CHAPTER 4

Group Homomorphisms and Isomorphisms

Consider the groups $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_{10}^*, \cdot)$. They have the group tables below.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	1	7	9	3
1	1	7	9	3
7	7	9	3	1
9	9	3	1	7
3	3	1	7	9

Note that for the group table on the right, we have deliberately permuted the elements of $\mathbb{Z}_{10}^*$ in order to highlight the similarity between the two groups. Indeed, if we match the elements $0, 1, 2, 3$ of $\mathbb{Z}_4$ respectively with the elements $1, 7, 9, 3$ of $\mathbb{Z}_{10}^*$, then although the two groups look different, they are "essentially the same".

4.1. Formal Definition

DEFINITION. Suppose that $(G, *)$ and $(H, \circ)$ are groups. A function $\phi : G \to H$ is said to be a group homomorphism if the following condition is satisfied:

(HOM) For every $x, y \in G$, $(x * y)\phi = x\phi \circ y\phi$.

DEFINITION. Suppose that $(G, *)$ and $(H, \circ)$ are groups. A function $\phi : G \to H$ is said to be a group isomorphism if the following conditions are satisfied:

(IS1) $\phi : G \to H$ is a group homomorphism.
(IS2) $\phi : G \to H$ is one-to-one.
(IS3) $\phi : G \to H$ is onto.

DEFINITION. We say that two groups G and H are isomorphic if there exists a group isomorphism $\phi : G \to H$.

EXAMPLES. (1) $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_{10}^*, \cdot)$ are isomorphic. To see this, define $\phi : \mathbb{Z}_4 \to \mathbb{Z}_{10}^*$ by taking $0\phi = 1$, $1\phi = 7$, $2\phi = 9$ and $3\phi = 3$.

(2) $(\mathbb{Z}_2, +)$ and $(\{\pm 1\}, \cdot)$ are isomorphic. To see this, define $\phi : \mathbb{Z}_2 \to \{\pm 1\}$ by taking $0\phi = 1$ and $1\phi = -1$.

(3) It is not difficult to show that $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$ are groups. Here $\mathbb{R}^+$ denotes the set of positive real numbers. These two groups are isomorphic. To see this, define $\phi : \mathbb{R} \to \mathbb{R}^+$ by writing $x\phi = \mathrm{e}^x$ for every $x \in \mathbb{R}$. Then ϕ is a group homomorphism, as $\mathrm{e}^{x+y} = \mathrm{e}^x \mathrm{e}^y$ for every $x, y \in \mathbb{R}$. On the other hand, it is well known that the exponential function is a one-to-one and onto function from $\mathbb{R}$ to $\mathbb{R}^+$.

(4) The set

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\},$$

together with matrix multiplication, forms a group. This group is isomorphic to $(\mathbb{Z}_4, +)$. To see this, define $\phi : G \to \mathbb{Z}_4$ to send the four matrices above to $0, 1, 2, 3$ respectively.

(5) The set

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\},$$

together with matrix multiplication, forms a group. This group is isomorphic to $(\mathbb{Z}_8^*, \cdot)$. To see this, define $\phi : G \to \mathbb{Z}_8^*$ to send the four matrices above to $1, 3, 5, 7$ respectively.

(6) Suppose that G is an abelian group, and let $n \in \mathbb{Z}$. Define $\phi : G \to G$ by writing $x\phi = x^n$ for every $x \in G$. Then ϕ is clearly a group homomorphism from G to itself. For every $x, y \in G$, we clearly have $(xy)\phi = (xy)^n = x^n y^n = (x\phi)(y\phi)$.

