Homework 7 Solutions

March 17, 2012

1 Chapter 9, Problem 10 (graded)

Let G be a cyclic group. That is, $G = \langle a \rangle$ for some $a \in G$. Then given any $g \in G$, $g = a^n$ for some integer n.

Let H be any normal subgroup of G (actually, since G is cyclic, it is also Abelian, so all subgroups of G are normal), and consider the factor group $G/H = \{gH : g \in G\}$. G/H is the group whose elements are left cosets of H. Let gH be any element of G/H. Since $g = a^n$ for some integer n, we have

$$gH = a^n H.$$

Next, by definition of multiplication in a factor group,

$$gH = a^n H = (aH)^n.$$

Therefore, if gH is any element of G/H, then $gH = (aH)^n$ for some integer n. This implies that $G/H = \langle aH \rangle$. That is, G/H is a cyclic group generated by the element aH.

2 Chapter 9, Problem 16 (graded)

Before presenting the solution, let me talk about computing order in a factor group G/H. Suppose gH is an element of G/H (so $g \in G$) and I want to compute its order as an element of G/H. In other words, I want to find an integer n such that

$$(gH)^n = eH = H$$

and if $1 \leq m < n$,

$$(gH)^m \neq H.$$

By definition of multiplication in a factor group, we need to find n so that

$$g^n H = H$$

and if $1 \leq m < n$,

$$g^m H \neq H.$$

By the Lemma on page 139, $g^n H = H$ iff $g^n \in H$, and $g^m H \neq H$ iff $g^m \notin H$.

Therefore, $|gH| = n$ in G/H iff n is the smallest positive integer for which $g^n \in H$. This allows you to switch between working in G/H and in G.

Now, consider the group D_6 and a subgroup $Z(D_6) = \{R_0, R_{180}\}$, the center of D_6. That is R_0 and R_{180} commute with any element in D_6. Note that $Z(D_6)$ is a normal subgroup of D_6 (see Example 2 on page 179). To find the order of the element $R_{60}Z(D_6)$ in $D_6/Z(D_6)$, we need to find the smallest positive integer n such that

$$R_{60}^n \in Z(D_6) = \{R_0, R_{180}\}\,.$$

Let us try some values for n:

- $n = 1$ gives us $R_{60}^1 = R_{60} \notin Z(D_6)$.
- $n = 2$ gives us $R_{60}^2 = R_{120} \notin Z(D_6)$.
- $n = 3$ gives us $R_{60}^3 = R_{180} \in Z(D_6)$.

Therefore, $n = 3$ is the smallest integer for which $R_{60}^n \in Z(D_6)$, and thus $R_{60}Z(D_6)$ has order 3 in $D_6/Z(D_6)$.

3 Chapter 9, Problem 20 (not graded)

Let $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$ be the group of positive integers coprime to 20 whose operation is multiplication mod 20. Then

$$U_5(20) = \{x \in U(20) : x = 1 \bmod 5\} = \{1, 11\}\,.$$

This is a subgroup of $U(20)$. It is normal because $U(20)$ is Abelian. Since $|U(20)| = 8$ and $|U_5(20)| = 2$, by Corollary 1 on page 142, there are $\frac{8}{2} = 4$ distinct cosets of $U_5(20)$. They are:

$$1U_5(20) = U_5(20) = \{1, 11\} = \{11, 1\} = \{11, 11 \cdot 11\} = 11U_5(20)$$

$$3U_5(20) = \{3, 33\} = \{3, 13\} = \{13, 3\} = \{13, 13 \cdot 11\} = 13U_5(20)$$
$$7U_5(20) = \{7, 77\} = \{7, 17\} = \{17, 7\} = \{17, 17 \cdot 11\} = 17U_5(20)$$
$$9U_5(20) = \{9, 99\} = \{9, 19\} = \{19, 9\} = \{19, 19 \cdot 11\} = 19U_5(20)$$

Remember, we are working mod 20. Hence

$$U(20)/U_5(20) = \{\{1, 11\}, \{3, 13\}, \{7, 17\}, \{9, 19\}\}\,.$$

We want to write our cosets as $aU_5(20)$. Let us use values of a between 1 and 9:

$$U(20)/U_5(20) = \{U_5(20), 3U_5(20), 7U_5(20), 9U_5(20)\}\,.$$

Multiplication in $U(20)/U_5(20)$ works like the multiplication on $U(20)$:

$$aU_5(20) \cdot bU_5(20) = (ab)U_5(20)$$

(make sure to reduce ab mod 20 as well).

