# Math 3124 Exam 3 Solutions

Apr 14, 2004

1. (a) (3 pts) State the definition of homomorphism.

   Let $G$ and $H$ be groups. A map $\alpha : G \to H$ is a homomorphism if $\alpha(xy) = \alpha(x)\alpha(y)$ for all $x, y \in G$.

   (b) (3 pts) State the definition of isomorphism.

   Let $G$ and $H$ be groups. A map $\alpha : G \to H$ is a isomorphism if it is invertible and is a homomorphism.

   (c) (5 pts) Prove that if $\alpha : G \to H$ is an isomorphism then $\alpha^{-1}$ is also an isomorphism.

   So $\alpha$ is invertible and hence $\alpha^{-1} : H \to G$ exists and is also invertible. Let $a, b \in H$ and $x = \alpha^{-1}(a)$, $y = \alpha^{-1}(b)$. As $x, y \in G$

   $$ab = \alpha(x)\alpha(y) = \alpha(xy).$$

   Now apply $\alpha^{-1}$ to both sides:

   $$\alpha^{-1}(ab) = \alpha^{-1}(\alpha(xy)) = xy = \alpha^{-1}(a)\,\alpha^{-1}(b).$$

   So $\alpha^{-1}$ is a homomorphism.

   (d) (6 pts) Prove that if $\alpha : G \to H$ is an isomorphism and $x \in G$ then $|\alpha(x)| = |x|$.

   Since $\alpha$ is a homomorphism, $\alpha(e_G) = e_H$. But $\alpha$ is also one-to-one, so $\alpha(g) = e_H$ iff $x = e_G$. So

   $$\alpha(x)^n = \alpha(x^n) = e_H \quad \iff \quad x^n = e_G.$$

   Therefore the smallest positive integer $n$ for which $\alpha(x)^n = e_H$ is the same as the smallest positive integer $n$ for which $x^n = e_G$. Hence $|\alpha(x)| = |x|$. If no such positive integer exists then both orders are infinite.

2. Let $G$ and $G$ be groups and $\alpha : G \to H$ a homomorphism. Let $\sim$ be a relation on $G$ such that

   $$x \sim y \quad \text{iff} \quad \alpha(x) = \alpha(y).$$

   (a) (6 pts) Show that this is an equivalence relation.

   **Reflexive:** If $x \in G$, then $x \sim x$ since $\alpha(x) = \alpha(x)$.

   **Symmetric:** If $x, y \in G$ and $x \sim y$ then $\alpha(x) = \alpha(y)$, so $\alpha(y) = \alpha(x)$, so $y \sim x$.

   **Transitive:** If $x, y, z \in G$ and $x \sim y$ and $y \sim z$ then $\alpha(x) = \alpha(y)$ and $\alpha(y) = \alpha(z)$, so $\alpha(x) = \alpha(z)$, so $x \sim z$.

   (b) (6 pts) Let $K = \{g \in G \mid \alpha(g) = e_H\}$. Prove that $K$ is a subgroup of $G$.

   Clearly, $K \subseteq G$. Since $\alpha(e_G) = e_H$, $e_G \in K$. If $x, y \in K$, then $\alpha(x) = \alpha(y) = e_H$, so $\alpha(xy) = \alpha(x)\alpha(y) = e_H$, and hence $xy \in K$. If $x \in K$ then $\alpha(x^{-1}) = \alpha(x)^{-1} = e_H^{-1} = e_H$, so $x^{-1} \in K$. Hence $K \triangleleft G$.

   (c) (5 pts) Let $x, y \in G$. Prove that $x \sim y$ iff $xy^{-1} \in K$.

   $$x \sim y \iff \alpha(x) = \alpha(y) \iff \alpha(x)\alpha(y)^{-1} = e_H \iff$$
   $$\alpha(xy^{-1}) = e_H \iff xy^{-1} \in K.$$

(d) (3 pts) What are the equivalence classes of $\sim$?

Notice that the condition in part (c) is the same that we used to define the equivalence relation whose equivalence classes are the right cosets of $K$. So the equivalence classes are the right cosets of $K$.

(e) (10 pts) **Extra credit problem.** Prove that $gK = Kg$ for all $g \in G$, that is the left and right cosets of $K$ are the same. (Hint: In general this does not mean $gk = kg$ for all $k \in K$.

Since we are dealing with sets, we prove they are equal by showing $gK \subseteq Kg$ and $Kg \subseteq gK$. First observe that for any $k \in K$ and $g \in G$,

$$\alpha(gkg^{-1}) = \alpha(g)\alpha(k)\alpha(g)^{-1} = \alpha(g)e_H\alpha(g)^{-1} = \alpha(g)\alpha(g)^{-1} = e_H \implies gkg^{-1} \in K$$

and

$$\alpha(g^{-1}kg) = \alpha(g)^{-1}\alpha(k)\alpha(g) = \alpha(g)^{-1}e_H\alpha(g) = \alpha(g)^{-1}\alpha(g) = e_H \implies gkg^{-1} \in K.$$

Hence

$$gk = gkg^{-1}g \in Kg \qquad \text{and} \qquad kg = gg^{-1}kg \in gK.$$

The first implies $gK \subseteq Kg$ and the second implies $Kg \subseteq gK$.

3. (a) (3 pts) Let $G$ be a group and $S \subseteq G$. What is the definition of $\langle S \rangle$ the subgroup generated by $S$?

$\langle S \rangle$ is the smallest subgroup of $G$ which contains $S$ in the sense that if $H \triangleleft G$ and $S \subseteq H$, then $\langle S \rangle \triangleleft H$.

(b) (10 pts) Let $G$ be a finite group and $g, h \in G$ such that $2\,|g| = |G|$. Prove that either $h = g^n$ for some $n \in \mathbb{Z}$ or $\langle g, h \rangle = G$.

Notice that $\langle g \rangle \triangleleft \langle g, h \rangle \triangleleft G$. Let $k = |\langle g, h \rangle|$. By Lagrange's Theorem, $|g| = |\langle g \rangle|$ divides $k$ which in turn divides $|G| = 2\,|g|$. So $k$ is a multiple of $|g|$ and $|g| \leq k \leq 2\,|g|$. Then $k$ must be either $|g|$ or $2\,|g|$.

If $k = |g|$, then $\langle g \rangle = \langle g, h \rangle$, so $h \in \langle g \rangle$, so $h = g^n$ for some $n \in \mathbb{Z}$.

If $k = 2\,|g|$, then $\langle g, h \rangle = G$.

(c) (5 pts) **Extra credit problem.** Do part (b) assuming $p\,|g| = |G|$ where $p$ is a prime.

Let $m = |g|$. Then $|G| = pm$. Notice that $\langle g \rangle \triangleleft \langle g, h \rangle \triangleleft G$. Since $|\langle g \rangle| = m$, Lagrange's Theorem says $m \mid |\langle g, h \rangle|$. So $|\langle g, h \rangle| = km$. Also by Lagrange, $km \mid |G| = pm$, so $k \mid p$. Hence $k = 1, p$.

If $k = 1$, then $\langle g \rangle = \langle g, h \rangle$, so $h \in \langle g \rangle$, so $h = g^n$ for some $n \in \mathbb{Z}$.

If $k = p$, then $\langle g, h \rangle = G$.

*Remark:* Part (b) is of course a special case of part (c), so I could have just given this second proof and it would have taken care of both. But I didn't expect you to come up with this slightly more sophisticated proof right away without looking at the special case first.