(7) Consider the multiplicative group $\mathcal{M}_{2,2}^*(\mathbb{R})$ of invertible 2×2 matrices with entries in $\mathbb{R}$. Consider also the set $\mathbb{R} \setminus \{0\}$; this forms a group under multiplication. Now define a function $\phi : \mathcal{M}_{2,2}^*(\mathbb{R}) \to \mathbb{R} \setminus \{0\}$ by writing $A\phi = \det(A)$, the determinant of A, for every matrix $A \in \mathcal{M}_{2,2}^*(\mathbb{R})$. This is clearly a group homomorphism, since $\det(AB) = \det(A)\det(B)$ for every $A, B \in \mathcal{M}_{2,2}^*(\mathbb{R})$.

(8) This is an example we almost take for granted. Consider the groups $(\mathbb{Z}, +)$ and $(\mathbb{Z}_4, +)$. We define a function $\phi : \mathbb{Z} \to \mathbb{Z}_4$ as follows. For every $n \in \mathbb{Z}$, we can clearly write $n = 4q + r$, where $q, r \in \mathbb{Z}$ and $0 \leqslant r < 4$. It is well known that for given n, the integers q and r are uniquely determined. Now let $n\phi = r$. So, for example, $4\phi = 0$, $707\phi = 3$ and $(-22)\phi = 2$. It can easily be shown that $\phi : \mathbb{Z} \to \mathbb{Z}_4$ is a group homomorphism. This is called reduction modulo 4.

(9) Similarly, for every $n \in \mathbb{N} \setminus \{1\}$, reduction modulo n is a group homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_n$.

4.2. Some Properties of Homomorphisms

PROPOSITION 4.1. *Suppose that $(G, *)$ and $(H, \circ)$ are groups, with identity elements e_G and e_H respectively. Suppose further that $\phi : G \to H$ is a group homomorphism. Then $e_G\phi = e_H$.*

PROOF. Simply note that $e_G\phi = (e_G * e_G)\phi = e_G\phi \circ e_G\phi$. ◯

THEOREM 4.2. *Suppose that $(G, *)$ and $(H, \circ)$ are groups, and that $\phi : G \to H$ is a group homomorphism. Then the set*

$$G\phi = \{x\phi : x \in G\}$$

is a subgroup of H.

DEFINITION. Suppose that $(G, *)$ and $(H, \circ)$ are groups, and that $\phi : G \to H$ is group homomorphism. Then the set $G\phi$ is called the image of the group homomorphism.

PROOF OF THEOREM 4.2. Clearly $G\phi$ is non-empty. Let $x\phi, y\phi \in G\phi$. In view of Theorem 1.5, it suffices to show that $x\phi \circ (y\phi)' \in G\phi$. Clearly $y'\phi \in G\phi$. Since ϕ is a homomorphism, we must have $y\phi \circ y'\phi = (y * y')\phi = e_G\phi = e_H$ by Proposition 4.1. Similarly $y'\phi \circ y\phi = (y' * y)\phi = e_G\phi = e_H$. It follows that $(y\phi)' = y'\phi$, so that $x\phi \circ (y\phi)' = x\phi \circ y'\phi = (x * y')\phi \in G\phi$, as required. ◯

EXAMPLE. Suppose that we do not know that

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\} \tag{4.1}$$

forms a group under matrix multiplication. We can remedy this in the following way if we know that $(\mathbb{Z}_4, +)$ is a group. We define a function $\phi : \mathbb{Z}_4 \to \mathcal{M}_{2,2}^*(\mathbb{R})$ by writing

$$0\phi = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad 1\phi = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad 2\phi = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad 3\phi = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix};$$

note Example (4) above. We then show that ϕ is a homomorphism from the group $(\mathbb{Z}_4, +)$ to the group $\mathcal{M}_{2,2}^*(\mathbb{R})$, and deduce our desired result by using Theorem 4.2 to conclude that (4.1) is a subgroup of $\mathcal{M}_{2,2}^*(\mathbb{R})$.

This simple example suggests the following improvement of our idea. To be precise, we do not need the knowledge that H, given by $\mathcal{M}_{2,2}^*(\mathbb{R})$ in this special example, is a group.