When making the Cayley table, we only want to use $U_5(20), 3U_5(20), 7U_5(20), 9U_5(20)$. So, if we were multiplying and somehow got $13U_5(20)$, we should replace it by the same coset $3U_5(20)$.

$\times$	$U_5(20)$	$3U_5(20)$	$7U_5(20)$	$9U_5(20)$
$U_5(20)$	$U_5(20)$	$3U_5(20)$	$7U_5(20)$	$9U_5(20)$
$3U_5(20)$	$3U_5(20)$	$9U_5(20)$	$U_5(20)$	$7U_5(20)$
$7U_5(20)$	$7U_5(20)$	$U_5(20)$	$9U_5(20)$	$3U_5(20)$
$9U_5(20)$	$9U_5(20)$	$7U_5(20)$	$3U_5(20)$	$U_5(20)$

4 Chapter 9, Problem 28 (graded)

4.1 Distinguishing between $\mathbb{Z}_4$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2$

The main difference between these two groups is that $\mathbb{Z}_4$ has elements of order four, while $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ does not. Thus, if we have a group G of order four, it is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, and we can figure out which one by either:

1. Showing that the order of every element in G is less than or equal to two (so $G \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2$), or

2. Showing that at least one element of G has order four (so $G \approx \mathbb{Z}_4$).

In this problem, we have an Abelian group $G = \mathbb{Z}_4 \oplus \mathbb{Z}_4$ and two (normal) subgroups

$$H = \{(0,0), (2,0), (0,2), (2,2)\}$$

and

$$K = \langle (1,2) \rangle = \{(0,0), (1,2), (2,0), (3,2)\}.$$

We will look at the factor groups G/H and G/K and determine if they are isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Note that the order of both G/H and G/K is 4, since G itself has order 16 and both H and K have order 4, so

$$|G/H| = \frac{|G|}{|H|} = \frac{4 \cdot 4}{4} = 4,$$

and similarly for G/K.

4.2 G/H

Let $(a,b) + H$ be an element of G/H. That is, $(a,b) \in G$, so a and b are integers between 0 and 3. Let us look at integer multiples of $(a,b) + H$ (in order to obtain information on the order of $(a,b) + H$).

$$2 \cdot ((a,b) + H) = (2 \cdot (a,b)) + H = (2a, 2b) + H.$$

Is $(2a, 2b) + H = H$, the identity element of G/H? In other words, is $(2a, 2b) \in H$? Note that $2a$ is either 0 or 2, while $2b$ is either 0 or 2 (remember to reduce mod 4), so $(2a, 2b) \in H$, and hence $(2a, 2b) + H = H$. Therefore, for any $(a, b) + H \in G/H$, since $2 \cdot ((a, b) + H) = H$,

$$|(a, b) + H| \leq 2.$$

We cannot say that the order of $(a, b) + H$ is two since it is possible that $1 \cdot ((a, b) + H) = H$ for certain choices of (a, b), but we can conclude that the order of every element of G/H is less than or equal to two, so G/H has no elements of order four. Therefore,

$$G/H \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

4.3 G/K

Let $(a, b)+K$ be an element of G/K. Let us look at integer multiples of $(a, b)+K$.

