Section 3.5

Problem # 7

Find an isomorphism ϕ from the additive group $\mathbb{Z}$ to the multiplicative group

$$H = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \middle| n \in \mathbb{Z} \right\}$$

Solution

Let $\phi : \mathbb{Z} \to H$ be defined as

$$\phi(x) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$$

Part (a)

It is clear that ϕ is both one to one and onto.

Part (b)

$$\begin{aligned} \phi(n)\phi(m) &= \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & n+m \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & m+n \\ 0 & 1 \end{bmatrix} \\ &= \phi(n+m) \end{aligned} \tag{1}$$

So ϕ preserves the operation. Therefore ϕ is an isomorphism from $\mathbb{Z}$ to H.

Problem # 30

For an arbitrary positive integer n, prove that any two cyclic groups of order n are isomorphic.

Solution

Let $A = \langle a \rangle$ be some cyclic group of order n and $\phi : \mathbb{Z}_n \to A$ defined by $\phi([x]) = a^x$. We know that $a^x = a^{[x]}$ because although there are many members of the equivalence class, they are all congruent to $x \mod n$. This is clearly a bijection because A is cyclic. Then for any $[x], [y] \in \mathbb{Z}_n$

$$\begin{aligned} \phi([x])\phi([y]) &= a^{[x]}a^{[y]} \\ &= a^{[x]+[y]} \\ &= \phi([x]+[y]) \end{aligned} \tag{2}$$

So ϕ preserves the operation and A and $\mathbb{Z}_n$ are isomorphic. So any cyclic group of order n is isomorphic to $\mathbb{Z}_n$ and thus by the transitive property, any two cyclic groups of the same order are isomorphic to each other.

Problem # 31

Prove that any infinite cyclic group is isomorphic to $\mathbb{Z}$ under addition.

Solution

Let G be the an infinite cyclic group defined by $\langle a \rangle$ and let $\phi : \mathbb{Z} \to G$ be defined by $\phi(x) = a^x$. ϕ is clearly both one to one and onto. Then

$$\begin{aligned} \phi(x)\phi(y) &= a^x a^y \\ &= a^{x+y} \\ &= \phi(x+y) \end{aligned} \tag{3}$$

So ϕ preserves the operation and G is isomorphic to $\mathbb{Z}$ under addition.

Problem # 32

Let H be the group $\mathbb{Z}_6$ under addition. Find all isomorphisms from the multiplicative group $\mathbb{U}_7$ of units in $\mathbb{Z}_7$ to H.

Solution

For a a mapping to be an isomorphism it must map the identity element of the first group to the identity element of the second. Therefore we know that in all isomorphisms $\phi : \mathbb{U}_7 \to H$, $\phi([1]) = [0]$. We also know that inverses must map to inverses. The element [6] is the only element in $\mathbb{U}_7$ that is its own inverse so it must map to [3], the only element in H that is its own inverse. We also know that the generators of $\mathbb{U}_7$ must map to the generators of H. Therefore $\phi([5])$ and $\phi([3])$ must map to either [1] or [5]. The remaining elements have no constraints. Therefore all isomorphisms can be listed as:

$\phi([1]) = [0]$	$\phi([1]) = [0]$	$\phi([1]) = [0]$	$\phi([1]) = [0]$
$\phi([2]) = [2]$	$\phi([2]) = [4]$	$\phi([2]) = [2]$	$\phi([2]) = [4]$
$\phi([3]) = [1]$	$\phi([3]) = [1]$	$\phi([3]) = [5]$	$\phi([3]) = [5]$
$\phi([4]) = [4]$	$\phi([4]) = [2]$	$\phi([4]) = [4]$	$\phi([4]) = [2]$
$\phi([5]) = [5]$	$\phi([5]) = [5]$	$\phi([5]) = [1]$	$\phi([5]) = [1]$
$\phi([6]) = [3]$	$\phi([6]) = [3]$	$\phi([6]) = [3]$	$\phi([6]) = [3]$

Section 3.6

Problem # 16

Suppose that G, G', and G'' are groups. If G' is a homomorphic image of G, and G'' is a homomorphic image of G', prove that G'' is a homomorphic image of G. (Thus the relation in Exercise 15 has the transitive property.

Solution

According to the given information there exist epimorphisms $\phi_1 : G \to G'$ and $\phi_2 : G' \to G''$. Let $\phi_3 = \phi_2 \circ \phi_1$.

Part (a)

By Theorem 1.16 regarding the composition of onto mappings we know that $\phi_2 \circ \phi_1 : G \to G''$ is onto.

Part (b)

For $x, y \in G$,

$$\begin{aligned} \phi_3(x)\phi_3(y) &= \phi_2(\phi_1(x))\phi_2(\phi_1(y)) \\ &= \phi_2(\phi_1(x)\phi_1(y)) \\ &= \phi_2(\phi_1(xy)) \\ &= \phi_3(xy) \end{aligned} \tag{4}$$

Therefore the mapping $\phi_3 : G \to G''$ is an epimorphism because it is both onto and preserves operation. Thus G'' is a homomorphic image of G.

Problem # 18

Suppose that ϕ is an epimorphism from the group G to a group G'. Prove that ϕ is an isomorphism if and only if $\ker \phi = \{e\}$, where e denotes the identity in G.