PROPOSITION 4.3. *Suppose that $(G, *)$ is a group, and that $\circ$ is a binary operation on a set S. Suppose further that the function $\phi : G \to S$ satisfies the condition that $(x * y)\phi = x\phi \circ y\phi$ for every $x, y \in G$. Then the set $G\phi = \{x\phi : x \in G\}$, together with the binary operation $\circ$, forms a group.*

SKETCH OF PROOF. All we need to do is to show that $(G\phi, \circ)$ forms a group. However, we already know that $(G, *)$ is a group. We can therefore use the property, that $(x * y)\phi = x\phi \circ y\phi$ for every $x, y \in G$, to "bring the group structure over" from G to $G\phi$. ◯

DEFINITION. Suppose that $(G, *)$ and $(H, \circ)$ are groups, and that $\phi : G \to H$ is group homomorphism. Suppose further that e_H is the identity element in H. Then the set

$$\ker \phi = \{x \in G : x\phi = e_H\}$$

is called the kernel of the group homomorphism.

EXAMPLES. (1) As in Example (8) above, consider the groups $(\mathbb{Z}, +)$ and $(\mathbb{Z}_4, +)$, and the group homomorphism reduction modulo 4. The kernel of this group homomorphism is clearly the set $\{4x : x \in \mathbb{Z}\}$.

(2) Consider the group $(\mathbb{Z}_{10}^*, \cdot)$. Define $\phi : (\mathbb{Z}_{10}^*, \cdot) \to (\mathbb{Z}_{10}^*, \cdot)$ by writing $x\phi = x^2$ for every $x \in \mathbb{Z}_{10}^*$. It can easily be shown that this is a group homomorphism. Furthermore, $\ker \phi = \{1, 9\}$.

(3) Suppose that G is a finite group of order n. Show that the function $\phi : G \to G$, defined by $x\phi = x^n$ for every $x \in G$, is a group homomorphism and that $\ker \phi = G$.

THEOREM 4.4. *Suppose that $(G, *)$ and $(H, \circ)$ are groups, and that $\phi : G \to H$ is a group homomorphism. Then $\ker \phi$ is a subgroup of G.*

PROOF. Clearly $e \in \ker \phi$. Let $x, y \in \ker \phi$. In view of Theorem 1.5, it clearly suffices to show that $x * y' \in \ker \phi$. Since ϕ is a homomorphism, we must have

$$y'\phi = e_H \circ y'\phi = y\phi \circ y'\phi = (y * y')\phi = e_G\phi = e_H$$

by Proposition 4.1. It follows that $(x * y')\phi = x\phi \circ y'\phi = e_H \circ e_H = e_H$, as required. ◯

Using an argument similar to the proof of Lagrange's theorem, we can prove the following result.

PROPOSITION 4.5. *Suppose that $(G, *)$ and $(H, \circ)$ are groups, and that $\phi : G \to H$ is a group homomorphism. Suppose further that G is finite. Then $|G\phi|$ divides $|G|$.*

PROOF. Define a relation $\mathcal{R}$ on G in the following way. For every $x, y \in G$, $x\mathcal{R}y$ if $x\phi = y\phi$. It is not difficult to check that $\mathcal{R}$ is an equivalence relation, and that $\ker \phi$ is one of the equivalence classes. Furthermore, the number of equivalence classes is $|G\phi|$. Suppose now that K is one of the equivalence classes. Let $a \in K$. For every $x \in \ker \phi$, we have $(a * x)\phi = a\phi \circ x\phi = a\phi \circ e_H = a\phi$, so that $(a * x)\mathcal{R}a$, whence $a * x \in K$. We now define $f : \ker \phi \to K$ by writing $f(x) = a * x$ for every $x \in \ker \phi$. Then clearly f is one-to-one, in view of left cancellation. To show that f is onto, note that for any $y \in K$, $(a' * y)\phi = a'\phi \circ y\phi = a'\phi \circ a\phi = e_H$, so that $a' * y \in \ker \phi$. Clearly $f(a' * y) = y$. It now follows that K and $\ker \phi$ have the same number of elements. Hence all the equivalence classes have the same number of elements, so that $|G| = |G\phi||\ker \phi|$. ◯

4.3. Normal Subgroups

For the rest of this chapter, we shall use multiplicative notation throughout. Note, however, that some of these results will be quoted in additive notation in Chapter 7.