$$2 \cdot ((a, b) + K) = (2 \cdot (a, b)) + K = (2a, 2b) + K.$$

Is $(2a, 2b) + K = K$, the identity element of G/K? In other words, is $(2a, 2b) \in K$? In this case, it is possible to choose (a, b) so that $(2a, 2b) \notin K$. For this to happen, we need to pick b so that $2b = 2$, and we need to pick a so that $2a$ is not equal to 1 or 3. Thus, we can try $(a, b) = (0, 1)$. Then $(2a, 2b) = (0, 2) \notin K$, so in G/K,

$$2 \cdot ((0, 1) + K) = (2 \cdot (0, 1)) + K = (0, 2) + K \neq K.$$

Furthermore, $(0, 1) + K$ itself is not equal to K since $(0, 1) \notin K$. Hence

$$|(0, 1) + K| > 2.$$

What could the order of $(0, 1) + K$ be in G/K? Since $|G/K| = 4$, we know the order of $(0, 1) + K$ must divide 4. Since $|(0, 1) + K| > 2$,

$$|(0, 1) + K| = 4.$$

Therefore, G/K has an element of order 4, so it must be isomorphic to $\mathbb{Z}_4$.

5 Chapter 9, Problem 30 (not graded)

We need to write 165 as a product of coprime integers in four different ways and use the formula in the middle of page 192 to write $U(165)$ as an internal direct product. In general, if $m = n_1 n_2 \dots n_k$ where $\gcd(n_i, n_j) = 1$ for $i \neq j$,

$$U(m) = U_{m/n_1}(m) \times U_{m/n_2}(m) \times \ldots \times U_{m/n_k}(m).$$

$165 = 3 \cdot 5 \cdot 11$

Here, $n_1 = 3$, $n_2 = 5$, and $n_3 = 11$. Then

$$U(165) = U_{165/3}(165) \times U_{165/5}(165) \times U_{165/11}(165) = U_{55}(165) \times U_{33}(165) \times U_{15}(165).$$

$165 = 15 \cdot 11$

Here, $n_1 = 15$, and $n_2 = 11$. Then

$$U(165) = U_{165/15}(165) \times U_{165/11}(165) = U_{11}(165) \times U_{15}(165).$$

$165 = 3 \cdot 55$

Here, $n_1 = 3$, and $n_2 = 55$. Then

$$U(165) = U_{165/3}(165) \times U_{165/55}(165) = U_{55}(165) \times U_3(165).$$

$165 = 5 \cdot 33$

Here, $n_1 = 5$, and $n_2 = 33$. Then

$$U(165) = U_{165/5}(165) \times U_{165/33}(165) = U_{33}(165) \times U_5(165).$$

6 Chapter 9, Problem 34 (not graded)

Since $\mathbb{Z}$ has addition as its operation, we should be proving that $\mathbb{Z} = H + K$. In other words,

$$\mathbb{Z} = \langle 5 \rangle + \langle 7 \rangle = \{5s + 7t : s, t \in \mathbb{Z}\}.$$

Notice that the definition of $\langle 5 \rangle + \langle 7 \rangle$ tells us that $\langle 5 \rangle + \langle 7 \rangle$ is the set of linear combinations of 5 and 7. Since $\gcd(5, 7) = 1$, there exist integers s_1, t_1 such that

$$1 = 5s_1 + 7t_1.$$

For example, take $s_1 = 3$ and and $t_1 = -2$. If n is any other integer, we can express it as a linear combination of 5 and 7:

$$n = n \cdot 1 = n\,(5s_1 + 7t_1) = 5(ns_1) + 7(nt_1) \in \langle 5 \rangle + \langle 7 \rangle.$$

Thus, $\mathbb{Z} \subseteq \langle 5 \rangle + \langle 7 \rangle$. Since $\langle 5 \rangle + \langle 7 \rangle \subseteq \mathbb{Z}$, we have

$$\mathbb{Z} = \langle 5 \rangle + \langle 7 \rangle.$$

However, $\langle 5 \rangle \cap \langle 7 \rangle \neq \{0\}$. In fact, $\langle 5 \rangle \cap \langle 7 \rangle = \langle 35 \rangle$, since 35 is a multiple of both 5 and 7. Indeed, $\mathbb{Z} \neq \langle 5 \rangle \times \langle 7 \rangle$, and we will show this by proving that $\mathbb{Z}$ is not isomorphic to $\langle 5 \rangle \oplus \langle 7 \rangle$ and applying the contrapositive of Theorem 9.6.

