Algebra Solutions by Richard

Chapter 10: Homomorphisms and Factor Groups

5. Are the following homomorphisms? If so, state their kernels.

(b) $\varphi : \mathbb{R} \to \mathrm{GL}_2(\mathbb{R})$, defined by $\varphi(a) = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$.

Observe that $\varphi(a+b) = \begin{pmatrix} 1 & 0 \\ a+b & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} = \varphi(a)\varphi(b)$. In other words, we've shown $\varphi(a+b) = \varphi(a)\varphi(b)$, so **YES**, φ is a homomorphism.

The kernel is $\left\{x \in \mathbb{R} : \varphi(x) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\} = \boxed{\{0\}.}$

(d) $\varphi : \mathrm{GL}_2(\mathbb{R}) \to \mathbb{R}^*$, defined by $\varphi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = ad - bc$.

Notice that this is just $\varphi(A) = \det(A)$. We know from linear algebra that $\det(AB) = \det(A)\det(B)$, so $\varphi(AB) = \det(AB) = \det(A)\det(B) = \varphi(A)\varphi(B)$. In summary we've shown $\varphi(AB) = \varphi(A)\varphi(B)$, so φ is indeed a homomorphism.

The kernel is the set of all matrices with determinant 1, that is, $\boxed{\text{the kernel is } \mathrm{SL}_2(\mathbb{R}).}$

(e) $\varphi : M_2(\mathbb{R}) \to \mathbb{R}$, defined by $\varphi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = b$.

Notice that $\varphi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}\right) = b+b' = \varphi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) + \varphi\left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right)$. In other words, we have $\varphi(A+B) = \varphi(A) + \varphi(B)$, so φ is indeed a homomorphism.

Its kernel is $\boxed{\ker(\varphi) = \left\{\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{R}\right\}.}$

9. Describe all of the homomorphisms from $\mathbb{Z}_{24}$ to $\mathbb{Z}_{18}$.

In class we talked about how if a cyclic group $G = \langle a \rangle$ has generator a, then any homomorphism $f : G \to H$ is completely determined by the element $f(a) = b \in H$, since for any element $a^k \in G$ we have $f(a^k) = f(a)^k = b^k$. In particular this means that if homomorphisms $f, g : G \to H$ satisfy $f(a) = g(a)$ (that is, if they agree on the generator a), then $f = g$.

In the setting of the current problem, the element $a = 1$ generates $\mathbb{Z}_{24}$, and we cannot have any more than 18 homomorphisms $f : \mathbb{Z}_{24} \to \mathbb{Z}_{18}$, because there are potentially 18 different values for $f(1)$.

However, for some of these 18 choices of $b \in \mathbb{Z}_{18}$, there may not be a homomorphism f with $f(1) = b$. The following lemma will help us out here.

Lemma. Suppose $G = \langle a \rangle$ is a finite cyclic group generated by a, and let H be an arbitrary group. Then there is a homomorphism $f : G \to H$ with $f(a) = b \in H$ if and only if the order of b (in H) divides $|G|$.

Proof. ($\Rightarrow$) Suppose that G and H are as stated and $f : G \to H$ is a homomorphism. Set $b = f(a)$. Notice that

$$\langle b \rangle = \{b^k : k \in \mathbb{Z}\} = \{f(a)^k : k \in \mathbb{Z}\} = \{f(a^k) : k \in \mathbb{Z}\} = f(\langle a \rangle) = f(G).$$

Therefore the map $f : G \to \langle b \rangle$ is simply $f : G \to f(G)$, and this is a surjective homomorphism. Consequently, the First Homomorphism Theorem gives $G/\ker(f) \cong \langle b \rangle$. Then $|G/\ker(f)| = |\langle b \rangle|$, which means $\frac{|G|}{|\ker(f)|} = |\langle b \rangle|$, or rather $|G| = |\langle b \rangle| \cdot |\ker(f)|$. Therefore the order of b divides $|G|$.

(⇐) Suppose the order of b divides $|G|$. We will construct a homomorphism $f : G \to H$ satisfying $f(a) = b$. First we show that the function $f : G \to H$ defined as $f(a^k) = b^k$ for each $k \in \mathbb{Z}$ is well-defined. For this we must show that if $a^k = a^\ell$, then $f(a^k) = f(a^\ell)$. Thus suppose $a^k = a^\ell$. Then $a^{k-\ell} = e_G$, so $k - \ell$ is a multiple of $|\langle a \rangle| = |G|$, that is $k - \ell = m|G|$ for some integer G. But also the order of b divides $|G|$, so $b^{|G|} = e_H$. This means $b^k b^{-\ell} = b^{k-\ell} = b^{m|G|} = (b^{|G|})^m = e_H^m = e_H$. From $b^k b^{-\ell} = e_H$, we get $b^k = b^\ell$, that is $f(a^k) = f(a^\ell)$. Therefore f is well-defined.

