MA541 Midterm

Solutions

1. Let G and G' be groups, and let $f\colon G \to G'$ be a homomorphism. This means that $f(gh) = f(g)f(h)$ for all $g, h \in G$. Let K be the subset of elements of G which map to the identity of G' under f. Show that K is a subgroup of G.

   Solution. Let e and e' be the identity elements of G and G', respectively. Since $e = e^2$, we have $f(e) = f(e^2) = f(e)^2$; canceling shows that $f(e) = e'$. Thus $e \in K$. Now suppose $g, h \in K$, so that $f(g) = f(h) = e$; then $f(gh) = f(g)f(h) = (e')^2 = e'$, so $gh \in K$. Finally, suppose $g \in K$, then $e = gg^{-1}$, and therefore $e' = f(e) = f(g)f(g^{-1}) = e'f(g^{-1}) = f(g^{-1})$, so that $g^{-1} \in K$. We have shown that K contains the identity, is closed under the operation of G, and contains inverses. Therefore it is a subgroup.

2. Let g be an element of a group G. Show that the map $f\colon G \to G$ defined by $f(x) = g^{-1}xg$ is an automorphism (meaning an isomorphism of G with itself).

   Solution. Let us check that f is a bijection. First we check that it is injective. If $x, y \in G$ with $f(x) = f(y)$, it means that $g^{-1}xg = g^{-1}yg$. Canceling g^{-1} from the left and g on the right gives $x = y$. For surjectivity, let $x \in G$. If $y = gxg^{-1}$, then $f(y) = g^{-1}gxg^{-1}g = x$.

   Now let us check that f is a homomorphism. For $x, y \in G$ we have $f(x)f(y) = g^{-1}xgg^{-1}yg = g^{-1}xyg = f(xy)$.

3. Let g and h be elements in a group. Show that gh has the same order as hg. (Don't neglect the case that the order of these elements could be infinite.)

   Solution 1. Let e be the identity of the group. Let us show that if $n \in \mathbb{Z}$, then $(gh)^n = e$ if and only if $(hg)^n = e$. Since the order of an element is the least positive such n (as is defined to be ∞ if such an n does not exist), this would show that the orders of gh and hg are equal. So we assume that $(gh)^n = e$. This means that $ghgh \cdots gh = e$, where there are n copies of gh. Multiplying on the left by g^{-1} and on the right by g, we see that $hghg \cdots hg = e$, so that $(hg)^n = e$. The reverse direction is similar.

   Solution 2. Let G be the group in question, and let $f\colon G \to G$ be the map $f(x) = g^{-1}xg$. The previous problem shows that f is an isomorphism of G

with itself. We have $f(gh) = hg$. Since order is a structural property, and isomorphisms preserve structural properties, the order of gh must equal the order of hg.

4. Let G be a group with at least two elements which has no subgroups other than itself and the trivial subgroup. Show that G is a cyclic group whose order is a prime number.

   Solution. Since G has two distinct elements we may assume there is an $a \in G$ other than the identity. Thus $\langle a \rangle$ is a subgroup of G which is not the trivial subgroup. By hypothesis we have $G = \langle a \rangle$, so that G is cyclic. G cannot have infinite order, because then $G \cong \mathbb{Z}$, and this has many nontrivial proper subgroups (for instance $2\mathbb{Z}$). If G has order n, then $n \geq 2$; let p be a prime divisor of n. We have seen that cyclic groups have subgroups of every order dividing n, so in particular G has a subgroup of order p. But by hypothesis this subgroup must be all of G. Thus $n = p$ is prime.

5. Let H be a subgroup of the symmetric group S_n for some $n \geq 1$. Show that either all the elements of H are even, or else exactly half of the elements of H are even.

   Solution. We will show that if H has at least one odd element, then exactly half the elements of H are odd. Let $K \subset H$ be the subset of elements which are even. Let τ be an odd element of H, so that $\tau \notin K$. We claim that H is the disjoint union of the cosets K and τK. If $\sigma \in H$ does not belong to K, then σ is odd, but then $\tau^{-1}\sigma$ is even, so that $\tau^{-1}\sigma \in K$, and therefore $\sigma \in \tau K$. Thus $H = K \cup \tau K$. But since cosets have equal cardinality, we have $|K| = |H|/2$.

6. Let g and h be elements of an abelian group. Let m be the order of g and let n be the order of h. Assume that m and n are relatively prime. Show that $\langle g, h \rangle = \langle gh \rangle$.

   Solution. For the inclusion $\langle gh \rangle \subset \langle g, h \rangle$, it is enough to show that $gh \in \langle g, h \rangle$. But this is clear because gh is a product of powers of g and h.

   For the other inclusion $\langle g, h \rangle \subset \langle gh \rangle$, it is enough to show that g and h both belong to $\langle gh \rangle$. Since m and n are relatively prime, there exist $x, y \in \mathbb{Z}$ with $mx + ny = 1$. Then $(gh)^{mx} = g^{mx}h^{mx} = h^{mx} = h^{1-ny} = hh^{-ny} = h$. This shows that $h \in \langle gh \rangle$. The argument for g is similar.