To show that $\mathbb{Z}$ is not isomorphic to $\langle 5 \rangle \oplus \langle 7 \rangle$, we will proceed by contradiction and assume that there is an isomorphism $\phi : \mathbb{Z} \to \langle 5 \rangle \oplus \langle 7 \rangle$. Let

$$\phi(1) = (5s, 7t) \in \langle 5 \rangle \oplus \langle 7 \rangle.$$

Then for any integer n,

$$\phi(n) = (5ns, 7nt).$$

Consider the element $(5s+5, 7t) \in \langle 5 \rangle \oplus \langle 7 \rangle$. Since ϕ is an isomorphism, it must be onto, so there is an integer m such that

$$\phi(m) = (5s + 5, 7t).$$

However,

$$\phi(m) = (5ms, 7mt),$$

so we need to find m so that $5s + 5 = 5ms$ and $7t = 7mt$. Thus, by setting components equal and canceling 5 and 7,

$$s + 1 = ms$$

and

$$t = mt.$$

If $t \neq 0$, then this forces $m = 1$, but then we get $s + 1 = 1s = s$, which is not possible. Thus, $t = 0$, but then for any integer n,

$$\phi(n) = (5ns, 7nt) = (5ns, 0),$$

so $\phi(\mathbb{Z}) = \langle 5s \rangle \oplus \{0\} \neq \langle 5 \rangle \oplus \langle 7 \rangle$. In other words, for any integer m, the second component of $\phi(m)$ must be zero. For example, there is no integer m for which

$$\phi(m) = (5, 7).$$

Therefore, ϕ is not onto, contradicting the assumption that it was an isomorphism. Therefore, $\mathbb{Z}$ is not isomorphic to $\langle 5 \rangle \oplus \langle 7 \rangle$, so by Theorem 9.6, $\mathbb{Z}$ is not equal to $\langle 5 \rangle \times \langle 7 \rangle$.

7 Chapter 9, Problem 44 (not graded, but take a look)

By Theorem 9.4, page 187, we have

$$D_{13}/Z(D_{13}) \approx \mathrm{Inn}(D_{13}),$$

which is pretty close to what we want. In order to prove that D_{13} itself is isomorphic to $\mathrm{Inn}(D_{13})$,we need to do the following:

1. Prove that $Z(D_{13}) = \{R_0\}$, where R_0 is the identity element of D_{13} (it is a trivial rotation by a multiple of 360 degrees).

2. Prove that $D_{13}/\{R_0\} \approx D_{13}$. This can be done by either defining an isomorphism from D_{13} to $D_{13}/\{R_0\}$, or by defining a homomorphism from D_{13} to D_{13} which is onto and has kernel equal to $\{R_0\}$. I will present both ways.

3. Apply part 2, part 1, and then Theorem 9.4:

$$D_{13} \approx D_{13}/\{R_0\} = D_{13}/Z(D_{13}) \approx \mathrm{Inn}(D_{13}).$$

7.1 $Z(D_{13}) = \{R_0\}$

Let R be a rotation by $\frac{360}{13}$ degrees counter-clockwise (so $R^{13} = R_0$) and k be an integer with $1 \leq k < 13$. Then R^k is a rotation by $\frac{360}{13}k$ degrees, and since $1 \leq k < 13$, R^k is not the identity (trivial rotation by a multiple of 360 degrees).

Let F be any flip.

Our goal is to prove that R^k and F are not in $Z(D_{13})$ for $1 \leq k < 13$. We will prove that

$$FR^k \neq R^k F$$

and hence F does not commute with R^k, so they cannot be in $Z(D_{13})$. This will leave R_0 as the only element in $Z(D_{13})$.

By exercise 32 on page 54, we have

$$FR^kF = R^{-k}.$$

First, let me point out that $R^k \neq R^{-k}$. This is because by Theorem 4.2 on page 75, $\left|R^k\right| = \frac{|R|}{\gcd(|R|,k)} = \frac{13}{\gcd(13,k)} = \frac{13}{1} = 13$. $|R| = 13$ because if a 13 sided figure is rotated by $\frac{360}{13}$ degrees, it would have to be rotated twelve more times for a total of thirteen rotations to get back to the original position. $\gcd(13, k) = 1$ since 13 is coprime to all integers between 1 and 12. Hence $\left(R^k\right)^{13} = R_0$, and $\left(R^k\right)^2 \neq R_0$ (2 is a positive integer less than the order of R^k). Since $\left(R^k\right)^2 \neq R_0$, $R^k \neq \left(R^k\right)^{-1} = R^{-k}$.