DEFINITION. Suppose that G is a group. Then a subgroup N of G is said to be normal if the following condition is satisfied:

(N) For every $n \in N$ and every $x \in G$, $x'nx \in N$.

EXAMPLES. (1) Check that A_3 is a normal subgroup of S_3.

(2) Both $\{e\}$ and G are normal subgroups of G.

(3) If G is abelian, then every subgroup of G is normal in G.

PROPOSITION 4.6. *Suppose that G and H are groups, and that $\phi : G \to H$ is a group homomorphism. Then $\ker \phi$ is a normal subgroup of G.*

PROOF. For every $n \in \ker \phi$ and every $x \in G$, we have

$$(x'nx)\phi = x'\phi\, n\phi\, x\phi = x'\phi\, x\phi = (x'x)\phi = e_H,$$

so that $x'nx \in \ker \phi$. ◯

DEFINITION. Suppose that G is a group, and that N is a subgroup of G. Suppose further that $x \in G$.

(i) The set $xN = \{xn : n \in N\}$ is called a left coset of N.
(ii) The set $Nx = \{nx : n \in N\}$ is called a right coset of N.
(iii) The set $x'Nx = \{x'nx : n \in N\}$ is called a conjugate set of N.

THEOREM 4.7. *Suppose that G is a group, and that N is a subgroup of G. Then the following statements are equivalent:*

(i) *N is a normal subgroup of G.*
(ii) *For every $x \in G$, $xN = Nx$.*
(iii) *For every $x \in G$, $x'Nx = N$.*

PROOF. ((i)⇒(ii)) Suppose that $y \in xN$. Then $y = xn$ for some $n \in N$, so that $y = (xnx')x \in Nx$, since $xnx' \in N$. It follows that $xN \subseteq Nx$. Suppose now that $y \in Nx$. Then $y = nx$ for some $n \in N$, so that $y = x(x'nx) \in xN$, since $x'nx \in N$. It follows that $Nx \subseteq xN$.
((ii)⇒(iii)) Note that $x'Nx = x'xN = N$.
((iii)⇒(i)) For every $n \in N$ and $x \in G$, $x'nx \in x'Nx = N$. ◯

PROPOSITION 4.8. *Suppose that G is a group, and that N is a normal subgroup of G. Then for every subgroup K of G, the set $NK = \{nk : n \in N \text{ and } k \in K\}$ is a subgroup of G.*

PROOF. Clearly NK is non-empty. Suppose that $n_1k_1, n_2k_2 \in NK$. In view of Theorem 1.5, it suffices to show that $n_1k_1(n_2k_2)' \in NK$. Now

$$n_1k_1(n_2k_2)' = n_1k_1k_2'n_2' = n_1(k_1k_2')n_2'(k_1k_2')'(k_1k_2').$$

Note that $(k_1k_2')n_2'(k_1k_2')' \in N$, so that $n_1(k_1k_2')n_2'(k_1k_2')' \in N$. Also $k_1k_2' \in K$. It therefore follows that $n_1k_1(n_2k_2)' \in NK$, as required. ◯

In Theorem 4.2 and Proposition 4.5, we have used a homomorphism $\phi : G \to H$ to deduce properties about the group H or its subgroups. Sometimes, information on G can be obtained through the homomorphism from properties of subgroups of H. To do this, we need the idea of a pre-image.

Suppose that $\phi : G \to H$ is a function from a set G to a set H. Then for every set $S \subseteq H$, the pre-image of S under ϕ is the set

$$S\phi^{-1} = \{x \in G : x\phi \in S\}.$$

Note that ϕ^{-1} may not represent the inverse function, as the function $\phi : G \to H$ may not be one-to-one or onto.