Finally, f is a homomorphism because for any $x, y \in G$ we have $x = a^m$ and $y = a^n$ for some integers m and n, and therefore $f(xy) = f(a^m a^n) = f(a^{mn}) = b^{mn} = b^m b^n = f(a^m)f(a^n) = f(x)f(y)$. ■

Now we can apply the lemma to solve the problem. The lemma says that whenever $G = \langle a \rangle$ and $b \in H$ is such that its order divides $|G|$, the map $f(a^k) = b^k$ is a homomorphism $f : G \to K$. Moreover any homomorphism $g : G \to H$ must have this form.

In the current situation we have $G = \mathbb{Z}_{24} = \langle 1 \rangle$, and the above paragraph implies every homomorphism $f : \mathbb{Z}_{24} \to \mathbb{Z}_{18}$ has form $f(k \cdot 1) = k \cdot b$, where $b \in \mathbb{Z}_{18}$ has an order that divides $|G| = 24$. Thus the number of homomorphisms from $\mathbb{Z}_{24}$ to $\mathbb{Z}_{18}$ equals the number of elements in $\mathbb{Z}_{18}$ whose order divides 24.

Recall the following homework problem from several weeks back: It lists the order of every element of $\mathbb{Z}_{18}$: The table is made with the aid of Theorem 4.6. Since $a = 1$ is a generator of $\mathbb{Z}_{18}$ the theorem asserts that any $b = k \cdot a = k \cdot 1 = k \in \mathbb{Z}_{18}$ has order $\frac{18}{\gcd(k,18)}$.

element $b \in \mathbb{Z}_{18}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
order of b	1	18	9	6	9	18	3	18	9	2	9	18	3	18	9	6	9	18

There are six elements of $\mathbb{Z}_{18}$ whose orders divide 24. They are 0,3,6,9,12 and 15.
Thus There are six homomorphisms from $\mathbb{Z}_{24}$ to $\mathbb{Z}_{18}$.

26. **(c)** Recall that the *center* of a group is the set $Z(G) = \{x \in G : xg = gx \text{ for all } g \in G\}$. Show that this is a normal subgroup of G.

Proof. Take an arbitrary element $g \in G$. We have to show $gZ(G) = Z(G)g$. This can be done simply as follows: we use the fact that $xg = gx$ for any $x \in Z(G)$.

$$\begin{aligned} gZ(G) &= \{gx : x \in Z(G)\} && \text{(by definition of the left coset } gZ(G)) \\ &= \{xg : x \in Z(G)\} && \text{(because } x \in Z(G)) \\ &= Z(G)g && \text{(by definition of the right coset } Z(G)g) \end{aligned}$$

This completes the proof. ■

32. Suppose $\varphi : G \to H$ is a group homomorphism. Prove φ is injective if and only if $\varphi^{-1}(e_H) = \{e_G\}$.

Proof. Notice that $\ker(\varphi) = \{x \in G : \varphi(x) = e_H\} = \varphi^{-1}(e_H)$, so we are being asked to prove that φ is injective if and only if $\ker(\varphi) = \{e_G\}$.

(⇒) Suppose φ is injective. We know that $\varphi(e_G) = e_H$, as this is a standard property of homomorphisms. But since φ is injective, for any $x \neq e_G$, we must have $\varphi(x) \neq \varphi(e_G)$, or $\varphi(x) \neq e_H$. Thus $e_G \in G$ is the only element of G that φ sends to $e_H \in H$. This means $\ker(\varphi) = \{e_G\}$.

(⇐) Suppose $\ker(\varphi) = \{e_G\}$. To show φ is injective, we must show $\varphi(x) = \varphi(y)$ implies $x = y$. Thus suppose $\varphi(x) = \varphi(y)$. Now left-multiply both sides of this equation by $\varphi(y^{-1})$. We get

$$\varphi(y^{-1})\varphi(x) = \varphi(y^{-1})\varphi(y),$$

and this becomes $\varphi(y^{-1}x) = \varphi(y^{-1}y)$, which is $\varphi(y^{-1}x) = \varphi(e_G)$, or $\varphi(y^{-1}x) = e_H$. This means $y^{-1}x \in \ker(\varphi) = \{e_G\}$, so $y^{-1}x = e_G$, which yields $x = y$. Therefore φ is injective.