MATH 100A: Homework #5

Due on November 9, 2023 at 12:00pm

Professor McKernan

Section A02 5:00PM - 5:50PM
Section Leader: Castellano

Source Consulted: Textbook, Lecture, Discussion

Ray Tsai
A16848188

Problem 1

Determine in each of the part if the given mapping is a homomorphism. If so, identify its kernal and whether or not the mapping is 1-1 or onto.

(a) $G = \mathbb{Z}$ under $+$, $G' = \mathbb{Z}_n$, $\phi(a) = [a]$ for $a \in \mathbb{Z}$.

Proof. Let $a, b \in \mathbb{Z}$. Since $\phi(a)\phi(b) = [a] + [b] = [a + b] = \phi(ab)$, ϕ is indeed a homomorphism. The kermal of ϕ is the set of elements $a \in G$ such that $\phi(a) = [0]$, namely Ker $\phi = \{a \in G \mid a = kn, k \in \mathbb{Z}\}$. Since Ker ϕ is not trivial, ϕ is not a 1-1 mapping. Lastly, ϕ is obviously onto, as for all $[a] \in \mathbb{Z}_n$ we have $\phi(a) = [a]$. $\square$

(b) G group, $\phi : G \to G$ defined by $\phi(a) = a^{-1}$ for $a \in G$.

Proof. Let $a, b \in G$. Since $\phi(a)\phi(b) = a^{-1}b^{-1} = (ba)^{-1} \neq (ab)^{-1} = \phi(ab)$, ϕ is not a homomorphism unless G is abelian. $\square$

(c) G abelian group, $\phi : G \to G$ defined by $\phi(a) = a^{-1}$ for $a \in G$.

Proof. We already know ϕ is a homomorphism, from part b. The kernal of ϕ is simply $\{e\}$ because e is the only element that has e as its inverse, and so ϕ is a 1-1 mapping. Since for all $c \in G$, we have $\phi(c^{-1}) = c$, ϕ is also onto. $\square$

(d) G group of all non-zero real numbers under multiplication, $G' = \{1, -1\}$, $\phi(r) = 1$ if r is positive, $\phi(r) = -1$ if r is negative.

Proof. Let $a, b \in G$. If a, b has the same sign, we know both ab and $\phi(a)\phi(b)$ are positive, and so $\phi(a)\phi(b) = 1 = \phi(ab)$. The converse also holds true, as both ab and $\phi(a)\phi(b)$ are negative, which implies $\phi(a)\phi(b) = -1 = \phi(ab)$. Thus, ϕ is indeed a homomorphism. The kernal of ϕ is the set of all non-zero real numbers that get map to 1, which contains all positive real numbers. Thus, ϕ is not a 1-1 mapping. However, since we can map 1 and -1 to themselves from G to G' respectively, ϕ is onto. $\square$

(e) G and abelian group, $n > 1$ a fixed integer, and $\phi : G \to G$ defined by $\phi(a) = a^n$ for $a \in G$.

Proof. Let $a, b \in G$. Since G is abelian, $\phi(a)\phi(b) = a^n b^n = (ab)^n = \phi(ab)$, and so ϕ is a homomorphism. The kernal of ϕ is the set of elements $a \in G$ such that $a^n = e$, which means that the order of a must divide n for a to be in Ker ϕ. Thus, ϕ is not injective unless $o(a) \nmid n$ for all a. Also, we claim that ϕ is not onto. Consider a group of order 2, namely $G = \{e, a\}$, and let $n = 2$. G is obviously abelian. Notice that $n = |G|$, so $\phi(g) = e$ for all $g \in G$. This implies that there does not exist g such that $\phi(g) = a$, which implies that ϕ is not onto. $\square$

Problem 2

Verify that in Example 9 of Section 1, the set $H = \{i, g, g^2, g^3\}$ is a normal subgroup of G, the dihedral group of order 8.