Thus, we have

$$FR^kF = R^{-k}.$$

Since $FF = R_0$, we can multiply on the right by F to get

$$FR^k = R^{-k}F.$$

Since $R^{-k} \neq R^k$, $R^{-k}F \neq R^kF$, so

$$FR^k = R^{-k}F \neq R^kF.$$

Therefore, F does not commute with R^k, and R^k does not commute with F, so neither of them can be in $Z(D_{13})$. Hence the only element in $Z(D_{13})$ is R_0, so

$$Z(D_{13}) = \{R_0\}.$$

7.2 $D_{13}/\{R_0\} \approx D_{13}$

There are two ways to prove this result.

7.2.1 Finding an isomorphism from D_{13} to $D_{13}/\{R_0\}$

Define $f : D_{13} \to D_{13}/\{R_0\}$ by

$$f(g) = g\{R_0\}.$$

Then for any $g, h \in D_{13}$,

$$f(gh) = gh\{R_0\} = g\{R_0\}h\{R_0\} = f(g)f(h)$$

so f preserves the operations.

Next, suppose

$$f(g) = f(h).$$

Then

$$g\{R_0\} = h\{R_0\}$$

so

$$\{g\} = \{h\}.$$

Therefore, $g = h$. We could also use part 5 of the Lemma on page 139 to say that

$$g^{-1}h \in \{R_0\}$$

so $g^{-1}h = R_0$, and thus $g = h$. Hence f is 1-1.

Finally, if we have a coset $g\{R_0\} \in D_{13}/\{R_0\}$, then by definition of f,

$$f(g) = g\{R_0\},$$

so f is onto. Therefore, f is an isomorphism, and

$$D_{13}/\{R_0\} \approx D_{13}.$$

7.2.2 Finding a homomorphism from D_{13} to D_{13} which is onto and has kernel equal to $\{R_0\}$

Define $\phi : D_{13} \to D_{13}$ by

$$\phi(g) = g.$$

That is, ϕ is the identity function on D_{13}.

Then for any $g, h \in D_{13}$,

$$\phi(gh) = gh = \phi(g)\phi(h).$$

Thus, ϕ is a homomorphism since it preserves operations. Now we need to prove that ϕ is onto and has kernel equal to $\{R_0\}$.

Given any $g \in D_{13}$,

$$\phi(g) = g.$$

Thus, ϕ is onto, so $\phi(D_{13}) = D_{13}$.

Finally, suppose $g \in \mathrm{Ker}\phi$. Then $\phi(g) = R_0$, so $g = \phi(g) = R_0$, and therefore $\mathrm{Ker}\phi \subseteq \{R_0\}$. On the other hand, since $\phi(R_0) = R_0$, $R_0 \in \mathrm{Ker}\phi$, so $\{R_0\} \subseteq \mathrm{Ker}\phi$. Thus, $\mathrm{Ker}\phi = \{R_0\}$.

By the First Isomorphism Theorem on page 207,

$$D_{13}/\mathrm{Ker}\phi \approx \phi(D_{13}).$$

Since $\mathrm{Ker}\phi = \{R_0\}$ and $\phi(D_{13}) = D_{13}$,

$$D_{13}/\{R_0\} \approx D_{13}.$$

7.3 Conclusion

By part 2,

$$D_{13} \approx D_{13}/\{R_0\}.$$

By part 1, since $Z(D_{13}) = \{R_0\}$,

$$D_{13}/\{R_0\} = D_{13}/Z(D_{13}).$$

By Theorem 9.4, page 187,

$$D_{13}/Z(D_{13}) \approx \mathrm{Inn}(D_{13}).$$

Putting all this together,

$$D_{13} \approx D_{13}/\{R_0\} = D_{13}/Z(D_{13}) \approx \mathrm{Inn}(D_{13}),$$

and therefore,

$$D_{13} \approx \mathrm{Inn}(D_{13}).$$

8 Chapter 9, Problem 70 (graded)

Let $H = \{e, h\}$ and let $Z(G)$ be the center of G. To show that $H \subseteq Z(G)$, we need to show that each element of H is an element of $Z(G)$. By definition, for any $g \in G$, since

$$eg = g = ge$$

$e \in Z(G)$. Now we need to show that h commutes with every element in G.

