Sam Tay
Professor Milnikiel
Math 335
Section 13: 4, 6, 19, 22, 37, 39, 47, 52, 53
12/23/11

Problem 4: Let $\phi : \mathbb{Z}_6 \to \mathbb{Z}_2$ be defined by $\phi(x) = x \pmod 2$. To see that ϕ is a homomorphism, let $a, b \in \mathbb{Z}_6$ and compute

$$\phi(a +_6 b) = (a + b \mod 6) \pmod 2$$

$$\begin{aligned} \phi(a) +_2 \phi(b) &= (a \mod 2) + (b \mod 2) \pmod 2 \\ &= a + b \pmod 2. \end{aligned}$$

Therefore, to show that $\phi(a +_6 b) = \phi(a) +_2 \phi(b)$, we must show

$$a + b \pmod 6 \equiv_2 a + b.$$

Using the Divisor Theorem to express $a + b = 6m + r$, where $0 \leq r < 6$, we see that $a + b \pmod 6 = r$. Now

$$a + b \equiv_2 6m + r \equiv_2 2(3m) + r \equiv_2 r,$$

which completes the proof.

Problem 6: Let $\phi : \mathbb{R} \to \mathbb{R}^*$, where $\mathbb{R}$ is additive and $\mathbb{R}^*$ is multiplicative, be given by $\phi(x) = 2^x$. To see that ϕ is a homomorphism, we let $x, y \in \mathbb{R}$ and compute

$$\phi(x + y) = 2^{x+y} = 2^x 2^y = \phi(x)\phi(y).$$

Problem 19: We have a group homomorphism $\phi : \mathbb{Z} \to S_8$ such that $\phi(1) = (1, 4, 2, 6)(2, 5, 7)$. Note that $(1, 4, 2, 6)(2, 5, 7) = (1, 4, 2, 5, 7, 6)$, from which it is clear that $|\phi(1)| = 6$. This means that $i = \phi(1)^6 = \phi(6)$, where i is the identity permutation and the second equality follows from the homomorphism property. However, we know that for any $n \in \mathbb{Z}$, we have $i^n = i$. Thus

$$i = \phi(6)^n = \phi(6n)$$

for all $n \in \mathbb{Z}$, and since 6 is the least such positive integer, $\ker \phi = 6\mathbb{Z}$. Now to compute $\phi(20)$, we use the previous assertions to find

$$\phi(20) = \phi(6 \cdot 3 + 2) = \phi(6)^3 \phi(2) = i^3 \phi(2) = \phi(2).$$

It is easy to see that

$$\phi(20) = \phi(2) = (1, 4, 2, 5, 7, 6)(1, 4, 2, 5, 7, 6) = (1, 2, 7)(4, 5, 6).$$

Problem 22: We have a group homomorphism $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ such that $\phi(1,0) = 3$ and $\phi(0,1) = -5$. Then $(z_1, z_2) \in \ker \phi$ if and only if $\phi(z_1, z_2) = 0$, where

$$\phi(z_1, z_2) = \phi\big((z_1, 0) + (0, z_2)\big) = \phi(z_1, 0) + \phi(0, z_2),$$

and with $z_1 + z_2$ applications of the homomorphism property,

$$\phi(z_1, z_2) = z_1\phi(1,0) + z_2\phi(0,1) = 3z_1 - 5z_2.$$

Therefore

$$\ker \phi = \{(z_1, z_2) \in \mathbb{Z} \times \mathbb{Z} : 3z_1 = 5z_2\}.$$

From above, we see that $\phi(-3, 2) = 3(-3) - 5(2) = -19$.

Problem 37: Let $\phi : \mathbb{Z}_3 \to S_3$ be defined by

$$\phi(n) = \begin{cases} i & \text{if } n = 0 \\ (1,2,3) & \text{if } n = 1 \\ (1,3,2) & \text{if } n = 2 \ . \end{cases}$$

The homomorphism property is obviously satisfied for operations involving the identity 0, so let us check the cases with $1, 2 \in \mathbb{Z}_3$. We have

$$\phi(1)\phi(2) = (1,2,3)(1,3,2) = i = \phi(0) = \phi(1+2)$$
$$\phi(2)\phi(1) = (1,3,2)(1,2,3) = i = \phi(0) = \phi(2+1)$$
$$\phi(1)\phi(1) = (1,2,3)(1,2,3) = (1,3,2) = \phi(2) = \phi(1+1)$$
$$\phi(2)\phi(2) = (1,3,2)(1,3,2) = (1,2,3) = \phi(1) = \phi(2+2),$$

and indeed ϕ is a nontrivial homomorphism.

