h_2$, the element $h_1 h_2^{-1} = h_1 h_1^{-1} = e$ were not in $H$, the set would not have an identity element and would not be a group.

Similarly, let $h_1 = e$. Then, if the element $h_1 h_2^{-1} = h_2^{-1}$ is not in $H$, then not every $h_2$ would have an inverse element $h_2^{-1}$ and $H$ would not be a group. Letting $h_2 = e$ identically shows that the inverse of every $h_1$ must be in the set.

By these contradictions, then, both properties must be true for $H$ to be a subgroup of $G$. ■

## 2.30

Let $G$ be a group and let $S \subseteq G$ be a subset of $G$.

$$\langle S \rangle = \bigcap_{S \subseteq H \subset G} H$$

*i.e., $\langle S \rangle$ is the intersection of all subgroups $H$ of $G$ that contain $S$*

(a) *Prove that $\langle S \rangle \neq \emptyset$*

All the subgroups $H$ must contain the identity element so, at minimum,

$$\langle S \rangle = \bigcap H = \{e\} \neq \emptyset \quad \blacksquare$$

(b) *Prove that $\langle S \rangle$ is a subgroup of $G$.*

From above, $\langle S \rangle$ has an identity. Additionally, all subgroups of $H \subseteq G$ have an inverse for every $h \in H$ by definition. As $\langle S \rangle$ is defined as the intersection of the subgroups $H$, every element in the intersection thus must also has an inverse in the intersection, so every $s \in \langle S \rangle$ has an inverse. Therefore, $\langle S \rangle$ satisfies the identity and inverse requirements and is a subgroup. $\blacksquare$

(c) *Suppose that $K \subseteq G$ is a subgroup of $G$ and that $S \subseteq K$. Prove that $\langle S \rangle \subset K$. ($\langle S \rangle$ is the smallest subgroup of $G$ that contains $S$.)*

If $S \subset K$, then by definition of $\langle S \rangle$,

$$\langle S \rangle = K \cap \left( \bigcap_{\substack{S \subseteq H \subset G \\ H \neq K}} H \right)$$

However, by the properties of intersection,

$$A \cap B \subseteq A \quad \forall B$$

so

$$K \cap \left( \bigcap_{\substack{S \subseteq H \subset G \\ H \neq K}} H \right) \subseteq K \implies \langle S \rangle \subseteq K \quad \blacksquare$$

(d) *Let $T$ be the set of inverses of elements in $S$,*

$$T = \{g^{-1} : g \in S\}$$

*Prove that $\langle S \rangle$ is equal to the following set of products:*

$$\langle S \rangle = \{g_1 g_2 \dots g_n : n \geq 0 \text{ and } g_1, \dots, g_n \in S \cup T\}$$

Because the product $g_1 g_2 \dots g_n$ is defined for all $n \geq 0$, every element $g_i \in S$ is in $S \cup T$ (Let $g_1 = g_i$ and $n = 1$) and so is $g_i^{-1}$ ($g_1 = g_i^{-1}$). The identity corresponds to $n = 0$. Thus $H = \{\prod_{i=1}^{n} g_n\}$ is a subgroup of $G$.

Because every element $g_i$ is either in $S$ or is the inverse of an element in $S$, removing any element from $H$ means that either there will be an element of $S$ that is not in $H$ or $H$ will not be a group. Thus, $H$ is the smallest subgroup of $G$ that contains all of $S$. But from part (c), $\langle S \rangle$ is the smallest subgroup of $G$ that contains $S$ so

$$\langle S \rangle = \{g_1 g_2 \dots g_n : n \geq 0 \text{ and } g_1, \dots, g_n \in S \cup T\} \quad \blacksquare$$

## 2.35

*Let $G$ be a group. The center of $G$ denoted $Z(G)$ is the set of elements of $G$ that commute with every other element:*

$$Z(G) = \{g \in G : gh = hg \; \forall h \in G\}$$

(a) *Prove that $Z(G)$ is a subgroup of $G$*

By definition, the identity element $e$ of $G$ satisfies $eh = he = h$ for all $h \in G$. Similarly, the inverse $h^{-1}$ is defined as the element which satisfies $hh^{-1} = h^{-1}h = e$ for all $h$ is $G$. Thus, as they are commutative with all elements of $G$, both the inverse and identity of $G$ are in $Z(G)$, so $Z(G)$ is a group. ■

(b) *When does $Z(G)$ equal $G$*

When $G$ is an abelian group.

(c) *Compute the center of the symmetric group $\mathcal{S}_n$*

For $n = 1$, the center is obviously the entire group. For $n = 2$, the two elements are the identity which is commutative (and so in the center) for all groups and the reversal of the elements which is its own inverse and is thus also in the center.

For $n \geq 3$, let $\sigma \in S_n : \sigma \neq e$ and let $i, j, k$ be distinct values in $\{1, 2, \ldots, n\}$. Let $\sigma(i) = j$ and $\sigma(j) = k$. Note that $\sigma$ is an arbitrary permutation of $\{1, 2, \ldots, n\}$. Now consider

$$\tau(x) = \begin{cases} j & x = i \\ i & x = j \\ x & \text{otherwise} \end{cases}$$

Thus,

$$\begin{aligned} (\tau \circ \sigma)(i) &= \tau(j) = i \\ (\sigma \circ \tau)(i) &= \sigma(j) = k \\ i \neq j &\implies (\tau \circ \sigma)(i) \neq (\sigma \circ \tau)(i) \end{aligned}$$

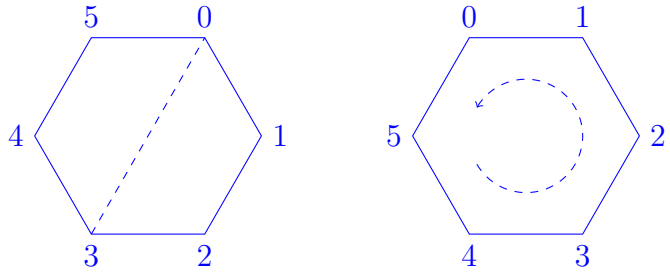
So we have found an element in $S_n$ which $\sigma$ does not commute with. But because $\sigma$ is any arbitrary permutation ($\sigma \neq e$), then there is no element in $S_{n\geq 3}$ which commutes with every element so the center of $S_n$ is $\{e\}$ ■.