Since H is normal, we know that for any $g \in G$, $gH = Hg$ and $gHg^{-1} \subseteq H$. This gives us two options to proceed.

8.1 Using $gH = Hg$

For any $g \in G$,

$$gH = \{ge, gh\} = \{g, gh\},$$

and

$$Hg = \{eg, hg\} = \{g, hg\}.$$

Therefore, since $gH = Hg$,

$$\{g, gh\} = \{g, hg\},$$

so $gh = hg$ for any $g \in G$. Therefore, $h \in Z(G)$, so $H \subseteq Z(G)$.

8.2 Using $gHg^{-1} \subseteq H$

For any $g \in G$, $gHg^{-1} \subseteq H$. Hence $geg^{-1} = e \in H$ and $ghg^{-1} \in H$, so ghg^{-1} is either e or h. If $ghg^{-1} = e$, then $h = g^{-1}eg = e$, a contradiction, so

$$ghg^{-1} = h.$$

Therefore, $gh = hg$ for any $g \in G$, so $h \in Z(G)$, and hence $H \subseteq Z(G)$.

9 Chapter 10, Problem 4 (not graded)

Let $\sigma : S_n \to \mathbb{Z}_2$ be the mapping described in example 11, page 206. We can describe σ better by using the fact that every permutation is a product of 2-cycles.

Let $\alpha \in S_n$, and suppose we can write α as a product of r 2-cycles. If r is an even number, then α is an even permutation, so $\sigma(\alpha) = 0$. If r is an odd number, then α is an odd permutation, so $\sigma(\alpha) = 1$. Notice that either way, $\sigma(\alpha) = r \bmod 2$. Theorem 5.5 on page 105 assures us that we do not need to worry about the exact value of r, only its remainder when dividing by 2.

Therefore, let $\alpha, \beta \in S_n$, and suppose α is a product of r 2-cycles and β as a product of s 2-cycles. Then $\alpha\beta$ is a product of $r + s$ 2-cycles. Thus,

$$\sigma(\alpha\beta) = r + s \bmod 2$$

and

$$\sigma(\alpha) + \sigma(\beta) = r \bmod 2 + s \bmod 2 = r + s \bmod 2$$

so

$$\sigma(\alpha\beta) = \sigma(\alpha) + \sigma(\beta).$$

Hence σ preserves operations, so it is a homomorphism.

10 Chapter 10, Problem 10 (graded)

Let $f : \mathbb{Z}_{12} \to \mathbb{Z}_{10}$ be a function given by $f(x) = 3x$ reduced mod 10. Be careful: $0 \le x \le 11$.

We will present a few ways to solve this problem.

10.1 Showing that f does not preserve the operations

In $\mathbb{Z}_{12}$, $6 + 6 = 0 \bmod 12$. However,

$$f(6 + 6) = f(0) = 0$$

while

$$f(6) + f(6) = 18 + 18 = 36 = 6$$

and $0 \ne 6$ in $\mathbb{Z}_{10}$. Thus, f does not preserve the operations because $f(6+6) \ne f(6) + f(6)$.

10.2 Showing that f does not preserve the operations (another example)

In $\mathbb{Z}_{12}$, $7 + 7 = 2 \bmod 12$. However,

$$f(7 + 7) = f(2) = 6$$

while

$$f(7) + f(7) = 21 + 21 = 42 = 2$$

and $6 \neq 2$ in $\mathbb{Z}_{10}$. Thus, f does not preserve the operations because $f(7+7) \neq f(7) + f(7)$.