PROPOSITION 4.9. *Suppose that G and H are groups, and that $\phi : G \to H$ is a group homomorphism. Then for every subgroup S of H, the pre-image $S\phi^{-1}$ is a subgroup of G. Furthermore, if S is normal in H, then $S\phi^{-1}$ is normal in G.*

PROOF. Obviously $S\phi^{-1}$ is non-empty. Suppose that $x, y \in S\phi^{-1}$. Since S is a subgroup of H, it follows that $(xy')\phi = x\phi\, y'\phi = x\phi(y\phi)' \in S$. Then $xy' \in S\phi^{-1}$, so that $S\phi^{-1}$ is a subgroup of G by Theorem 1.5. Suppose now that $x \in G$ and $n \in S\phi^{-1}$. Then $(x'nx)\phi = x'\phi\, n\phi\, x\phi = (x\phi)'n\phi\, x\phi \in S$ since S is normal in H. Hence $x'nx \in S\phi^{-1}$, so that $S\phi^{-1}$ is normal in G. ◯

4.4. Cosets and Factor Groups

We now return to the study of cosets. The following result has been used implicitly in the proof of Lagrange's theorem as well as in the proof of Proposition 4.5.

PROPOSITION 4.10. *Suppose that G is a group, and that N is a subgroup of G. Suppose further that $x, y \in G$. Then $xN = yN$ if and only if $x'y \in N$. In particular, $xN = N$ if and only if $x \in N$.*

PROOF. Suppose first of all that $xN = yN$. Since $e \in N$, we must have $y = ye \in yN = xN$, so that $y = xn$ for some $n \in N$. Clearly $n = x'y$, so that $x'y \in N$. Suppose now that $x'y \in N$. Write $x'y = n_0$, where $n_0 \in N$. Then $y = xn_0$. Let $z \in yN$. Then $z = yn = xn_0n$, where $n \in N$. Clearly $n_0n \in N$, so that $z \in xN$. Hence $yN \subseteq xN$. On the other hand, since $x'y \in N$, we must also have $y'x = (x'y)' \in N$. A similar argument gives $xN \subseteq yN$. It follows that $xN = yN$. ◯

Our aim is to define a binary operation on the collection of cosets arising from a subgroup N of G. This is in general an impossible task. However, normal subgroups are rather special.

THEOREM 4.11. *Suppose that G is a group, and that N is a normal subgroup of G. Then the multiplication of cosets $xN \cdot yN = (xy)N$ is well defined. In other words, if $x_1, x_2, y_1, y_2 \in G$ and $x_1N = x_2N$ and $y_1N = y_2N$, then $(x_1y_1)N = (x_2y_2)N$.*

PROOF. By Proposition 4.10, $(x_1y_1)N = (x_2y_2)N$ if and only if $(x_1y_1)'(x_2y_2) \in N$. Now

$$(x_1y_1)'(x_2y_2) = y_1'x_1'x_2y_2 = y_1'(x_1'x_2)y_1(y_1'y_2),$$

so it suffices to show that $y_1'(x_1'x_2)y_1 \in N$ and $y_1'y_2 \in N$. As $y_1N = y_2N$, it follows from Proposition 4.10 that $y_1'y_2 \in N$. On the other hand, since $x_1N = x_2N$, it again follows from Proposition 4.10 that $x_1'x_2 \in N$. Since N is normal in G, it now follows that $y_1'(x_1'x_2)y_1 \in N$, as required. ◯

REMARK. An alternative proof of Theorem 4.11 is as follows. We have

$$x_1y_1N = x_1Ny_1 = x_2Ny_1 = x_2y_1N = x_2y_2N.$$

Having obtained a binary operation, we now show that there is a group structure.