Problem 39: Define $\phi : \mathbb{Z}\times\mathbb{Z} \to 2\mathbb{Z}$ by $\phi(z_1, z_2) = 2(z_1+z_2)$. For $(x_1, y_1), (x_2, y_2) \in \mathbb{Z} \times \mathbb{Z}$, we have

$$\phi\big((x_1, y_1) + (x_2, y_2)\big) = \phi(x_1 + x_2, y_1 + y_2) = 2(x_1 + x_2 + y_1 + y_2),$$

and

$$\phi(x_1, y_1) + \phi(x_2, y_2) = 2(x_1 + y_1) + 2(x_2 + y_2) = 2(x_1 + x_2 + y_1 + y_2),$$

and thus ϕ is a nontrivial homomorphism.

Problem 47: If $\phi : G \to G'$ is a group homomorphism and $|G|$ is prime, then ϕ is trivial or one-to-one.

Proof. Since $|G|$ is finite, $|\phi[G]|$ is a finite divisor of $|G|$ by Exercise 44. Since $|G|$ is prime, this means $|\phi[G]| = 1$ or $|\phi[G]| = |G|$. We know $e' \in \phi[G]$ so in the former case, ϕ is trivial. In the latter case, if $|G|$ distinct elements map to $|G|$ distinct elements, clearly ϕ is one-to-one (if not, then we would have $|\phi[G]| < |G|$). $\square$

Problem 52: Let $\phi : G \to G'$ be a homomorphism with kernel H and let $a \in G$. Then $\{x \in G : \phi(x) = \phi(a)\} = Ha$.

Proof. ($\subseteq$) Suppose $x \in G$ such that $\phi(x) = \phi(a)$. Then $\phi(x)\phi(a)^{-1} = e'$ and by Theorem 13.12, $\phi(a)^{-1} = \phi(a^{-1})$. It follows then by the homomorphism property that $e' = \phi(x)\phi(a^{-1}) = \phi(xa^{-1})$. Therefore xa^{-1} is in the kernel such that $xa^{-1} = h$ for some $h \in H$. Since G is a group, $x = ha$ and we conclude $x \in Ha$.

($\supseteq$) Next suppose $x \in Ha$, such that $x = ha$ for some $h \in H$. Then

$$\phi(x) = \phi(ha) = \phi(h)\phi(a) = e'\phi(a) = \phi(a),$$

so $x \in \{x \in G : \phi(x) = \phi(a)\}$, and this completes the proof. $\square$

Problem 53: Let G be a group with $h, k \in G$ and define $\phi : \mathbb{Z} \times \mathbb{Z} \to G$ by $\phi(m, n) = h^m k^n$. Then ϕ is a homomorphism if and only if $hk = kh$.

Proof. ($\Leftarrow$) Suppose $hk = kh$. Then for all $n, m \in \mathbb{Z}$, $h^m k^n = k^n h^m$. To see this, first note that

$$h^m k = h^{m-1}hk = h^{m-1}kh = h^{m-2}hkh = h^{m-2}kh^2 = \cdots = kh^m.$$

Using this result, we find similarly that

$$h^m k^n = h^m k k^{n-1} = kh^m k^{n-1} = kh^m k k^{n-2} = k^2 h^m k^{n-2} = \cdots = k^n h^m.$$

Now let $m_1, n_1, m_2, n_2 \in \mathbb{Z}$ and we have

$$\begin{aligned} \phi(m_1, n_1)\phi(m_2, n_2) &= h^{m_1} k^{n_1} h^{m_2} k^{n_2} = h^{m_1} h^{m_2} k^{n_1} k^{n_2} \\ &= h^{m_1+m_2} k^{n_1+n_2} = \phi(m_1 + m_2, n_1 + n_2) \\ &= \phi\big((m_1, n_1) + (m_2, n_2)\big). \end{aligned}$$

Therefore ϕ is a homomorphism.

