

SOLUTIONS FOR ASSIGNMENT 1, M6390 FALL 08

- (1) Group homomorphisms were defined in the notes as structure-preserving maps. However, the definition contains a redundancy. Prove that the multiplication-preserving property of a group homomorphism implies the following:

- (a) $f(e_G) = e_H$
 (b) for all $g \in G$, $f(g^{-1}) = (f(g))^{-1}$

Solution: Since $f(e_G) = f(e_G e_G) = f(e_G)f(e_G)$, $f(e_G)$ is an identity element for H . By uniqueness of identity elements, $f(e_G) = e_H$. Since $\forall g \in G$ we have $e_H = f(e_G) = f(gg^{-1}) = f(g)f(g^{-1})$, $f(g^{-1})$ is the (unique) inverse of $f(g)$.

- (2) Prove that for any finite group G and any $g \in G$, there exists $n \in \mathbf{N}^+$ such that $g^n = 1$. (Note: the smallest such n is called the *order* of g , and is denoted $|g|$).

Solution: If G is finite, $\{g^p\}_{p \in \mathbf{N}}$ is a finite set. Thus there must be $q > p$ such that $g^q = g^p$. Then $g^{q-p} = e$, and $q - p > 0$.

- (3) Prove the following:

Proposition (The Subgroup Criterion). : *A subset H of a group G is a subgroup if and only if*

- (a) H is non-empty.
 (b) For all $h_1, h_2 \in H$, $h_1 h_2^{-1} \in H$.

Furthermore, if H is finite then it suffices to show that H is non-empty and closed under multiplication.

Solution: If $H \leq G$, then H has at least one element e . $h_2 \in H$ implies $h_2^{-1} \in H$ and if also $h_1 \in H$ then by multiplication $h_1 h_2^{-1} \in H$. Conversely, if h is any element in (non-empty) H , then $hh^{-1} = e_H \in H$. Then also $e_H h^{-1} = h^{-1} \in H$. Finally, if $h_1, h_2 \in H$, then $h_1(h_2^{-1})^{-1} = h_1 h_2 \in H$. Thus $H \leq G$.

If G is finite then for any $h \in H$ such that $h \neq e$ there exists $n > 1$ such that $h^n = e$. Then h^{n-1} , which is an element of H by closure under multiplication, is equal to h^{-1} . Thus if H is non-empty and closed under multiplication, it is closed under inverses. Thus $H \leq G$.

- (4) Prove that the orbits of a group action partition a group G into equivalence classes as described in Proposition 1.11 in the notes.

Solution: need to show \sim is reflexive, transitive and symmetric. Since $e \cdot x = x$, $x \sim x$. If $y \sim x$ then $y = g \cdot x$ for some $g \in G$. Thus $x = g^{-1} \cdot y$.

If additionally $z \sim y$, then $z = g' \cdot y$ for some $g' \in G$. Thus $z = g' \cdot g \cdot x = (g'g) \cdot x$.

- (5) The *center* $Z(G)$ of a group G is the set of elements that commute with every element in G . Prove the following:
- $Z(G)$ is a normal subgroup of G .
 - Action of G on itself by conjugation is a faithful action iff $Z(G) = \{e\}$.

Solution: Since $e \in Z(G)$, $Z(G)$ is nonempty. If $z_1, z_2 \in Z(G)$ Then for all $g \in G$, $z_1 z_2^{-1} g = z_1 z_2^{-1} g z_2 z_2^{-1} = z_1 z_2^{-1} z_2 g z_2^{-1} = z_1 g z_2^{-1} = g z_1 z_2^{-1} \rightarrow (z_1 z_2^{-1}) \in Z(G)$. By the subgroup criterion, $Z(G) \leq G$. Furthermore, for all $z \in Z(G)$ and all $g \in G$ we have $gzg^{-1} = zgg^{-1} = z$. Thus $Z(G)$ is normal in G .

For part two the action is faithful iff for any $g \in G$ such that $g \neq e$, there exists $x \in G$ such that $g \cdot x \neq e \cdot x$, i.e. $gxg^{-1} \neq x \leftrightarrow gx \neq xg$. This in turn is equivalent to the statement that $g \notin Z(G)$.

- (6) Let $\phi : G \rightarrow H$ be a surjective homomorphism. Prove the following:
- For each $h \in H$, $\phi^{-1}(h)$ is a coset of $\ker(\phi)$.
 - The quotient group of G by $\ker\phi$ is isomorphic to H .

Solution: Let $g_1, g_2 \in G$ Then $g_1 = g_2(g_2^{-1}g_1)$. $\phi(g_1) = \phi(g_2)$ iff $\phi(g_2^{-1}g_1) = \phi(g_2^{-1})\phi(g_1) = \phi(g_1)^{-1}\phi(g_1) = e$ iff $g_2^{-1}g_1 \in \ker(\phi)$ iff g_1 and g_2 are in the same coset.

We've just shown the quotient map is a bijection. Let g_1 and g_2 be coset representatives. Then $\phi([g_1][g_2]) = \phi([g_1g_2]) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = \phi([g_1])\phi([g_2])$. Thus the quotient map is a homomorphism.

- (7) We required both $e * s = s$ and $s * e = e$ in the definition of a monoid. Give an example of a semigroup which is not a monoid, but has a *right identity*, i.e. $s * e = s$ for all $s \in S$.

Solution: Correct solutions given were either of the form: 2×2 matrices of the form $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$, with right identity $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ or a binary operation on an arbitrary set S with at least two elements such that for all $s_1, s_2 \in S$, $s_1 * s_2 = s_1$. In this case, every element is a right identity!

- (8) The the groups D_4 and Q_8 have eight elements. Prove that they aren't isomorphic.

Q_8 is defined as follows. As a set, $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$. 1 is the identity element. $-1 * -1 = 1$ and for $x \in \{i, j, k\}$, $-x = -1 * x = x * -1$. Finally, we have the following table (which should be read such that $i * j = k$):

	i	j	k
i	-1	k	-j
j	-k	-1	i
k	j	-i	-1

Solution: Count the number of elements of various orders. Isomorphic groups should give identical results, but these groups don't.