(d) *Compute the center of the dihedral group* $\mathcal{D}_n$

Let $P$ be a $2n$-gon. Let $a$ be a reflection. Label the vertices of $P$ by $0, 1, \ldots 2n-1$.

Let $a$ be a flip such that $a(0) = 0$, $a(n) = n$, and all the other vertices are moved counterclockwise (i.e. $a(1) = 2n-1$). Let $b$ be the clockwise rotation $b(0) = 1, b(1) = 2, \ldots$.

For $n = 3$, for example, the two transformations can be represented:




$a = (0)(15)(24)(3)$ $\qquad$ $b = (012345)$

Then

$$(a \circ b)(0) = a(1) = 2n-1$$
$$(b \circ a)(0) = b(0) = 1$$
$$1 \neq 2n-1 \implies ab \neq ba$$

But as $a$ is an arbitrary reflection that can be transformed into any other reflection through a re-labeling of vertices or a rotation of the entire system, we can conclude that no reflections are commutative with every element of $D_{2n}$ (because we have a counter example) so no reflection is part of the center of $D_{2n}$.

For odd n-gons we can make exactly the same argument but with $a$ satisfying only $a(0) = 0$, $a(1) = n-1$. Using the same $b$,

$$(a \circ b)(0) = a(1) = n-1$$
$$(b \circ a)(0) = b(0) = 1$$
$$1 \neq n-1 \implies ab \neq ba$$

So reflections are not in the center of any dihedral group.

Now, all that remains is to classify the rotations. Notice, however, that reversing the argument given above shows that a rotation by $\frac{2\pi}{n}$ radians (for an n-gon) does not commute with any reflection so it cannot be in the center. Are any of the composite rotations $r^m = \frac{2\pi}{n}m \quad (m \leq n)$ in $Z(D_n)$?

First we observe that all reflections are commutative with each other because $\langle r \rangle$ is an abelian subgroup. Then we notice that the composition of a clockwise rotation and a flip results in a net counterclockwise rotation (the order of $\langle r \rangle = n$ so every vertex is can be permuted to every other vertex by rotations) and vice versa. Meanwhile, the composition of a flip and a rotation preserves the direction of the rotation. Thus, the only way that the two compositions could commute were if a clockwise and counterclockwise rotation resulted in the same point. For odd n-gons the only rotation with this property is the identity. For even n-gons, a rotation by $\pi$ radians (i.e. when $m = \frac{n}{2}$) satisfies the property $r^{\frac{n}{2}} = r^{\frac{-n}{2}}$. Thus the only rotation that can commute with any reflection is the rotation by $\pi$ radians for n-gons of even $n$. Then because all rotations commute, the rotation $r^{n/2}$ commutes with every element of $D_n$.

Thus, the only elements in $Z(D_n)$ are $\{e\}$ and $r^{n/2}$ (for n-gons of even $n$). ■

(e) *Compute the center of the quaternion group* $\mathcal{Q}$

$$\mathcal{Q} = \{\pm 1, \pm i, \pm j, \pm k\}$$

From Exercise 2.17,

$$\begin{aligned} i \cdot j &= k, & j \cdot k &= i, & k \cdot i &= j \\ j \cdot i &= -k, & k \cdot j &= -i, & i \cdot k &= -j \end{aligned}$$

So none of the compositions of $i, j, k$ are commutative so the only operations in the center are $\boxed{\{1, -1\}}$

## 2.38

*Let $G$ be a finite group whose only subgroups are $\{e\}$ and $G$. Prove that either $G = \{e\}$ or else that $G$ is a cyclic group with prime order.*

If $G = \{e\}$, we are done. Otherwise, it has an element $g$ and a subgroup $H = \langle g \rangle$. However, because we know that the only subgroups of $G$ are $\{e\}$ and $G$, $H = \{e\}$ or $H = G$. If $H = \{e\}$ then the only element is $e$ which is a contradiction so $H = \langle g \rangle = G$. Thus, $g$ is a generator of $G$ so $G$ is cyclic with order $o(g)$.

$o(g)$ can either be composite or prime. Assume it is composite. Then $o(g)$ has a prime factorization, i.e. there are at least two primes $p, q$ for which $p^n | o(g)$ and $q^m | o(g)$ for some $m$ and $n$. By Sylow's theorem, $G$ thus has subgroups of order $p^n$ and $q^m$. But this contradicts the fact that $G$ only has two subgroups. Thus $o(g)$ can only have one prime factor $p^n = o(g)$. Further, we can use a similar argument to show that if $p^n = o(g)$, $p | o(g)$ so $G$ must have a subgroup with order $p$ but its only subgroup is order $o(g)$ so $n = 1$ and $p = o(g)$.

Hence, $o(g)$ must be a cyclic group of prime order. ■