10.3 Using Theorem 10.1, Part 2

In $\mathbb{Z}_{12}$, $2 \cdot 8 = 4 \bmod 12$. However,

$$f(2 \cdot 8) = f(4) = 12 = 2$$

while

$$2 \cdot f(8) = 2 \cdot (24) = 48 = 8$$

and $2 \neq 8$ in $\mathbb{Z}_{10}$. Thus, f fails Part 2 of Theorem 10.1 because $f(2 \cdot 8) \neq 2 \cdot f(8)$. It cannot be a homomorphism.

10.4 Using Theorem 10.1, Part 3

In $\mathbb{Z}_{12}$, $2 \cdot 6 = 0$ and $1 \cdot 6 \neq 0$, so $|6| = 2$. However,

$$f(6) = 18 = 8$$

and in $\mathbb{Z}_{10}$, $|8| = |8 \cdot 1| = \frac{10}{\gcd(10,8)} = 5$, which does not divide 2, the order of 6 in $\mathbb{Z}_{12}$. Thus, f fails Part 3 of Theorem 10.1.

10.5 Using Theorem 10.1, Part 4

$\text{Ker} f = \{x \in \mathbb{Z}_{12} : f(x) = 0\}$. We see that $\text{Ker} f = \{0, 10\}$ since $f(0) = 0 = 30 = f(10) \bmod 10$. $\text{Ker} f$ is not a subgroup of $\mathbb{Z}_{12}$ since it is not closed ($10 + 10 = 8 \notin \text{Ker} f$), and does not have inverses (the additive inverse of 10 in $\mathbb{Z}_{12}$ is 2, which is not in $\text{Ker} f$ since $f(2) = 6 \neq 0$ in $\mathbb{Z}_{10}$). Thus, f cannot be a homomorphism.

10.6 Using Theorem 10.1, Part 5

We have $f(1) = 3 = 33 = f(11) \bmod 10$, but

$$1 + \text{Ker} f = \{1 + 0, 1 + 10\} = \{1, 11\}$$

and (since $21 = 9 \bmod 12$),

$$11 + \text{Ker} f = \{11 + 0, 11 + 10\} = \{11, 9\}$$

so

$$1 + \text{Ker} f \neq 11 + \text{Ker} f.$$

10.7 Using Theorem 10.1, Part 6

We have $f(3) = 9$, but the set $f^{-1}(9) = \{3\}$, while $3+\text{Ker}f = \{3+0, 3+10\} = \{3, 1\}$. $f^{-1}(9) \neq 3 + \text{Ker}f$.

10.8 Using Theorem 10.2, Part 1

Let $H = \{0, 6\}$ be a subgroup of $\mathbb{Z}_{12}$. Then $f(\{0,6\}) = \{f(0), f(6)\} = \{0, 8\}$, which is not a subgroup of $\mathbb{Z}_{10}$ since it is not closed ($8+8 = 6 \notin f(\{0,6\})$) and it does not contain all inverses (it does not have 2, the additive inverse of 8).

10.9 Using Theorem 10.2, Part 5

$|\text{Ker}f| = 2$, but f is not a 2-to-1 mapping because only one element in $\mathbb{Z}_{12}$, 3, is mapped to $9 \in \mathbb{Z}_{10}$. A 2-to-1 mapping would send exactly two elements in $\mathbb{Z}_{12}$ to each element in $\mathbb{Z}_{10}$.

10.10 Using Theorem 10.2, Part 6

$|\mathbb{Z}_{12}| = 12$. However, $f(\mathbb{Z}_{12}) = \{0, 3, 6, 9, 2, 5, 8, 1, 4, 7\} = \mathbb{Z}_{10}$, which has order 10. Since 10 does not divide 12, f cannot be a homomorphism.

10.11 Using Theorem 10.2, Part 7

Let $\overline{K} = \{0, 5\}$ be a subgroup of $\mathbb{Z}_{10}$. Then $f^{-1}\left\{\overline{K}\right\} = \{0, 10, 5\}$, which is not a subgroup of $\mathbb{Z}_{12}$ (it is not closed).

Conclusion

f is not a homomorphism.