THEOREM 4.12. *Suppose that G is a group, and that N is a normal subgroup of G. Then the set*

$$G/N = \{xN : x \in G\}$$

of all left cosets of N, together with multiplication defined by $xN \cdot yN = (xy)N$ for every $x, y \in G$, forms a group.

DEFINITION. The group G/N in Theorem 4.12 is called the factor group G modulo N.

PROOF OF THEOREM 4.12. (G1) is obvious. Also, it follows from the associativity of G that $(xy)z = x(yz)$. (G2) follows. To check (G3), note that $N = eN$ satisfies the requirements for the identity element. To check (G4), note that $x'N$ satisfies the requirements for the inverse element of xN. *bigcirc*

REMARK. A similar result holds for right cosets.

We now exhibit a nice relationship between a group and its factor group by a normal subgroup.

PROPOSITION 4.13. *Suppose that G is a group, and that N is a normal subgroup of G. Then the function $\Phi : G \to G/N$, defined by $x\Phi = xN$ for every $x \in G$, is a group homomorphism. Furthermore, the function $\Phi : G \to G/N$ is onto, and $\ker \Phi = N$.*

DEFINITION. The homomorphism $\Phi : G \to G/N$ in Proposition 4.13 is called the natural homomorphism of G onto G/N.

PROOF OF PROPOSITION 4.13. For every $x, y \in G$, $(xy)\Phi = (xy)N = xN \cdot yN = x\Phi\, y\Phi$ in view of Theorems 4.11 and 4.12. It follows that $\Phi : G \to G/N$ is a group homomorphism. It is clear that $\Phi : G \to G/N$ is onto. The assertion $\ker \Phi = N$ follows from the second part of Proposition 4.10.

To illustrate the importance of this "apparently simple" result, we shall deduce the following result.

PROPOSITION 4.14. *Suppose that G is a finite group, and that N is a normal subgroup of G. Then $|G/N| = |G|/|N|$.*

PROOF. Recall the proof of Proposition 4.5. For any group homomorphism $\phi : G \to H$, where G is finite, we have $|G| = |G\phi||\ker \phi|$. Note that in this particular case, $\ker \Phi = N$ and $G\Phi = G/N$. ◯

4.5. The Fundamental Theorem of Group Homomorphisms

Note that our proof of Proposition 4.14 on factor groups depends on the natural homomorphism Φ onto the factor group in question. This suggests an intimate connection between homomorphisms and factor groups.

Suppose that G and H are groups, and that $\phi : G \to H$ is a group homomorphism. The question is whether there is some normal subgroup N of G such that there is some nice correspondence between the factor group G/N and the subgroup $G\phi$ of H.

We answer this question in the affirmative by proving the following fundamental result.

THEOREM 4.15 (Fundamental theorem of group homomorphisms). *Suppose that G and H are groups, and that $\phi : G \to H$ is a group homomorphism. Then $G/\ker\phi$ is isomorphic to $G\phi$.*

PROOF. For simplicity, write $\ker\phi = N$. Then N is a normal subgroup of G. Define a function $\psi : G/N \to G\phi$ in the following way. For every element $xN \in G/N$, let $(xN)\psi = x\phi$. Then clearly

$$(xN \cdot yN)\psi = (xyN)\psi = (xy)\phi = x\phi\, y\phi$$

for every $xN, yN \in G/N$, so that ψ is a homomorphism. Now, ψ is onto, for every element in $G\phi$ can be written in the form $x\phi$ for some $x \in G$. Take $xN \in G/N$. Then $(xN)\psi = x\phi$. On the other hand, ψ is one-to-one, for if $x, y \in G$ such that $(xN)\psi = (yN)\psi$, then $x\phi = y\phi$, so that $(x'y)\phi = e_H$. It follows that $x'y \in \ker\phi = N$, so that $xN = yN$ by Proposition 4.10. It is now clear that $\psi : G/N \to G\phi$ is an isomorphism. ◯

Problems for Chapter 4

1. For each of the following pairs, state whether the groups are isomorphic, and justify your assertion:

(i) $(\mathbb{Z}_{14}^*, \cdot)$ and $(\mathbb{Z}_6, +)$
(ii) $(\mathbb{Z}_8^*, \cdot)$ and $(\mathbb{Z}_4, +)$

2. Suppose that $\phi : G \to H$ is a group homomorphism, and that $x \in G$ is of finite order. Show that the order of $x\phi$ in H divides the order of x in G. Comment on the case when $\phi : G \to H$ is a group isomorphism.