Proof. We first prove that $gf = fg^{-1}$. Note that since $e = g^4$, $g^{-1} = g^3 = (y, -x)$. On LHS, we have

$$(g * f)(x, y) = g(f(x, y)) = g(-x, y) = (-y, -x).$$

On RHS, we have

$$(f * g^{-1})(x, y) = f(g^3(x, y)) = f(y, -x) = (-y, -x),$$

and thus $g * f = f * g^{-1} = (-y, -x)$.

We then show that $g^n f = fg^{-n}$ by induction. The base case $gf = fg^{-1}$ is done above. For $n > 1$, we get

$$g^n f = g(g^{n-1} f) = (gf)g^{-(n-1)} = fg^{-n}, \tag{1}$$

by induction.

Let $a = f^i g^j f^{-i} \in f^i H f^{-i}$. We can assume $f^i = f$, otherwise $a = ig^j i = g^j \in H$, and we are done. By the result we proved above, $a = fg^j f^{-1} = g^j ff^{-1} = g^j \in H$. Thus, we know $f^i H f^{-i} \subset H$.

Let $b = f^k g^l \in G$. Then, we know $bg^j b^{-1} = f^k g^l g^j g^{-l} f^{-k} = f^k g^j f^{-k} \in f^i H f^{-i} \subset H$, and thus we know H is a normal subgroup of G. ☐

Problem 3

Prove that if $Z(G)$ is the center of G, then $Z(G) \lhd G$.

Proof. Let $z \in Z(G)$ and $g \in G$. We know $zg = gz$, and so $gzg^{-1} = z \in Z(G)$. Thus, $gZ(G)g^{-1} \subset Z(G)$ for all g, and we are done. $\square$

Problem 4

If $N \lhd G$ and $M \lhd G$ and $MN = \{mn \,|\, m \in M, n \in N\}$, prove that MN is a subgroup of G and that $MN \lhd G$.

Proof. We first check that MN is a subgroup of G. Since M, N are normal subgroups, they are non-empty, and so MN is non-empty.

Let $m_1n_1, m_2n_2 \in MN$, where $m_1, m_2 \in M$ and $n_1, n_2 \in N$. Since $N \lhd G$, we know $n_1m_2 = m_2n_1'$, for some $n_1' \in N$. This immediately follows that $(m_1n_1)(m_2n_2) = m_1(m_2n_1')n_2 = mn$, for some $m = m_1m_2 \in M$ and $n = n_1'n_2 \in N$, and thus MN is closed under multiplication.

Since $N \lhd G$, $(m_1n_1)^{-1} = n_1^{-1}m_1^{-1} = m_1^{-1}n' \in MN$, for some $n' \in N$. Thus, MN is closed under inverse, and so MN is indeed a subgroup of G.

We now prove that $MN \lhd G$ Let $gmng^{-1} \in gMNg^{-1}$, where $g \in G$, $m \in M$, and $n \in N$. Since $N, M \lhd G$, $gmng^{-1} = gmg^{-1}n' = gg^{-1}m'n' = m'n' \in MN$, for some $m' \in M$ and $n' \in N$. Thus, $gMNg^{-1} \subset MN$, and this completes the proof. $\square$

Problem 5

Let $G = S_3$, the symmetric group of degree 3 and let $H = \{i, f\}$, where $f(x_1) = x_2, f(x_2) = x_1, f(x_3) = x_3$.

(a) Write down all the left cosets of H in G.

Proof. We know $S_3 = \{a, b, c, d, f, i\}$, where

$$\begin{aligned} a &= (1,2,3) & b &= (1,3,2) & c &= (2,3) \\ d &= (1,3) & f &= (1,2) & i &= (). \end{aligned}$$

Then, the left cosets of H are $iH = \{i, f\}, aH = \{a, d\}, bH = \{b, c\}$. □

(b) Write down all the right cosets of H in G.

Proof. The right cosets are $Hi = \{i, f\}, Ha = \{a, c\}, Hb = \{b, d\}$. □

(c) Is every left coset of H a right coset of H?

Proof. No. $aH \neq Ha$. □

Problem 6

Let G be a group such that all subgroups of G are normal in G. If $a, b \in G$, prove that $ba = a^j b$ for some j.

