Math 350, Spring 2025 Professor Rob Benedetto

Solutions to Midterm Exam 1, Section 02

1. **(15 points)** Let G be a group, and let $a, b \in G$ be elements for which the following equation holds:

$$ba = a^6 b.$$

Use induction to prove, for all positive integers $n \geq 1$, that $ba^n = a^{6n} b$.

Solution. **Base Case**: For $n = 1$, we have $ba^1 = ba = a^6 b = a^{6(1)} b$ by hypothesis.

Inductive Step: Suppose the conclusion holds for some $n = k \geq 1$; we must show it for $k+1$. We have $ba^{k+1} = ba^k a = a^{6k} ba = a^{6k} a^6 b = a^{6k+6} b = a^{6(k+1)} b$, as desired. Here, the second equality is by the inductive hypothesis, and the third is by the original hypothesis. QED

---

2. **(15 points)** Compute the order of the element $(30, 28)$ in the group $C_{80} \times C_{48}$.

Solution. Since 1 is a generator for C_{80}, a theorem [namely Theorem 4.4(iii), but you don't need to know that number] says that

$$\text{in } C_{80}, \text{ we have } o(30) = \frac{80}{(80, 30)} = \frac{80}{10} = 8,$$

since $80 = 2^4 \cdot 5$ and $30 = 2 \cdot 3 \cdot 5$, so $\gcd(80, 30) = 2 \cdot 5 = 10$. Similarly,

$$\text{in } C_{48}, \text{ we have } o(28) = \frac{48}{(48, 28)} = \frac{48}{4} = 12,$$

since $48 = 2^4 \cdot 3$ and $28 = 2^2 \cdot 7$, so $\gcd(48, 28) = 2^2 = 4$.
Thus, by another theorem [namely Theorem 6.1(i)], we have

$$o\big((30, 28)\big) = \operatorname{lcm}(8, 12) = \boxed{24}$$

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

---

3. **(15 points)** Let G be a group, and let $y \in G$. Suppose that

$$y^{77} = e \quad \text{and} \quad y^{42} = e, \quad \text{but} \quad y^{18} \neq e,$$

where e is the identity element of G. Prove that $o(y) = 7$.

Solution. Let $n = o(y)$. Since $y^{77} = e$, n must be finite, i.e., $n \geq 1$ is a positive integer.
By a theorem [Theorem 4.4(ii)], we must have both $n|77$ and $n|42$, since $a^{77} = e = a^{42}$.
Thus, $n|\gcd(77, 42)$, i.e., $n|7$, since $77 = 7 \cdot 11$ and $42 = 2 \cdot 3 \cdot 7$. That is, n is either 1 or 7.
If $n = 1$, then we would have $y^{18} = e$, since $1|18$. This is a contradiction, so $n \neq 1$.
Thus, we must have $n = 7$. QED

---

4. **(20 points)** Let G be the set $\mathbb{Z}$, and for $x, y \in \mathbb{Z}$, define $x * y$ to be

$$x * y = x + y - 5.$$

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

Solution. **(Bin Op)**: Given $x, y \in \mathbb{Z}$, then $x * y = x + y - 5 \in \mathbb{Z}$.

(Assoc): Given $x, y, z \in \mathbb{Z}$, we have
$(x*y)*z = (x+y-5)*z = (x+y-5)+z-5 = x+(y+z-5)-5 = x*(y+z-5) = x*(y*z)$.

(Id): Let $e = 5 \in \mathbb{Z}$.
Given $x \in \mathbb{Z}$, then $x * e = x + 5 - 5 = x$ and $e * x = 5 + x - 5 = x$.

(Inv): Given $x \in \mathbb{Z}$, let $y = 10 - x \in \mathbb{Z}$.
Then $x * y = x + (10 - x) - 5 = 5 = e$ and $y * x = (10 - x) + x - 5 = 5 = e$. QED

---

5. **(20 points)** Let H be the following set of 2×2 matrices:

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

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

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

(Closed): Given $A, B \in H$, write $A = \begin{bmatrix} a & 0 \\ a-b & b \end{bmatrix} \in H$ and $B = \begin{bmatrix} c & 0 \\ c-d & d \end{bmatrix} \in H$, with $a, b, c, d \in \mathbb{R}$ and $a, b, c, d \neq 0$.
Then $AB = \begin{bmatrix} ac & 0 \\ ac-bd & bd \end{bmatrix} \in H$,
since the lower left entry is $(a - b)c + b(c - d) = ac - bc + bc - bd = ac - bd$.
Since $ac, bd \in \mathbb{R}$ with $ac, bd \neq 0$, and the lower left entry is indeed their difference $ac - bd$, we have $AB \in H$.

(Inverses): Given $A \in H$, write $A = \begin{bmatrix} a & 0 \\ a-b & b \end{bmatrix} \in H$, with $a, b \in \mathbb{R}$ and $a, b \neq 0$.
Then $A^{-1} = \dfrac{1}{ab - 0} \begin{bmatrix} b & 0 \\ b-a & a \end{bmatrix} = \begin{bmatrix} 1/a & 0 \\ 1/a - 1/b & 1/b \end{bmatrix}$. Since $a, b \neq 0$, we have $1/a, 1/b \in \mathbb{R}$. We also have $1/a, 1/b \neq 0$, and the lower left entry is indeed their difference $1/a - 1/b$, so we have $A^{-1} \in H$. QED

---

6. **(15 points)** Let G be a group, and let $b \in G$. Define a function $f : G \to G$ by

$$f(x) = bx^{-1}.$$

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

Solution. **(One-to-one)**: Given $x_1, x_2 \in G$ such that $f(x_1) = f(x_2)$, we have $bx_1^{-1} = bx_2^{-1}$, and hence [by left cancellation] we have $x_1^{-1} = x_2^{-1}$.
Therefore, $x_1 = (x_1^{-1})^{-1} = (x_2^{-1})^{-1} = x_2$, as desired.

(Onto): Given $y \in G$, let $x = y^{-1}b \in G$. Then
$f(x) = bx^{-1} = b(y^{-1}b)^{-1} = bb^{-1}(y^{-1})^{-1} = ey = y$ QED

OPTIONAL BONUS. (2 points.) Let G be a **nontrivial** group. Prove that $\mathbb{Z} \times G$ is **not** cyclic.

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

Let e denote the identity element of G. Since G is nontrivial, there exists $c \in G \smallsetminus \{e\}$.

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

That is, $(1, e) = (im, a^i)$ and $(1, c) = (jm, a^j)$. In particular, $im = 1$, so $m \neq 0$, and $im = 1 = jm$, so that $i = j$.

But also $a^i = e$ and $a^j = c$. That is, $c = a^j = a^i = e$, contradicting the fact that $c \in G \smallsetminus \{e\}$.

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