Math 350, Spring 2026 Professor Rob Benedetto

Solutions to Midterm Exam 1

1. **(16 points)** Compute the order of the element $(15, 15)$ in the group $C_{40} \times C_{36}$.

Solution. Since 1 is a generator for C_{40}, a theorem [namely Theorem 4.4(iii), but you don't need to know that number] says that

$$\text{in } C_{40}, \text{ we have } o(15) = \frac{40}{(40, 15)} = \frac{40}{5} = 8,$$

since $40 = 2^3 \cdot 5$ and $15 = 3 \cdot 5$, so $\gcd(40, 15) = 5$. Similarly,

$$\text{in } C_{36}, \text{ we have } o(15) = \frac{36}{(36, 15)} = \frac{36}{3} = 12,$$

since $36 = 2^2 \cdot 3^2$ and $15 = 3 \cdot 5$, so $\gcd(36, 15) = 3$.
Thus, by another theorem [namely Theorem 6.1(i)], we have

$$o\big((15, 15)\big) = \text{lcm}(8, 12) = \boxed{24}$$

since $8 = 2^3$ and $12 = 2^2 \cdot 3$, so their lcm is $2^3 \cdot 3 = 24$.

---

2. **(20 points)** Let H be the following set of 2×2 matrices:

$$H = \left\{ \begin{bmatrix} a & 0 \\ b & 1 \end{bmatrix} \in GL(2, \mathbb{R}) \,\middle|\, a, b \in \mathbb{R} \text{ and } a \neq 0 \right\}.$$

Prove that H is a subgroup of $GL(2, \mathbb{R})$.

Proof. **(Nonempty)**: Choosing $a = 1$ and $b = 0$ we have $a, b \in \mathbb{R}$ with $a \neq 0$, so $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H$, and hence $H \neq \varnothing$.

(Closed): Given $A, B \in H$, write $A = \begin{bmatrix} a & 0 \\ b & 1 \end{bmatrix} \in H$ and $B = \begin{bmatrix} c & 0 \\ d & 1 \end{bmatrix} \in H$, with $a, b, c, d \in \mathbb{R}$ and $a, c \neq 0$.
Then $AB = \begin{bmatrix} ac & 0 \\ bc + d & 1 \end{bmatrix}$. Since $ac, bc + d \in \mathbb{R}$ with $ac \neq 0$, we have $AB \in H$.

(Inverses): Given $A \in H$, write $A = \begin{bmatrix} a & 0 \\ b & 1 \end{bmatrix} \in H$, with $a, b \in \mathbb{R}$ and $a \neq 0$.
Then $A^{-1} = \dfrac{1}{a - 0} \begin{bmatrix} 1 & 0 \\ -b & a \end{bmatrix} = \begin{bmatrix} 1/a & 0 \\ -b/a & 1 \end{bmatrix}$. Since $a \neq 0$, we have $-b/a \in \mathbb{R}$ and $1/a \in \mathbb{R}$ with $1/a \neq 0$.
Thus, $A^{-1} \in H$. QED

---

3. **(16 points)** Let G be a group, and let $a \in G$. Let $f : G \to G$ be the function given by

$$f(x) = (ax)^{-1} \qquad \text{for all } x \in G.$$

Prove that f is one-to-one and onto.

Proof. **(One-to-one)**: Given $x_1, x_2 \in G$ such that $f(x_1) = f(x_2)$, we have $(ax_1)^{-1} = (ax_2)^{-1}$.
Taking inverses of both sides, we have $ax_1 = ax_2$. Therefore, [by right cancellation] we have $x_1 = x_2$.
QED 1-1

(Onto): Given $y \in G$, let $x = a^{-1}y^{-1} \in G$. Then
$f(x) = (ax)^{-1} = \big(a(a^{-1}y^{-1})\big)^{-1} = \big((aa^{-1})y^{-1}\big)^{-1} = (ey^{-1})^{-1}) = (y^{-1})^{-1} = y.$ QED

4. **(16 points)** Let G be a group, and let $a, b \in G$ be elements that happen to satisfy the equation

$$ba = a^5 b.$$

Use induction to prove, for all positive integers $n \geq 1$, that

$$ba^n = a^{5n} b.$$

Proof. **Base Case**: For $n = 1$, we have $ba^1 = ba = a^5 b = a^{5(1)} b$ by hypothesis.

Inductive Step: Suppose the conclusion holds for some $n = k \geq 1$; we must show it for $k + 1$.
We have $ba^{k+1} = ba^k a = a^{5k} ba = a^{5k} a^5 b = a^{5k+5} b = a^{5(k+1)} b$, as desired. Here, the second equality is by the inductive hypothesis, and the third is by the original hypothesis. QED

---

5. **(12 points)** Let G be a group, and suppose that for every $x, y \in G$, we have $(xy)^2 = x^2 y^2$. Prove that G is abelian.

Proof. Given $x, y \in G$, then by hypothesis we have $(xy)^2 = x^2 y^2$. That is, $xyxy = xxyy$.
By left cancellation (of the x's on the left), we have $yxy = xyy$.
So by right cancellation (of the y's on the right), we have $yx = xy$. QED

---

6. **(20 points)** Let G be the set $\mathbb{R}$, and for $x, y \in \mathbb{R}$, define $x * y$ to be

$$x * y = x + y - 2.$$

Prove that $(G, *)$ is a group.

Proof. **(Bin Op)**: Given $x, y \in \mathbb{R}$, then $x * y = x + y - 2 \in \mathbb{R}$.

(Assoc): Given $x, y, z \in \mathbb{R}$, we have
$(x * y) * z = (x + y - 2) * z = (x + y - 2) + z - 2 = x + (y + z - 2) - 2 = x * (y + z - 2) = x * (y * z)$.

(Id): Let $e = 2 \in \mathbb{R}$.
Given $x \in \mathbb{R}$, then $x * e = x + 2 - 2 = x$ and $e * x = 2 + x - 2 = x$.

(Inv): Given $x \in \mathbb{R}$, let $y = 4 - x \in \mathbb{R}$.
Then $x * y = x + (4 - x) - 2 = 2 = e$ and $y * x = (4 - x) + x - 2 = 2 = e$. QED

OPTIONAL BONUS. (2 points.) Prove that the group $\mathbb{Z} \times C_3$ is not cyclic.

Proof. Suppose (towards contradiction) that $\mathbb{Z} \times C_3$ **is** cyclic. Then there is a generator $(m, a) \in \mathbb{Z} \times C_3$.

Recall that $C_3 = \{0, 1, 2\}$, with the identity element of C_3 being 0.

We have $(1, 0), (1, 1) \in \mathbb{Z} \times C_3 = \langle (m, a) \rangle$, so there exist integers $i, j \in \mathbb{Z}$ such that $(1, 0) = (m, a)^i$ and $(1, 1) = (m, a)^j$.

That is, $(1, 0) = (im, ia)$ and $(1, 1) = (jm, ja)$. In particular, $im = 1$, so $m \neq 0$, and $im = 1 = jm$, so that $i = j$. [Remember, all three of i, j, m are just plain old integers, and we just noted that $m \neq 0$.]

But also $ia = 0$ and $ja = 1$ in C_3. That is, $1 = ja = ia = 0$ in C_3, contradicting the fact that $1 \neq 0$ in C_3.

By this contradiction, our original supposition is false. Thus, $\mathbb{Z} \times C_3$ is **not** cyclic. QED