Proof. Since $\langle a \rangle$ is a subgroup of G and all subgroups of G are normal, $bab^{-1} \in \langle a \rangle$, and so $bab^{-1} = a^j$ for some j. This immediately follows that $ba = a^j b$. $\square$

Problem 7

If G is a group and $a \in G$, define $\sigma_a : G \to G$ by $\sigma_a(g) = aga^{-1}$. We saw in Example 9 in this section that σ_a is an isomorphism of G onto itself, so $\sigma_a \in A(G)$, the group of all 1-1 mappings of G (as a set) onto itself. Define $\psi : G \to A(G)$ by $\psi(a) = \sigma_a$ for all $a \in G$. Prove that:

(a) ψ is a homomorphism of G into $A(G)$.

Proof. Let $a, b \in G$. Since $\psi(a)\psi(b) = \sigma_a \circ \sigma_b(g) = (ab)g(b^{-1}a^{-1}) = \psi(ab)$, ψ is a homomorphism. □

(b) Ker $\psi = Z(G)$, the center of G.

Proof. Note that the identity elemtnt of $A(G)$ is the identity mapping $\sigma_e(g) = g$. Let $a \in$ Ker ψ. Then $\sigma_a(g) = aga^{-1} = g$. This immediately follows that $ag = ga$, for all $g \in G$, and so $a \in Z(G)$, which implies Ker $\psi \subset Z(G)$. Let $b \in Z(G)$. Since $bg = gb$ for all $g \in G$, we know $\sigma_b = bgb^{-1} = g$, so $Z(G) \subset$ Ker ψ. Therefore, we conclude that Ker $\psi = Z(G)$. □

Problem 8

Let θ, ψ be automorphism of G, and let $\theta\psi$ be the product of θ and ψ as mappings on G. Prove that $\theta\psi$ is an automorphism of G, and that θ^{-1} is an automorphism of G, so that the set of all automorphisms of G is itself a group.

Proof. Let $a, b \in G$. We first show that the set of all automorphisms of G is closed under multiplication. We know

$$\theta\psi(a)\theta\psi(b) = \theta(\psi(a))\theta(\psi(b)) = \theta(\psi(a)\psi(b)) = \theta(\psi(ab)) = \theta\psi(ab),$$

so $\theta\psi$ is a homomorphism. This immediately follows that since θ and ψ are bijective mappings, their composition $\theta\psi$ is also bijective, which makes $\theta\psi$ an automorphism. Since $\theta : G \to G$ is a bijective mapping, there exists a bijective mapping $\theta^{-1} : G \to G$, such that $\theta\theta^{-1}(g) = \theta^{-1}\theta(g) = g$. Thus, θ^{-1} is also an automorphism, and this completes the proof. $\square$

Problem 9

If G is a nonabelian group of order 6, prove that $G \simeq S_3$.

Proof. We first show that there must exists an element in G that is of order 2. Let $G = \{e, a, b, c, d, f\}$, where e is the identity element. By Lagrange's Theorem, we know the orders of the elements in G must be one of $1, 2, 3, 6$. Notice that G is nonabelian, so G is not a cyclic group, which implies that no element in G is of order 6. Suppose for the sake of contradiction that there are no elements in G that are of order 2. Then, each of the non-identity elements in G must have an order of 3. Suppose without loss of generality that $c = a^2$ and $d = b^2$. We investigate on f^2. f^2 cannot be a, otherwise $c = a^2 = f^4 = f$. f^2 cannot be c, otherwise $a = a^4 = c^2 = f^4 = f$. The same arguments apply for b and d, and thus we reach a contradiction. Suppose that f is the element of order 2 in G. Let $H = \{e, f\}$ be the cyclic subgroup of G, and let $S = \{Hk \mid k \in G\}$ be the set of all right cosets of H in G. Define, for $g \in G$, $T_g : S \to S$ by $T_g(Hk) = Hkg^{-1}$. Notice that since $|S| = [G : H] = 3$, $A(S) \simeq S_3$. For $m, n \in G$, we know $T_m T_n(Hk) = T_m(Hkn^{-1}) = Hkn^{-1}m^{-1} = Hk(mn)^{-1} = T_{mn}(Hk)$, and so the function $\psi : G \to A(S) \simeq S_3$ defined by $\psi(g) = T_g$ is a homomorphism. We now show that ψ is injective by investigating its kernal. Suppose that $l \in \text{Ker } \psi$. Then $\psi(l) = T_l = T_e$. This implies that $Hl^{-1} = T_l(H) = T_e(H) = H$, and so $l \in H$. Consider $T_l(Hk)$, for some $k \neq f$. $T_l(Hk) = Hkl^{-1} = Hk$, and so $klk^{-1} \in H$. Suppose for the sake of contradiction that $l = f$. $kfk^{-1} \neq e$, otherwise we get $f = e$, contradiction. Thus we can assume $kfk^{-1} = f$, namely $kf = fk$. Notice that since $\langle f, k \rangle$ contains a subgroup H of order 2, by Lagrange's Theorem it must have even order, and so $\langle f, k \rangle$ is of order 6 and thus it generates G. However, since f and k commute, $\langle f, k \rangle = G$ is abelian, contradiction. Therefore, we know $kfk^{-1} \notin H$, and so $l = e$. It immediately follows that ψ is injective since Ker ψ is trivial, and this completes the proof. □

