Solutions to Midterm Exam 1, Section 01

1. **(15 points)** Compute the order of the element $(18,15)$ in the group $C_{28} \times C_{50}$.

Solution. Since 1 is a generator for C_{28}, a theorem [namely Theorem 4.4(iii), but you don't need to know that number] says that

$$\text{in } C_{28}, \text{ we have } o(18) = \frac{28}{(28,18)} = \frac{28}{2} = 14,$$

since $28 = 2^2 \cdot 7$ and $18 = 2 \cdot 3^2$, so $\gcd(28,18) = 2$. Similarly,

$$\text{in } C_{50}, \text{ we have } o(15) = \frac{50}{(50,15)} = \frac{50}{5} = 10,$$

since $50 = 2 \cdot 5^2$ and $15 = 3 \cdot 5$, so $\gcd(50,15) = 5$.
Thus, by another theorem [namely Theorem 6.1(i)], we have

$$o\big((18,15)\big) = \operatorname{lcm}(14,10) = \boxed{70}$$

since $14 = 2 \cdot 7$ and $10 = 2 \cdot 5$, so their lcm is $2 \cdot 5 \cdot 7 = 70$.

---

2. **(15 points)** Let G be a group, and let $a \in G$. Suppose that

$$a^{500} = e \quad \text{and} \quad a^{35} = e, \quad \text{but} \quad a^{32} \neq e,$$

where e is the identity element of G. Prove that $o(a) = 5$.

Solution. Let $n = o(a)$. Since $a^{500} = e$, n must be finite, i.e., $n \geq 1$ is a positive integer.
By a theorem [Theorem 4.4(ii)], we must have both $n|500$ and $n|35$, since $a^{500} = e = a^{35}$.
Thus, $n|\gcd(500,35)$, i.e., $n|5$, since $500 = 2^2 \cdot 5^3$ and $35 = 5 \cdot 7$. That is, n is either 1 or 5.
If $n = 1$, then we would have $a^{32} = e$, since $1|32$. This is a contradiction, so $n \neq 1$.
Thus, we must have $n = 5$. QED

---

3. **(15 points)** Let G be a group, and let $a, b \in G$ be elements for which the following equation holds:

$$ba = a^4 b.$$

Use induction to prove, for all positive integers $n \geq 1$, that $ba^n = a^{4n}b$.

Solution. **Base Case**: For $n = 1$, we have $ba^1 = ba = a^4 b = a^{4(1)}b$ by hypothesis.

Inductive Step: Suppose the conclusion holds for some $n = k \geq 1$; we must show it for $k+1$. We have $ba^{k+1} = ba^k a = a^{4k}ba = a^{4k}a^4 b = a^{4k+4}b = a^{4(k+1)}b$, as desired. Here, the second equality is by the inductive hypothesis, and the third is by the original hypothesis. QED

---

4. **(20 points)** Let H be the following set of 2×2 matrices:

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

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

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

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

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

---

5. **(15 points)** Let G be a group, and let $a \in G$. Define a function $f : G \to G$ by

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

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 $x_1^{-1}a = x_2^{-1}a$, and hence [by right 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 $x = ay^{-1} \in G$. Then
$f(x) = x^{-1}a = (ay^{-1})^{-1}a = (y^{-1})^{-1}a^{-1}a = ye = y$ QED

---

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

$$x * y = 3 + x + y.$$

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

Solution. **(Bin Op)**: Given $x, y \in \mathbb{R}$, then $x * y = 3 + x + y \in \mathbb{R}$.

(Assoc): Given $x, y, z \in \mathbb{R}$, we have
$(x*y)*z = (3+x+y)*z = 3+(3+x+y)+z = 3+x+(3+y+z) = x*(3+y+z) = x*(y*z)$.

(Id): Let $e = -3 \in \mathbb{R}$.
Given $x \in \mathbb{R}$, then $x * e = 3 + x + (-3) = x$ and $e * x = 3 + (-3) + x = x$.

(Inv): Given $x \in \mathbb{R}$, let $y = -6 - x \in \mathbb{R}$.
Then $x * y = 3 + x + (-6 - x) = -3 = e$ and $y * x = 3 + (-6 - x) + x = -3 = e$. QED

OPTIONAL BONUS. (2 points.) Let G be a group of order 350. Prove that there is an element $x \in G$ **other than the identity** such that $x^{-1} = x$.

Proof. Let $S_0 = \{g \in G : g^{-1} \neq g\}$. I claim that $|S_0|$ is even.

[The idea is that elements of S_0 come in pairs: g and g^{-1}.]

To prove the claim, if $S_0 \neq \varnothing$, then pick $g_0 \in S_0$, so that $g_0^{-1} \neq g_0$, and so also $g_0^{-1} \in S_0$. Define $S_1 = S_0 \setminus \{g_0, g_0^{-1}\}$.

If $S_1 \neq \varnothing$, then similarly, pick $g_1 \in S_1$, so that $g_1^{-1} \neq g_1$, and so also $g_1^{-1} \in S_1$. Define $S_2 = S_1 \setminus \{g_1, g_1^{-1}\}$.

Continue in this fashion, defining $S_3, S_4, \ldots$ by removing two elements at a time, until eventually we get to $S_m = \varnothing$. [**Note**: Technically we need an induction here, but never mind.]

Then $|S_0| = 2 + |S_1| = 4 + |S_2| = \cdots = 2m + |S_m| = 2m$ is even, proving the claim.

——— ——— ——— ——— ——— ——— ———

Now define $T = G \setminus S_0 = \{g \in G : g^{-1} = g\}$. So $|T| = 350 - |S_0|$ is also even. However, we have $e \in T$, since $e^{-1} = e$. So $|T|$ is an even number at least 1; thus, $|T| \geq 2$. Which means there is at least one element $x \in T$ **besides** the identity.

That is, there is some $x \in G \setminus \{e\}$ such that $x^{-1} = x$. QED