Exercise 19

1. Compute the inverse of $[3]$ in $(\mathbb{Z}/8\mathbb{Z})^*$.

   Proof.
   We have that $[3] \in (\mathbb{Z}/8\mathbb{Z})^*$ if and only if $\gcd(3,8) = 1$. Since $\gcd(3,8) = 1$, we have that $[3]$ is invertible in $(\mathbb{Z}/8\mathbb{Z})^*$. We can find the inverse of $[3]$ by solving the following equation:

   $$\begin{aligned} [3]x &\equiv [1] \pmod 8 \\ 3x &\equiv 1 \pmod 8 \\ x &\equiv 3^{-1} \pmod 8 \end{aligned}$$

   We can find the inverse of $[3]$ by using the Extended Euclidean Algorithm. We have that:

   $$\begin{aligned} 8 &= 3(2) + 2 \\ 3 &= 2(1) + 1 \end{aligned}$$

   We can now find the inverse of $[3]$ by working backwards:

   $$\begin{aligned} 1 &= 3 - 2(1) \\ &= 3 - (8 - 3(2)) \\ &= 3 - 8 + 6 \\ &= -8 + 9 \\ &= 1 \end{aligned}$$

   Therefore, the inverse of $[3]$ in $(\mathbb{Z}/8\mathbb{Z})^*$ is $[3]^{-1} = [3]$. □

2. Compute the inverse of $[5]$ in $(\mathbb{Z}/13\mathbb{Z})^*$.

   Proof.

   $$\gcd(5, 13) = 1$$

   Since 5 is invertible, we seek b such that:

   $$5b \equiv 1 \mod 13$$

   Using the Extended Euclidean Algorithm:

$$\begin{aligned}
13 &= 2 \cdot 5 + 3 \\
5 &= 1 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

Now, we backtrack:

From the third equation:

$$1 = 3 - 1 \cdot 2$$

Substituting for 2:

$$1 = 3 - 1 \cdot (5 - 1 \cdot 3) = 3 - 5 + 3 = 2 \cdot 3 - 5$$

Substituting for 3:

$$1 = 2 \cdot (13 - 2 \cdot 5) - 5 = 2 \cdot 13 - 4 \cdot 5 - 5 = 2 \cdot 13 - 5 \cdot 5$$

This implies:

$$1 \equiv -5 \cdot 5 \mod 13$$

Thus, the inverse of [5] in $(\mathbb{Z}/13\mathbb{Z})^*$ is:

$$\boxed{[8]}$$

Therefore, the inverse of [5] in $(\mathbb{Z}/13\mathbb{Z})^*$ is $[5]^{-1} = [-2] = [11]$.

□

Exercise 20

Prove that the inverse map of a group isomorphism is also a group homomorphism.

Proof.
Let G and H be groups and let $\phi : G \to H$ be a group isomorphism. We know that ϕ is bijective, so it has an inverse $\phi^{-1} : H \to G$. We want to show that ϕ^{-1} is a group homomorphism. Let $a, b \in H$. We have that:

$$\begin{aligned}
\phi^{-1}(a \cdot b) &= \phi^{-1}(\phi(\phi^{-1}(a)) \cdot \phi(\phi^{-1}(b))) \\
&= \phi^{-1}(\phi(\phi^{-1}(a) \cdot \phi^{-1}(b))) \\
&= \phi^{-1}(a) \cdot \phi^{-1}(b)
\end{aligned}$$

Therefore, ϕ^{-1} is a group homomorphism. □

Exercise 21

Prove that G is abelian if and only if the map $f : G \to G$ given by $f(g) = g^2$ is a group homomorphism.

Proof.
Let G be a group, and define the map $f : G \to G$ by $f(g) = g^2$.

Assume G is abelian. We want to show that f is a homomorphism, i.e., $f(g_1g_2) = f(g_1)f(g_2)$ for all $g_1, g_2 \in G$.

Calculating the left-hand side:

$$f(g_1g_2) = (g_1g_2)^2 = g_1g_2g_1g_2$$

Since G is abelian, we can rearrange the terms:

$$g_1g_2g_1g_2 = g_1g_1g_2g_2 = g_1^2g_2^2$$

Now calculating the right-hand side:

$$f(g_1)f(g_2) = g_1^2g_2^2$$

Thus,

$$f(g_1g_2) = f(g_1)f(g_2)$$

This shows that f is a homomorphism.
now assume f is a homoomorphism

We need to show that G is abelian, i.e., $g_1g_2 = g_2g_1$ for all $g_1, g_2 \in G$.