Problem 10

If G is the group of all nonzero real numbers under multiplication and N is the subgroup of all positive real numbers, write out G/N by exhibiting the cosets of N in G, and construct the multiplication in G/N.

Proof. Since multiplication is commutative for real numbers, $gN = Ng$ for all $g \in G$, and thus N is normal. Notice that $gN = N$ if g is positive and $gN = -N$, the set of all negative real numbers, if g is negative. Thus, $G/N = \{N, -N\} = \{[1], [-1]\}$, where $[g] = \{x \in G \mid xg^{-1} \in N\}$. Since N is normal in G, G/N is relative to the operation $[a][b] = [ab]$, for $a, b \in G$. $\square$

Problem 11

If G is the group of nonzero real numbers under multiplication and $N = \{1, -1\}$, show how you can "identify" G/N as the group of all positive real numbers under multiplication. What are the cosets of N in G?

Proof. Since multiplication is commutative for real numbers, $gN = Ng$ for all $g \in G$, and thus N is normal. Notice that $gN = \{g, -g\}$, which implies that numbers of the same absolute value are put into the same calss, namely $G/N = \{[a] \mid a \in R_{>0}\}$. Since N is normal in G, G/N is relative to the operation $[a][b] = [ab]$, for $a, b \in G$, and this makes G/N the group of all positive real numbers under multiplication. The cosets of N in G is simply all the elements in G/N by definition. $\square$

Problem 12

If G is a group and $N \lhd G$, show that if $\bar{M}$ is a subgroup of G/N and $M = \{a \in G \mid Na \in \bar{M}\}$, then M is a subgroup of G, and $N \subset M$.

Proof. Let $a, b \in M$. We know $Na, Nb \in \bar{M}$. Since N is normal and $\bar{M}$ is a subgroup, $NaNb = N(ab) \in M$, so $ab \in M$. Thus, M is closed under multiplication. Since N is the identity element in G/N, we know $N \in \bar{M}$, and so there exists $Nc \in \bar{M}$ such that $NaNc = Nac = N$. This immediately follows that there exists $n' \in N$ such that $n'ac = e$, and so we get $a^{-1} = cn'$. We can easily check that $a^{-1} \in M$, as $Na^{-1} = Ncn' = Nc \in \bar{M}$. Thus, M is also closed under taking inverse, and so M is indeed a subgroup of G. We already know $N \in \bar{M}$, so if $n \in N$, then $Nn = N \in \bar{M}$, and thus $N \subset M$. $\square$

Problem 13

If $\bar{M}$ in Problem 3 is normal in G/N, show that the M defined is normal in G.

Proof. Let $m \in M$ and $g \in G$. Since $\bar{M}$ is normal in G/N, $NgNmNg^{-1} = N(gmg^{-1}) \in \bar{M}$, and thus $gmg^{-1} \in M$. Therefore, M is normal in G. $\square$