Solution

Part (a)

Let ϕ be an isomorphism. We know that $e \in \ker \phi$. Assume that there is another element x of G that is also in $\ker \phi$. This means that for $x \neq e, \phi(x) = \phi(e) = e$. This means that ϕ is not one-to-one and is therefore not an isomorphism. Therefore, if ϕ is an isomorphism, $\ker \phi = \{e\}$.

Part (b)

Let $\ker \phi = \{e\}$. Assume there are two elements in G such that $\phi(x) = \phi(y)$. We know that either $x = y = e$ or that $\phi(x)$ and $\phi(y)$ are not equal to e or x and y would be members of $\ker \phi$.

$$\begin{aligned} \phi(x^{-1})\phi(y) &= \phi(x^{-1}y) \\ \phi(x)^{-1}\phi(y) &= \phi(x^{-1}y) \\ \phi(y)^{-1}\phi(y) &= \phi(x^{-1}y) \\ e &= \phi(x^{-1}y) \end{aligned} \tag{5}$$

We know that e is the only member of $\ker \phi$ so $x^{-1}y = e$. Then x^{-1} is the inverse of both x and y. Inverses are unique so $x = y$. Therefore ϕ is an isomorphism.

Problem # 19

Let ϕ be a homomorphism from a group G to a group G'. Prove that $\ker \phi$ is a subgroup of G.

Solution

Part (a)

$e \in \ker \phi$ so $\ker \phi$ is not empty and contains the identity element.

Part (b)

For two elements $x, y \in \ker \phi$

$$\begin{aligned} \phi(x)\phi(y) &= \phi(xy) \\ e \cdot e &= \phi(xy) \\ e &= \phi(xy) \end{aligned} \tag{6}$$

Therefore $xy \in \ker \phi$ and $\ker \phi$ is closed.

Part (c)

For any $x \in \ker \phi$, $\phi(x^{-1}) = \phi(x)^{-1}$.

$$\begin{aligned} e &= \phi(x)^{-1} \\ &= \phi(x^{-1}) \end{aligned} \tag{7}$$

Therefore $x^{-1} \in \ker \phi$ and $\ker \phi$ contains inverses. Having satisfied the necessary conditions, $\ker \phi$ is a subgroup of G.

Problem # 20

If G is an abelian group and the group G' is a homomorphic image of G, prove that G' is abelian.

Solution

G' is a homomorphic image of G so any elements a, b in G' can be represented as $\phi(x), \phi(y)$ for some $x, y \in G$. Therefore

$$\begin{aligned} ab &= \phi(x)\phi(y) \\ &= \phi(xy) \\ &= \phi(yx) \\ &= \phi(y)\phi(x) \\ &= ba \end{aligned} \tag{8}$$

Therefore G' is abelian.

Problem # 23

Assume that ϕ is a homomorphism from the group G to the group G'.

- Prove that if H is any subgroup of G, then $\phi(H)$ is a subgroup of G'.
- Prove that if K is any subgroup of G', then $\phi^{-1}(K)$ is a subgroup of G.

Solution

- (a) $e \in H$ and $\phi(e) = e$ so $\phi(H)$ is nonempty and contains the identity element.

  (b) Any $a, b \in \phi(H)$ can be written as $\phi(x), \phi(y)$ for $x, y \in H$. So

  $$\begin{aligned} ab &= \phi(x)\phi(y) \\ &= \phi(xy) \end{aligned} \tag{9}$$

  H is closed so xy is in H. Therefore ab is in $\phi(H)$ and $\phi(H)$ is closed.

  (c) Any $a \in \phi(H)$ can be written as $\phi(x)$ for some $x \in H$. Then

  $$\begin{aligned} a^{-1} &= \phi(x)^{-1} \\ &= \phi(x^{-1}) \end{aligned} \tag{10}$$

  H is a group so x^{-1} must be an element of H and thus a^{-1} is an element of $\phi(H)$. So $\phi(H)$ contains inverses. Having satisfied all the necessary conditions, $\phi(H)$ is a subgroup of G'.

- (a) $e \in K$ and $\phi^{-1}(e) = e$ so $\phi^{-1}(K)$ is nonempty and contains the identity element.

  (b) Any $a, b \in \phi^{-1}(K)$ can be written as $\phi(x), \phi(y)$ for $x, y \in K$. So

  $$\begin{aligned} ab &= \phi^{-1}(x)\phi^{-1}(y) \\ &= \phi^{-1}(xy) \end{aligned} \tag{11}$$

  K is closed so xy is in K. Therefore ab is in $\phi^{-1}(K)$ and $\phi^{-1}(K)$ is closed.

(c) Any $a \in \phi^{-1}(K)$ can be written as $\phi^{-1}(x)$ for some $x \in K$. Then

$$\begin{aligned} a^{-1} &= \phi^{-1}(x)^{-1} \\ &= \phi^{-1}(x^{-1}) \end{aligned} \tag{12}$$

K is a group so x^{-1} must be an element of K and thus a^{-1} is an element of $\phi^{-1}(K)$. So $\phi(K)$ contains inverses. Having satisfied all the necessary conditions, $\phi^{-1}(K)$ is a subgroup of G.