11 Chapter 10, Problem 51 (presented on 3/15 during a review session)

Let G be any group, $Z(G)$ be its center, and $\text{Inn}(G) = \{\phi_g : g \in G\}$, where ϕ_g is a function from G to G defined as follows: for any $x \in G$,

$$\phi_g(x) = gxg^{-1}.$$

The function ϕ_g is called the inner automorphism of G induced by g. Each element of g gives an inner automorphism, but it is possible to have two different elements g and h in G induce the same inner automorphism ($\phi_g(x) = \phi_h(x)$ for all $x \in G$). $\text{Inn}(G)$ is a group whose operation is function composition read from right to left.

To prove that

$$G/Z(G) \approx \text{Inn}(G),$$

we need to find a function f from G to $\text{Inn}(G)$ with the following properties:

1. f is a homomorphism (preserves operations).
2. f is onto. That is, $f(G) = \text{Inn}(G)$.
3. $\text{Ker} f = Z(G)$.

Once these three properties are proven, we can apply the First Isomorphism Theorem on page 207 to show that

$$G/Z(G) \approx \text{Inn}(G).$$

Again, when using the First Isomorphism Theorem, the domain of the homomorphism is G, not $G/Z(G)$.

For $g \in G$, define

$$f(g) = \phi_g.$$

In other words, $f(g)$ is the inner automorphism of G induced by g.

11.1 f is a homomorphism

Let $g, h \in G$. Then

$$f(gh) = \phi_{gh}$$

$$f(g)f(h) = \phi_g \circ \phi_h$$

In order to show that $f(gh) = f(g)f(h)$, we need to prove that the functions ϕ_{gh} and $\phi_g \circ \phi_h$ are equal. To do this, let $x \in G$. Then

$$\phi_{gh}(x) = (gh)x(gh)^{-1} = ghxh^{-1}g^{-1}$$

and

$$\phi_g \circ \phi_h(x) = \phi_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = ghxh^{-1}g^{-1}.$$

Thus, $\phi_{gh}(x) = \phi_g \circ \phi_h(x)$ for any $x \in G$. Hence the functions ϕ_{gh} and $\phi_g \circ \phi_h$ are equal, so $f(gh) = f(g)f(h)$. Therefore, f preserves the operations, so it is a homomorphism.

11.2 f is onto (so $f(G) = \textbf{Inn}(G)$)

Let ϕ_g be any element of $\text{Inn}(G)$. Then ϕ_g is the inner automorphism of G induced by $g \in G$. Then by definition,

$$f(g) = \phi_g,$$

so f is onto.

11.3 Ker$f = Z(G)$

Before we begin, let us point out that the identity element of Inn(G) is ϕ_e, the function given by

$$\phi_e(x) = exe^{-1} = x.$$

To determine Ker$f$, we start by looking at an element $g \in$ Ker$f$. Then $f(g)$ is the identity element of Inn(G):

$$f(g) = \phi_e.$$

We need to show that $g \in Z(G)$. Since $f(g) = \phi_g$, we have

$$\phi_g = \phi_e.$$

Therefore, for any $x \in G$, we have

$$gxg^{-1} = exe^{-1} = x$$

$$gxg^{-1} = x$$

$$gx = xg.$$

Therefore, $g \in Z(G)$. This implies that Ker$f \subseteq Z(G)$.

Now, if $g \in Z(G)$, then for any $x \in G$, $gx = xg$, so

$$\phi_g(x) = gxg^{-1} = (gx)g^{-1} = (xg)g^{-1} = x(gg^{-1}) = x = exe^{-1} = \phi_e(x)$$

so

$$f(g) = \phi_g = \phi_e,$$

and hence $g \in$ Ker$f$. Thus, $Z(G) \subseteq$ Ker$f$, and therefore Ker$f = Z(G)$.

11.4 Conclusion

Since f is a homomorphism, we can use Theorem 10.3 on page 207 to say

$$G/\text{Ker}f \approx f(G).$$

Since $f(G) = \text{Inn}(G)$, and Ker$f = Z(G)$, we have

$$G/Z(G) \approx \text{Inn}(G).$$