# Solution Outlines for Chapter 10

**# 8: Let $G$ be a group of permutations. For each $\sigma$ in $G$, define**

$$\operatorname{sgn}(\sigma) = \begin{cases} +1 & \textbf{if } \sigma \textbf{is an even permutation.} \\ -1 & \textbf{if } \sigma \textbf{is an odd permutation.} \end{cases}$$

**Prove that $\operatorname{sgn}(\sigma)$ is a homomorphism from $G$ to the multiplicative group $\{+1, -1\}$. What is the kernel? Why does this homomorphism allow you to conclude that $A_n$ is a normal subgroup of $S_n$ of index 2? Why does this prove Exercise 23 of Chapter 5?**

Let $G$ be a group of permutations, and $\alpha, \beta \in G$. Every permutation is either even or odd. If both $\alpha$ and $\beta$ are odd, $\phi(\alpha\beta) = 1$, since the composition of two odd permutations is even. But this is the same as $(-1)(-1) = \phi(\alpha)\phi(\beta)$. If both permutations are even, $\alpha\beta$ is even, so $\phi(\alpha\beta) = 1 = (1)(1) = \phi(\alpha)\phi(\beta)$. Finally, assume one of the permutations is even and one is odd. Without loss of generality, assume $\alpha$ is even and $\beta$ is odd. Then $\alpha\beta$ is odd.So $\phi(\alpha\beta) = -1 = 1(-1) = \phi(\alpha)\phi(\beta)$. Hence, $\phi$ is a homomorphism.

The $\ker \phi$ is the subgroup of even permutations in $G$.

If $G = S_n$, then $\ker \phi = A_n$ so $A_n$ is a normal subgroup. The first isomorphism theorem tells us that $S_n/A_n \approx \{1, -1\}$ so $A_n$ has index 2 in $S_n$. It's also clear that if $H$ is a subgroup of $S_n$ then it is either all even or this homomorphism shows that $H$ consists of half even and half odd permutations since the two cosets of H have equal size and split $H$ in this way.

**# 13: Prove that $(A \oplus B)/(A \oplus \{e\}) \approx B$.**

Define $\phi : (A \oplus B) \to B$ by $(a, b) \mapsto b$. Then $\phi$ is a homomorphism since $\phi((a, b)(c, d)) = \phi((ac, bd)) = bd = \phi((a, b))\phi((c, d))$. Further, the image of $\phi$ is $B$ since for each $y \in B$, $\phi(a, b)$ maps to $b$ for any $a \in A$. Finally, the $ker\phi = A \oplus \{e\}$. Thus, by the first isomorphism theorem, $(A \oplus B)/(A \oplus \{e\}) \approx B$.

**# 15: Suppose that $\phi$ is a homomorphism from $\mathbb{Z}_{30}$ to $\mathbb{Z}_{30}$ and $Ker\phi = \{0, 10, 20\}$. If $\phi(23) = 9$ determine all elements that map to 9.**

Notice that this question is really just asking for $\phi^{-1}(9)$. By the properties of homomorphisms, we know that this is the coset $23Ker\phi$, or $\{23, 3, 13\}$.

**# 20: How many homomorphisms are there from $\mathbb{Z}_{20}$ onto $\mathbb{Z}_8$? How many are there to $\mathbb{Z}_8$?**

Notice that the difference between the first and second question is onto. If I want to map onto $\mathbb{Z}_8$, the image of $\phi$ is 8. But the order of the image must divide the order of $\mathbb{Z}_{20}$ since $|\mathbb{Z}_{20}| = |Im\phi| \times |\ker \phi|$. But 8 does not divide 20 so there is no onto homomorphism between $\mathbb{Z}_{20}$ and $\mathbb{Z}_8$.

Now, consider homomorphisms in general from $\mathbb{Z}_{20}$ to $\mathbb{Z}_8$. The order of $\phi(1)$ must divide 8 and 20, or divide the $gcd(8,20) = 4$. Thus the $\phi(1)$ has order 1, 2 or 4. If it has order 1, then $\phi$ is the identity map. If it has order 2, the image is $\{4, 0\}$ so $\phi(x) = 4x$. If it has order 4, the image is $\{2, 4, 6, 0\}$ so either $\phi(x) = 2x$ or $\phi(x) = 6x$. Hence there are 4 homomorphisms to $\mathbb{Z}_8$.

**# 21: If $\phi$ is a homomorphism from $\mathbb{Z}_{30}$ onto a group of order 5, determine the kernel of $\phi$.**

Since $\phi$ is onto a group of order 5, the order of the kernel is $\frac{30}{5} = 6$. Hence the kernel must be the order 6 subgroup of $\mathbb{Z}_{30}$, namely $\{5, 10, 15, 20, 25, 0\} =< 5 >$.

