Math 350, Section 02, Fall 2022

Solutions to Exam 1

1. **(15 points)** Compute the order of the element $(9, 35)$ in the group $C_{24} \times C_{100}$.

Solution. By a Theorem [Theorem 4.4(iii)], the orders of $9 \in C_{24}$ and $35 \in C_{100}$ are

$$o(9) = \frac{24}{\gcd(9, 24)} = \frac{24}{3} = 8 \qquad \text{and} \qquad o(35) = \frac{100}{\gcd(35, 100)} = \frac{100}{5} = 20,$$

and because $\gcd(9, 24) = \gcd(3^2, 2^3 \cdot 3) = 3$ and $\gcd(35, 100) = \gcd(5 \cdot 7, 2^2 \cdot 5^2) = 5$.

So by another Theorem [Theorem 6.1(i)], we have

$$o((9, 35)) = \operatorname{lcm}(8, 20) = \operatorname{lcm}(2^3, 2^2 \cdot 5) = 2^3 \cdot 5 = \boxed{40}$$

---

2. **(15 points)** Find all elements of $C_{40} = \{0, 1, 2, \ldots, 39\}$ of order 10.

Solution. By a Theorem, for any $m \in C_{40}$, we have $o(m) = \dfrac{40}{\gcd(m, 40)}$. To get this to equal 10, we must find all $m \in C_{40}$ for which $\gcd(m, 40) = 4$.

Thus, we need m such that $4 | m$ but $8 \nmid m$ and $5 \nmid m$.

The multiples of 4 in C_{40} are $0, 4, 8, 12, 16, 20, 24, 28, 32, 36$.

Crossing out the ones divisible by 5 or 8, we are left with $4, 12, 28, 36$.

Thus, each of $\boxed{4, 12, 28, 36}$ has order 10 in C_{40}, and no other elements in C_{40} do.

---

3. **(15 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. By induction on $n \geq 1$:

Base Case: For $n = 1$, we have

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

as desired.

Inductive Step: Given $n \geq 2$, suppose the result is true for $n - 1$. Then

$$ba^n = (ba^{n-1})a = (a^{5(n-1)}b)a = a^{5(n-1)}(ba) = a^{5(n-1)}(a^5 b) = (a^{5(n-1)}a^5)b = a^{5(n-1)+5}b = a^{5n}b$$

as desired. QED

---

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

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

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

Proof. [Subset: any element $A \in H$ as written above has determinant $ab \neq 0$, so $A \in GL(2, \mathbb{R})$. Technically this should be checked, but I won't deduct points for missing this.]

Nonempty: Let $a = b = 1 \in \mathbb{R} \setminus \{0\}$. Then $\begin{bmatrix} 1 & 1-1 \\ 0 & 1 \end{bmatrix} \in H$.

[Note: Yes, you could simplify that, but why bother? The point is to show that there's something in H, which we did.]

Closure: Given $A, B \in H$, write

$$A = \begin{bmatrix} a & a-b \\ 0 & b \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} c & c-d \\ 0 & d \end{bmatrix} \quad \text{with} \quad a, b, c, d \in \mathbb{R} \setminus \{0\}.$$

Then

$$AB = \begin{bmatrix} ac & a(c-d)+(a-b)d \\ 0 & bd \end{bmatrix} = \begin{bmatrix} ac & ac-bd \\ 0 & bd \end{bmatrix},$$

and hence $AB \in H$ because $ac, bd \in \mathbb{R} \setminus \{0\}$.

Inverses: Given $A \in H$, write $A = \begin{bmatrix} a & a-b \\ 0 & b \end{bmatrix}$. Then

$$A^{-1} = \frac{1}{ab}\begin{bmatrix} b & -(a-b) \\ 0 & a \end{bmatrix} = \begin{bmatrix} \frac{1}{a} & \frac{1}{a}-\frac{1}{b} \\ 0 & \frac{1}{b} \end{bmatrix},$$

and hence $A^{-1} \in H$ because $\frac{1}{a}, \frac{1}{b} \in \mathbb{R} \setminus \{0\}$. QED

---

5. **(15 points)** Let G be a cyclic group of order 39. Define a function $f : G \to G$ by $f(x) = x^2$. Prove that f is onto.

Proof #1. Let $a \in G$ be a generator. Given $y \in G$, there is some integer $m \in \mathbb{Z}$ such that $y = a^m$.

Case 1: m is even: Then $m = 2k$ for some $k \in \mathbb{Z}$. Let $x = a^k \in G$. Then

$$f(x) = x^2 = (a^k)^2 = a^{2k} = a^m = y$$

as desired.

Case 2: m is odd: Then $m = 2k+1$ for some $k \in \mathbb{Z}$. Let $x = a^{k+20} \in G$. Then

$$f(x) = x^2 = (a^{k+20})^2 = a^{2k+40} = a^{m+39} = a^m a^{39} = ye = y$$

as desired. QED

Proof #2. Let $a \in G$ be a generator. We have $o(a) = |\langle a \rangle| = |G| = 39$, and therefore by a Theorem,

$$o(a^2) = \frac{39}{\gcd(2,39)} = \frac{39}{1} = 39.$$

Hence, $|\langle a^2 \rangle| = 39$, so $\langle a^2 \rangle$ must be all of G, i.e., a^2 is a generator for G.

Given $y \in G$, then because a^2 is a generator for G, there is some integer $m \in \mathbb{Z}$ such that $y = (a^2)^m$, i.e., $y = a^{2m}$.

Let $x = a^m \in G$. Then $f(x) = x^2 = (a^m)^2 = a^{2m} = y$. QED

Proof #3 (Slick). Let $a \in G$ be a generator.
Given $y \in G$, there is some integer $m \in \mathbb{Z}$ such that $y = a^m$.

Let $x = y^{20}$. Then $f(x) = (y^{20})^2 = y^{40} = y^{39}y = (a^m)^{39}y = a^{39m}y = (a^{39})^m y = e^m y = y$. QED

---

6. **(20 points)** Let G be the set $\mathbb{R}$ with binary operation $*$ given by

$$x * y = x + y - 4.$$

You may take my word for it that $*$ **is** in fact a binary operation on G. Prove that $(G, *)$ is a group.

Proof. **Associative**: Given $x, y, z \in G$, we have

$$(x * y) * z = (x + y - 4) * z = (x + y - 4) + z - 4 = x + (y + z - 4) - 4 = x + (y * z) - 4 = x * (y * z).$$

Identity: Let $e = 4 \in \mathbb{R} = G$. Given $x \in G$, we have

$$x * e = x + 4 - 4 = x \qquad \text{and} \qquad e * x = 4 + x - 4 = x,$$

confirming that e is an identity for G.

Inverses: Given $x \in G$, let $y = 8 - x \in G$. Then

$$x * y = x + (8 - x) - 4 = 4 = e \qquad \text{and} \qquad y * x = (8 - x) + x - 4 = 4 = e,$$

confirming that y is an inverse for x in G. 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 $c \in G \setminus \{e\}$.

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 $c \in G \setminus \{e\}$.

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