Using the homomorphism property, we have:

$$f(g_1g_2) = f(g_1)f(g_2)$$

Substituting the definition of f:

$$(g_1g_2)^2 = g_1^2g_2^2$$

Expanding the left-hand side:

$$g_1g_2g_1g_2 = g_1^2g_2^2$$

Rearranging gives:

$$g_1g_2g_1g_2 = g_1g_1g_2g_2$$

Cancelling g_1 from the left (since G is a group and hence has inverses), we can assume:

$$g_2g_1 = g_1g_2$$

This shows $g_1g_2 = g_2g_1$ for all $g_1, g_2 \in G$, confirming that G is abelian. □

Excercise 24

Prove that $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{R})$ has infinite order in the group $GL_2(\mathbb{R})$.

Proof.
Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{R})$. We want to show that A has infinite order in $GL_2(\mathbb{R})$. We have that:

$$\begin{aligned} A^n &= \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n \\ &= \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \end{aligned}$$

We can see that A^n is the identity matrix if and only if $n = 0$. Since there are no positive integers n such that $A^n = I$, we conclude that A has infinite order in $GL_2(\mathbb{R})$.Therefore, A has infinite order in $GL_2(\mathbb{R})$.

□

Exercise 26

Let G be an abelian group, K a group, and $f : G \to K$ a group homomorphism. We want to show that $f(G) \subseteq K$ is an abelian subgroup of K.

Proof.
Let G be an abelian group, K a group, and $f : G \to K$ a group homomorphism. We aim to show that $f(G)$ is an abelian subgroup of K.

To show that $f(G)$ is a subgroup of K, we need to verify that it satisfies the subgroup criteria:

1. e: Since f is a homomorphism and e_G is the identity in G, we have:

$$f(e_G) = e_K,$$

where e_K is the identity in K. Thus, $e_K \in f(G)$.

2. Closures: Let $x, y \in f(G)$. Then there exist $g_1, g_2 \in G$ such that $x = f(g_1)$ and $y = f(g_2)$. Since f is a homomorphism, we have:

$$xy = f(g_1)f(g_2) = f(g_1g_2).$$

Since $g_1g_2 \in G$, it follows that $xy \in f(G)$.

3. inverse Let $x \in f(G)$. Then there exists $g \in G$ such that $x = f(g)$. The inverse of x in K is given by:

$$x^{-1} = f(g)^{-1} = f(g^{-1}).$$

Since $g^{-1} \in G$, we have $x^{-1} \in f(G)$.

Since all three conditions for a subgroup are satisfied, we conclude that $f(G)$ is a subgroup of K.

Let $x, y \in f(G)$. Then there exist $g_1, g_2 \in G$ such that $x = f(g_1)$ and $y = f(g_2)$. Since G is abelian, we have:

$$g_1 g_2 = g_2 g_1.$$

Using the homomorphism property, we get:

$$xy = f(g_1)f(g_2) = f(g_1 g_2) = f(g_2 g_1) = f(g_2)f(g_1) = yx.$$

Thus, $xy = yx$, showing that $f(G)$ is abelian.

Therefore, we conclude that $f(G)$ is an abelian subgroup of K. □

Exercise 28

Prove that $(\mathbb{Z}/13\mathbb{Z})^*$ is a cyclic group by finding a generator.

Proof.
We want to show that $(\mathbb{Z}/13\mathbb{Z})^*$ is a cyclic group by finding a generator. We know that $(\mathbb{Z}/13\mathbb{Z})^*$ is the set of all elements in $\mathbb{Z}/13\mathbb{Z}$ that are relatively prime to 13. We can find a generator for $(\mathbb{Z}/13\mathbb{Z})^*$ by finding an element of order 12. We can find an element of order 12 by checking the orders of the elements in $(\mathbb{Z}/13\mathbb{Z})^*$:

$$\begin{aligned}
[1]^1 &= [1] \\
[2]^1 &= [2] \\
[3]^1 &= [3] \\
[4]^1 &= [4] \\
[5]^1 &= [5] \\
[6]^2 &= [1] \\
[7]^1 &= [7] \\
[8]^2 &= [1] \\
[9]^2 &= [1] \\
[10]^2 &= [1] \\
[11]^2 &= [1] \\
[12]^2 &= [1]
\end{aligned}$$

We can see that [6] is an element of order 12 in $(\mathbb{Z}/13\mathbb{Z})^*$. Therefore, $(\mathbb{Z}/13\mathbb{Z})^*$ is a cyclic group with generator [6]. □

Exercise 31

31. (i) write down all the elements with order 7 in Z/28Z? (ii) How many subgroups are there of order 7 in Z/28Z?