($\Rightarrow$) Next suppose ϕ as defined above is a homomorphism. Then for any $m_1, n_1, m_2, n_2 \in \mathbb{Z}$ we must have $\phi(m_1, n_1)\phi(m_2, n_2) = \phi\big((m_1, n_2) + (m_2, n_2)\big)$, where

$$\phi(m_1, n_1)\phi(m_2, n_2) = h^{m_1} k^{n_1} h^{m_2} k^{n_2}$$
$$\phi\big((m_1, n_1) + (m_2, n_2)\big) = \phi(m_1 + m_2, n_1 + n_2) = h^{m_1+m_2} k^{n_1+n_2}.$$

Then

$$h^{m_1} k^{n_1} h^{m_2} k^{n_2} = h^{m_1} h^{m_2} k^{n_1} k^{n_2},$$

and since G is a group, left and right cancellation gives

$$k^{n_1} h^{m_2} = h^{m_2} k^{n_1}.$$

Since this must hold for all integers, it must hold for $n_1 = m_2 = 1$, so that $hk = kh$. $\square$

Questions from the Unstarred Problems

Problem 24: Would the answer change if the permutations $\phi(1,0)$ and $\phi(0,1)$ were not independent cycles (and therefore did not commute)? As the problem is written, I found

$$\ker\phi = \{(2n, 4m) : n, m \in \mathbb{Z}\},$$

which follows because $|\phi(1,0)| = 2$ and $|\phi(0,1)| = 4$. My thinking is that it wouldn't change the image $\phi^{-1}[\{i\}] = \ker\phi$, but that ϕ would no longer be a homomorphism... is that right?

Problem 26: For a function $\phi : \mathbb{Z} \to \mathbb{Z}$, suppose $\phi(1) = a$. Then $\phi(z) = az$ for all $z \in \mathbb{Z}$ and ϕ is a homomorphism. Since a was arbitrary, there are countably infinitely many homomorphisms from $\mathbb{Z}$ into $\mathbb{Z}$.

Problem 32 (a): Is A_n a normal subgroup of S_n? I would think not, but only because the elements of A_n don't generally commute with the rest of S_n. Is there a better reason?

Problem 32 (j): Is it possible to have a nontrivial homomorphism of a finite group into an infinite group? I think you could if the elements were sent to some finite subgroup of the codomain. Perhaps a function $\phi : \mathbb{Z}_n \to U$, where U is the infinite set of complex numbers of unit magnitude, but the $\operatorname{Ran}\phi = U_n$.

Problem 33: I don't think it's possible to have a nontrivial homomorphism, but I have trouble showing it. I think, in regards to Problem 4, we would need

$$a + b \pmod{12} \equiv_5 a + b,$$

and using the Divisor Theorem to write $a + b = 12m + r$, we need

$$a + b \equiv_5 12m + r \equiv_5 r,$$

but if $m|5$ then this can hold. Then it follows that for all $c \in \mathbb{Z}_{12}$, we must have $c = 60n + r$ for some $n, r \in \mathbb{Z}$. However can't we choose representatives for $\mathbb{Z}_{12}$ to make this possible? I'm confused.

Problem 34: If we define $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_4$ by $\phi(a) = a \pmod 4$, do we have a homomorphism?

Problem 35: Define $\phi : \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_5$ by $\phi(z_1, z_2) = (z_1, 0)$, then ϕ is a homomorphism.

Problem 36: There are no nontrivial homomorphisms from $\mathbb{Z}_3$ into $\mathbb{Z}$ because if $\phi(1) = z$, then

$$3z = z + z + z = \phi(1) + \phi(1) + \phi(1) = \phi(0) = 0,$$

such that $z = 0$. It follows that $\operatorname{Ran}\phi = 0$.

Problem 41: This took me forever to figure out. I feel that there must be a better way to think about these problems; don't really have any intuition for questions like these. I think, however, that we can define a nontrivial homomorphism $\phi : D_4 \to S_3$ by defining the function as follows:

$$\phi(x) = \begin{cases} i & \text{if } x \text{ is } \rho_0, \rho_1, \rho_2, \text{ or } \rho_3 \\ (1,2) & \text{if } x \text{ is } \mu_1, \mu_2, \delta_1, \text{ or } \delta_2. \end{cases}$$

Does that look good to you?

Problem 42: For $\phi : S_3 \to S_4$, can we just send $\phi(\sigma) = \sigma$, such that the fourth element of S_4 is left alone?

Problem 51: Let G be a group and $a \in G$. Then $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$ is a homomorphism. This is easy enough to show, but in exploring the properties of the kernel, do I have these things correct:

1. $\operatorname{Ran} \phi = \langle a \rangle$.
2. If $\ker \phi = \{0\}$ then $\langle a \rangle$ is infinite.
3. If $z \in \ker \phi$ then $kz \in \ker \phi$ for all $k \in \mathbb{Z}$.