Solutions to Midterm Exam 1

1. **(10 points.)** Find integers $x, y \in \mathbb{Z}$ such that $87x + 40y = 1$.

Solution. Apply the Euclidean Algorithm:

$$87 = 2 \cdot 40 + 7, \quad 40 = 5 \cdot 7 + 5, \quad 7 = 1 \cdot 5 + 2, \quad 5 = 2 \cdot 2 + 1, \quad 2 = 2 \cdot 1 + 0,$$

so going back one remainder, we have $(87, 40) = 1$. Then, working backwards, we have

$$1 = 5 - 2(2) = 5 - 2(7 - 1(5)) = 3(5) - 2(7) = 3(40 - 5(7)) - 2(7) = 3(40) - 17(7)$$
$$= 3(40) - 17(87 - 2(40)) = 37(40) - 17(87)$$

That is, choosing $\boxed{x = -17 \text{ and } y = 37}$ gives $87x + 40y = 1$.

---

2. **(15 points.)** Compute the order of the element $(20, 15)$ in the group $C_{24} \times C_{50}$.

Solution. In the cyclic group C_{24}, a theorem gives us $o(20) = \dfrac{24}{(24, 20)} = \dfrac{24}{4} = 6$, where we computed $(24, 20) = 4$ by noting $24 = 2^3 \cdot 3$ and $20 = 2^2 \cdot 5$, so their gcd is $2^2 = 4$.
In the cyclic group C_{50}, a theorem gives us $o(15) = \dfrac{50}{(50, 15)} = \dfrac{50}{5} = 10$, where we computed $(50, 15) = 5$ by noting $50 = 2 \cdot 5^2$ and $15 = 3 \cdot 5$, so their gcd is $5^1 = 5$.
Finally, another theorem gives $o((20, 15)) = \text{lcm}(o(20), o(15)) = \text{lcm}(6, 10) = 30$, because $6 = 2 \cdot 3$ and $10 = 2 \cdot 5$, so the lcm is $2 \cdot 3 \cdot 5$. That is, the order is $\boxed{30}$

---

3. **(15 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. (**1-1**): Given $x, y \in G$ such that $f(x) = f(y)$, we have $(ax)^{-1} = (ay)^{-1}$, so taking inverses of both sides gives $\big((ax)^{-1}\big)^{-1} = \big((ay)^{-1}\big)^{-1}$, i.e., $ax = ay$. By the cancellation law, then, we have $x = y$.
(**Onto**): Given $y \in G$, let $x = a^{-1}y^{-1} \in G$.
Then $f(x) = \Big(a\big(a^{-1}y^{-1}\big)\Big)^{-1} = \big(ey^{-1}\big)^{-1} = \big(y^{-1}\big)^{-1} = y$. QED

---

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

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

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

Proof. (**Nonempty**): Note that choosing $a = 1 \in \mathbb{R}^\times$ gives $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H$.

(**Closure**): Given $A, B \in H$, write $A = \begin{bmatrix} 1 & a-1 \\ 0 & a \end{bmatrix}$ and $B = \begin{bmatrix} 1 & b-1 \\ 0 & b \end{bmatrix}$. Then

$$AB = \begin{bmatrix} 1 & (b-1) + (ab - b) \\ 0 & ab \end{bmatrix} = \begin{bmatrix} 1 & ab - 1 \\ 0 & ab \end{bmatrix} \in H,$$

because $ab \in \mathbb{R}$ with $ab \neq 0$.

(**Inverses**): Given $A \in H$, write $A = \begin{bmatrix} 1 & a-1 \\ 0 & a \end{bmatrix}$ with $a \in \mathbb{R}^\times$.

Then $A^{-1} = \dfrac{1}{a - 0} \begin{bmatrix} a & -a+1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \frac{1}{a} - 1 \\ 0 & \frac{1}{a} \end{bmatrix}$, which is in H because $1/a \in \mathbb{R}^\times$. QED

---

5. **(20 points.)** Let G be an **abelian** group, let $K = G \times G$, and let

$$H = \big\{(a, b) \in K \,\big|\, ab^2 = e\big\},$$

where e is the identity element of G. Prove that H is a subgroup of K.

Proof. (**Nonempty**): Note that $(e, e) \in K$ has $ee^2 = e$, so $(e, e) \in H$.

(**Closure**): Given $(a, b), (c, d) \in H$, then we compute

$$(ac)(bd)^2 = acbdbd = (ab^2)(cd^2) = ee = e,$$

where the second equality is because G is abelian, and the third is because $(a, b), (c, d) \in H$. Thus, $(a, b)(c, d) = (ac, bd) \in H$.

(**Inverses**): Given $(a, b) \in H$, we compute

$$(a^{-1})(b^{-1})^2 = a^{-1}b^{-2} = b^{-2}a^{-1} = (ab^2)^{-1} = e^{-1} = e,$$

where the second equality is because G is abelian, and the fourth is because $(a, b) \in H$. Thus, $(a, b)^{-1} = (a^{-1}, b^{-1}) \in H$. QED

---

6. **(20 points.)** Let G be a group. Prove that G is abelian if and only if $(xy)^2 = x^2y^2$ for all $x, y \in G$.

Proof. ($\Rightarrow$) Given $x, y \in G$, then $(xy)^2 = xyxy = xxyy = x^2y^2$, where the second equality is because G is abelian.

($\Leftarrow$) Given $a, b \in G$, then by assumption we have $(ab)^2 = a^2b^2$, i.e., $abab = aabb$.
Applying cancellation of a on the left and b on the right, we have $ba = ab$, as desired. QED

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

Proof. Given a supposed generator $(k, g) \in \mathbb{Z} \times G$, there is an integer $m \in \mathbb{Z}$ such that $(k, g)^m = (1, e)$. That is,

$$(mk, g^m) = (1, e),$$

which means $mk = 1$, and hence $k = \pm 1$.
Case 1: If $g = e$, then pick $a \in G \setminus \{e\}$; this is possible because G is nontrivial. For any $n \in \mathbb{Z}$, we have

$$(k, g)^n = (k, e)^n = (nk, e^n) = (nk, e) \neq (0, a),$$

and hence $(0, a) \notin \langle (k, g) \rangle$ even though $(0, a) \in \mathbb{Z} \times G$. Thus, (k, g) is not a generator.
Case 2: If $g \neq e$ and $k = 1$, then for any $n \in \mathbb{Z}$, we have

$$(k, g)^n = (n, g^n) \neq (1, e),$$

because if $(n, g^n) = (1, e)$, then $n = 1$ and $g^n = e$, and hence $g = e$, a contradiction. Thus, $(1, e) \notin \langle (k, g) \rangle$ even though $(1, e) \in \mathbb{Z} \times G$. Hence, (k, g) is not a generator.
Case 3: The only remaining possibility is that $g \neq e$ and $k = -1$. Then for any $n \in \mathbb{Z}$, we have

$$(k, g)^n = (-n, g^n) \neq (-1, e),$$

because if $(-n, g^n) = (-1, e)$, then $n = 1$ and $g^n = e$, and hence $g = e$, a contradiction. Thus, $(-1, e) \notin \langle (k, g) \rangle$ even though $(-1, e) \in \mathbb{Z} \times G$. Hence, (k, g) is not a generator. QED