**# 22: Suppose that $\phi$ is a homomorphism from a finite group $G$ onto $\bar{G}$, and that $\bar{G}$ has an element of order 8. Prove that $G$ has an element of order 8. Generalize.**

Since $\phi$ is onto, there exists a $g \in G$ such that $\phi(g)$ has order 8. Thus (Thm 10.1), the order of $g$ is divisible by 8. Say $|g| = 8k$ for some integer $k$. Since $< g >$ is cyclic, and has order $8k$, there exists $\phi(8) = 4$ elements of order 8 in $< g > \subseteq G$. Hence, $G$ has an element of order 8.

**# 24: Suppose that $\phi : \mathbb{Z}_{50} \to \mathbb{Z}_{15}$ is a group homomorphism with $\phi(7) = 6$.**

1. **Determine $\phi(x)$.**
   Let $\phi(1) = k$. Then $\phi(x) = kx$. In particular, $\phi(7) = 7k \bmod 15 = 6$. So $k = 3$. Hence, $\phi(x) = 3x$.

2. **Determine the image of $\phi$.**
   The image of $\phi$ is $< 3 >$ in $\mathbb{Z}_{15}$, which is $\{3, 6, 9, 12, 0\}$.

3. **Determine the kernel of $\phi$.**
   The $Ker\phi$ has order $\frac{50}{5} = 10$ in $\mathbb{Z}_{50}$. So $Ker\phi =< 5 >= \{5, 10, 15, 20, 25, 30, 35, 40, 45, 0\}$ in $\mathbb{Z}_{50}$.

4. **Determine $\phi^{-1}(3)$.**
   $\phi^{-1}(3) = 1 + \ker\phi = 1+ < 5 >= \{6, 11, 16, 21, 26, 31, 36, 41, 46, 1\}$.

**# 25: How many homomorphisms are there from $\mathbb{Z}_{20}$ onto $\mathbb{Z}_{10}$? How many are there to $\mathbb{Z}_{10}$?**

Again, the difference here is onto. We know that the image of $\phi$ will have order 10 if it is onto, and this is possible since 10 does divide 20. To have an image of $\mathbb{Z}_{10}$, $\phi(1)$ must generate $\mathbb{Z}_{10}$. Hence, $\phi(1)$ is either 1, 3, 7, or 9. So there are 4 homomorphisms onto $\mathbb{Z}_{10}$.

Now, let's examine homomorphisms to $\mathbb{Z}_{10}$. Then $\phi(1)$ must have an order that divides 10 and that divides 20. However, this means that $\phi(1)$ could be any number is $\mathbb{Z}_{10}$ (since 10 divides 20)! Thus there are 10 homomorphisms to $\phi(1)$: $\phi(x) = kx$ for any $k \in \mathbb{Z}_{10}$.

**# 26: Determine all homomorphisms from $\mathbb{Z}_4$ to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.**

There are four such homomorphisms. The image of any such homomorphism can have order 1, 2 or 4. If it has order 1, then $\phi$ maps everything to the identity or $\phi(x) = (0, 0$. The image can not have order 4 since such a map would have to be an isomorphism and $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is not cyclic. Finally, the map could have image of size 2 so the images could be $< (1,0) >$, $< (0,1) >$ or $< (1,1) >$. The maps would then be $x \mapsto (x \text{ mod } 2, 0)$, $x \mapsto (0, x \text{ mod } 2)$ and $x \mapsto (x \text{ mod } 2, x \text{ mod } 2)$ respectively.

**# 31: Suppose that $\phi$ is a homomorphism from $U(30)$ to $U(30)$ and that $Ker\phi = \{1, 11\}$. If $\phi(7) = 7$, find all elements of $U(30)$ that map to 7.**

$\phi^{-1}(7) = 7Ker\phi = \{7, 17\}$.

**# 35: Prove that the mapping $\phi : \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z}$ given by $(a, b) \mapsto a - b$ is a homomorphism. What is the kernel of $\phi$? Describe the set $\phi^{-1}(3)$.**

Let $\phi$ defined as above. Then $\phi((a, b) + (c, d)) = \phi((a + c, b + d)) = (a + c) - (b + d) = (a - b) + (c - d) = \phi((a, b)) + \phi((c, d))$. Hence $\phi$ is a homomorphism. The kernel of $\phi$ is the set of pairs such that $a - b = 0$, or $\{(a, a) | a \in \mathbb{Z}\}$. Finally, to find $\phi^{-1}(3)$ observe that $(3, 0)$ maps to 3. Thus $\phi^{-1}(3) = (3, 0) + Ker\phi = \{(a + 3, a) | a \in \mathbb{Z}\}$.