1. write down all the elements with order 7 in $\mathbb{Z}/28\mathbb{Z}$.

Proof. We want to find all the elements of order 7 in $\mathbb{Z}/28\mathbb{Z}$. An element $[x]$ has order 7 if and only if $7x \equiv 0 \mod 28$ and $x \not\equiv 0 \mod 28$.

This means x must be a multiple of 4 (since $\frac{28}{7} = 4$), but not a multiple of 28. The candidates are $4, 8, 12, 16, 20, 24$.

Calculating orders:

$$\begin{aligned}
[4]^7 &\equiv [0], \\
[8]^7 &\equiv [0], \\
[12]^7 &\equiv [0], \\
[16]^7 &\equiv [0], \\
[20]^7 &\equiv [0], \\
[24]^7 &\equiv [0].
\end{aligned}$$

The elements of order 7 in $\mathbb{Z}/28\mathbb{Z}$ are $[4]$ and $[24]$. □

2. How many subgroups are there of order 7 in $\mathbb{Z}/28\mathbb{Z}$?

Proof. The number of subgroups of order 7 in $\mathbb{Z}/28\mathbb{Z}$ corresponds to the number of elements of order 7. Since 7 is prime and divides 28, there are $\phi(7) = 6$ distinct elements of order 7.

Hence, there are 6 subgroups of order 7 in $\mathbb{Z}/28\mathbb{Z}$. □

z/3 x z/5z

Exercise 32

1. prove that the cyclic group $(\mathbb{Z}/15\mathbb{Z})^*$ is isomorphic to the product group $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$.

Proof.
We want to show that the cyclic group $(\mathbb{Z}/15\mathbb{Z})^*$ is isomorphic to the product group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. We know that $(\mathbb{Z}/15\mathbb{Z})^*$ is the set of all elements in $\mathbb{Z}/15\mathbb{Z}$ that are relatively prime to 15. We can find a generator for $(\mathbb{Z}/15\mathbb{Z})^*$ by finding an element of order 8. We can find an element of order 8 by checking the orders of the elements in $(\mathbb{Z}/15\mathbb{Z})^*$:

$$\begin{aligned}
[1]^1 &= [1] \\
[2]^4 &= [1] \\
[4]^2 &= [1] \\
[7]^4 &= [1] \\
[8]^2 &= [1] \\
[11]^4 &= [1] \\
[13]^4 &= [1] \\
[14]^2 &= [1]
\end{aligned}$$

We can see that [2] is an element of order 8 in $(\mathbb{Z}/15\mathbb{Z})^*$. Therefore, $(\mathbb{Z}/15\mathbb{Z})^*$ is a cyclic group with generator [2]. We can now define a group isomorphism $\phi : (\mathbb{Z}/15\mathbb{Z})^* \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ by:

$$\begin{aligned}
\phi([2]^0) &= ([0],[0]) \\
\phi([2]^1) &= ([1],[2]) \\
\phi([2]^2) &= ([2],[4]) \\
\phi([2]^3) &= ([0],[1]) \\
\phi([2]^4) &= ([1],[3]) \\
\phi([2]^5) &= ([2],[1]) \\
\phi([2]^6) &= ([0],[2]) \\
\phi([2]^7) &= ([1],[4])
\end{aligned}$$

We can see that ϕ is a group isomorphism. Therefore, $(\mathbb{Z}/15\mathbb{Z})^*$ is isomorphic to the product group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

□

2. Prove that the group $(\mathbb{Z}/15\mathbb{Z})^*$ is isomorphic to the product group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Conclude that $(\mathbb{Z}/15\mathbb{Z})^*$ is not cyclic

Proof.
We want to show that the group $(\mathbb{Z}/15\mathbb{Z})^*$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

From Part 1, we know $(\mathbb{Z}/15\mathbb{Z})^*$ has 8 elements and can be expressed as:

$$(\mathbb{Z}/15\mathbb{Z})^* \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

We will verify that this is also isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ through structure analysis.

The orders of elements in $(\mathbb{Z}/15\mathbb{Z})^*$ reveal that there are 2 elements of order 2 and 4 elements of order 4. Hence, the group cannot be cyclic since it contains non-cyclic subgroups.

The structure $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ is not cyclic either, hence concluding:

$$(\mathbb{Z}/15\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \text{ and is not cyclic.}$$

□