3. Prove each of the following:

(i) Any infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$.
(ii) Any cyclic group of order $n \geqslant 2$ is isomorphic to $(\mathbb{Z}_n, +)$.
(iii) Suppose that $\phi : G \to H$ is a group homomorphism, and that G is cyclic. Then $G\phi$ is cyclic.

4. Show that isomorphism of groups is an equivalence relation.

5. Consider the groups S_6 and $(\{\pm 1\}, \cdot)$, and consider the function $\phi : S_6 \to \{\pm 1\}$, defined by

$$x\phi = \begin{cases} -1, & \text{if } x \text{ is odd,} \\ 1, & \text{if } x \text{ is even.} \end{cases}$$

Show that ϕ is a group homomorphism. What is $\ker \phi$?

6. Show that each of the following functions $\phi : G \to H$ is a homomorphism, and determine the image and the kernel:

(i) $G = H = (\mathbb{Z}_{16}^*, \cdot)$ and $x\phi = x^4$
(ii) $G = (\mathbb{Z}, +)$, $H = (\mathbb{R} \setminus \{0\}, \cdot)$ and $x\phi = 3^x$

7. Show that there is only one group homomorphism from S_3 to $(\mathbb{Z}_{21}, +)$.
[*Hint*: Note Question 2.]

8. Find all the subgroups of S_3 and determine which of these are normal in S_3.

9. Show that $\{i, (1\ 2\ 3), (1\ 3\ 2)\}$ is a subgroup of S_4 but not a normal subgroup of S_4.

10. Give an example of a group G and subgroups N and K of G such that NK is not a subgroup of G.

11. Suppose that N and K are both normal subgroups of G. Prove that NK is a normal subgroup of G.

12. Suppose that $\phi : G \to H$ is a group homomorphism, and that N is a normal subgroup of G. Prove that $N\phi = \{n\phi : n \in N\}$ is a normal subgroup of $G\phi$.

13. For each of the following factor groups, determine whether the given cosets are equal:

(i) $\mathbb{Z}_{20}^*/\langle 3\rangle$; cosets $7\langle 3\rangle$ and $11\langle 3\rangle$
(ii) $\mathbb{Z}_{20}/\langle 3\rangle$; cosets $7\langle 3\rangle$ and $11\langle 3\rangle$

14. Suppose that G is a finite group, and that N is a normal subgroup of G. Let $x \in G$. Show that the order of xN in G/N is given by n, where n is the smallest natural number satisfying $x^n \in N$.

15. Suppose that G is a cyclic group. Show that for every subgroup N of G, the factor group G/N exists and is cyclic.

16. Suppose that N is a normal subgroup of a group G, and that the factor group G/N is cyclic. Suppose further that $gn = ng$ for every $n \in N$ and every $g \in G$. Show that G is abelian.

17. Prove that every group G of order p^2, where p is a prime, is abelian by following the steps below:

(i) Prove that the centre $Z(G)$ is a normal subgroup of G.
(ii) Determine the possible orders of $Z(G)$.
(iii) Assuming without proof that $|Z(G)| \neq 1$, prove that $|Z(G)| = p^2$.
[*Hint*: Study the factor group $G/Z(G)$, and use Question 16.]

18. Show that for every $n \in \mathbb{N} \setminus \{1\}$, the factor group S_n/A_n is isomorphic to $(\mathbb{Z}_2, +)$.