Solutions to Midterm Exam 1

1. **(15 points.)** Compute the order of the element $(8, 21)$ in the group $C_{100} \times C_{35}$.

Solution. In the cyclic group C_{100}, a theorem gives us $o(8) = \dfrac{100}{(100,8)} = \dfrac{100}{4} = 25$, where we computed $(100, 8) = 4$ by noting $100 = 2^2 \cdot 5^2$ and $8 = 2^3$, so their gcd is $2^2 = 4$.
In the cyclic group C_{35}, a theorem gives us $o(21) = \dfrac{35}{(35,21)} = \dfrac{35}{7} = 5$, where we computed $(35, 21) = 7$ by noting $35 = 5 \cdot 7$ and $21 = 3 \cdot 7$, so their gcd is $7^1 = 7$.
Finally, another theorem gives $o((8, 21)) = \text{lcm}(o(8), o(21)) = \text{lcm}(25, 5) = 25$, because $25 = 5^2$ and $5 = 5^1$, so the lcm is 5^2. That is, the order is $\boxed{25}$

---

2. **(10 points.)** Find integers $x, y \in \mathbb{Z}$ such that $109x + 25y = 1$.

Solution. Apply the Euclidean Algorithm:

$$109 = 4 \cdot 25 + 9, \quad 25 = 2 \cdot 9 + 7, \quad 9 = 1 \cdot 7 + 2, \quad 7 = 3 \cdot 2 + 1, \quad 2 = 2 \cdot 1 + 0,$$

so going back one remainder, we have $(109, 25) = 1$. Then, working backwards, we have

$$1 = 7 - 3(2) = 7 - 3(9 - 1(7)) = 4(7) - 3(9) = 4(25 - 2(9)) - 3(9) = 4(25) - 11(9)$$
$$= 4(25) - 11(109 - 4(25)) = 48(25) - 11(109)$$

That is, choosing $\boxed{x = -11 \text{ and } y = 48}$ gives $109x + 25y = 1$.

---

3. **(20 points.)** Let G be an **abelian** group, let $K = G \times G$, and let

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

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 $e^2 e = e$, so $(e, e) \in H$.

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

$$(ac)^2(bd) = acacbd = (a^2 b)(c^2 d) = ee = e,$$

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

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

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

---

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

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

$$AB = \begin{bmatrix} ac & 0 \\ bc + d & 1 \end{bmatrix} \in H,$$

because $ac, bc + d \in \mathbb{R}$ with $ac \neq 0$.

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

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

---

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

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

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 $x^{-1}a = y^{-1}a$, so $x^{-1} = y^{-1}$ by the cancellation laws. Taking inverses, we have $x = (x^{-1})^{-1} = (y^{-1})^{-1} = y$, as desired.

(**Onto**): Given $y \in G$, let $x = ay^{-1} \in G$.
Then $f(x) = \left(ay^{-1}\right)^{-1}a = \left(y^{-1}\right)^{-1}a^{-1}a = ye = y$. QED

---

6. **(20 points.)** Let G be a group. Prove that G is abelian if and only if $(xy)^{-1} = x^{-1}y^{-1}$ for all $x, y \in G$.

Proof. ($\Rightarrow$) Given $x, y \in G$, then $(xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1}$, where the second equality is because G is abelian.

($\Leftarrow$) Given $a, b \in G$, let $x = a^{-1}$ and $y = b^{-1}$. Then

$$ab = x^{-1}y^{-1} = (xy)^{-1} = \left(a^{-1}b^{-1}\right)^{-1} = \left(b^{-1}\right)^{-1}\left(a^{-1}\right)^{-1} = ba,$$

where the second equality is by our assumption. QED

OPTIONAL BONUS. (2 points.) Let G be a group of order 4000. 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 $S_1 = S_0 \smallsetminus \{g_0, g_0^{-1}\}$.

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 $S_2 = S_1 \smallsetminus \{g_1, g_1^{-1}\}$.

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.

So now let $T = G \smallsetminus S_0 = \{g \in G : g^{-1} = g\}$. So $|T| = 4000 - |S_0|$ 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 $x \in G \smallsetminus \{e\}$ such that $x^{-1} = x$. QED