**# 36: Suppose that there is a homomorphism $\phi$ from $\mathbb{Z} \oplus \mathbb{Z}$ to a group $G$ such that $\phi((3, 2)) = a$ and $\phi((2, 1)) = b$. Determine $\phi((4, 4))$ in terms of $a$ and $b$. Assume that the operation of $G$ is addition.**

First notice that $c(3, 2) + d(2, 1) = (4, 4)$ implies that $3c + 2d = 4$ and $2c + d = 4$. Hence $d = 4 - 2c$ so $3c + 8 - 4c = 8 - c = 4$. Therefore $c = 4$ and $d = -4$. So $\phi((4, 4)) = \phi(4(3, 2) + -4(2, 1)) = 4\phi(3, 2) - 4\phi(2, 1) = 4a - 4b$.

**# 37: Let $H = \{z \in \mathbb{C}^* \big| |z| = 1\}$. Prove that $\mathbb{C}^*/H$ is isomorphic to $\mathbb{R}^+$, the group of positive real numbers under multiplication.**

Define $\phi$ from $\mathbb{C}^*$ to $\mathbb{R}^+$ by $a + bi \mapsto |a + bi| = \sqrt{a^2 + b^2}$. So $\phi((a + bi)(c + di)) = \phi((ac - bd) + (ad + bc)i) = \sqrt{(ac - bd)^2 + (ad + bc)^2} = \sqrt{a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2} = \sqrt{a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2} = \sqrt{a^2(c^2 + d^2) + b^2(c^2 + d^2)} = \sqrt{(a^2 + b^2)(c^2 + d^2)} = \sqrt{a^2 + b^2}\sqrt{c^2 + d^2} = \phi(a + bi)\phi(c + di)$. Thus $\phi$ is a homomorphism. It is clear that this map is onto since for any $r \in \mathbb{R}^+$, $r$ is in $\mathbb{C}^*$ and $r \mapsto r$. Finally, by definition, $H$ is the kernel of $\phi$. Hence, by the first isomorphism theorem, $\mathbb{C}^*/H$ is isomorphic to $\mathbb{R}^+$.

**# 42: (Third Isomorphism Theorem) If $M$ and $N$ are normal subgroups of $G$ and $N \leq M$, prove that $(G/N)/(M/N) \approx G/M$.**

Consider the map $\phi$ from $G/N$ to $G/M$ defined by $gN \mapsto gM$. Then $\phi$ is a homomorphism since $\phi(gNhN) = \phi(ghN) = ghM = gMhM = \phi(gN)\phi(gM)$. This map is clearly onto since $gM$ is mapped to by $gN$. The kernel of this map is $\{gN | \phi(gN) = M\} = \{gN | gM = M\} = \{gN | g \in M\} = M/N$. Hence by the first isomorphism theorem, the third isomorphism theorem is true.

**# 48: Suppose that $\mathbb{Z}_{10}$ and $\mathbb{Z}_{15}$ are both homomorphic images of a finite group $G$. What can be said about $|G|$? Generalize.**

If $\mathbb{Z}_{10}$ is a homomorphic image of $G$, 10 divides the order of $G$. Similarly, 15 divides the order of $G$. Hence the order of $G$ is divisible by $lcm(10, 15) = 30$. In general, the order of $G$ is divisible by the least common multiple of the orders of all its homomorphic images.

**# 55: Let $\mathbb{Z}[x]$ be the group of polynomials in $x$ with integer coefficients under addition. Prove that the mapping from $\mathbb{Z}[x]$ into $\mathbb{Z}$ given by $f(x) \mapsto f(3)$ is a homomorphism. Give a geometric description of the kernel of this homomorphism. Generalize.**

Define $\phi$ to be the mapping given above. Then $\phi(f(x) + g(x)) = \phi((f + g)(x)) = (f + g)(3) = f(3) + g(3) = \phi(f(x)) + \phi(g(x))$ so $\phi$ is a homomorphism. Its kernel is $\{f(x)|\phi(f(x)) = f(3) = 0\}$. This is the set of functions with integer coefficients whose graphs go through the point (0,3). To generalize, 3 could be replaced with any integer.

**# 65: Prove that the mapping from $\mathbb{C}^*$ to $\mathbb{C}^*$ given by $\phi(z) = z^2$ is a homomorphism and that $\mathbb{C}^*/\{1, -1\}$ is isomorphic to $\mathbb{C}^*$.**

Let $\phi$ be defined as the mapping above. We observe that $\phi$ is a homomorphism since $\phi(xy) = (xy)^2 = x^2y^2 = \phi(x)\phi(y)$ since $\mathbb{C}^*$ is Abelian. Let $x \in \mathbb{C}^*$. Then $\phi(\sqrt{x}) = x$. Since we are in $\mathbb{C}^*$, $\sqrt{x}$ is defined for all elements and it is indeed in $\mathbb{C}$. [There are a variety of formulas available for this.] Finally, the kernel of this map is $\{1, -1\}$. So we are done by the first isomorphism theorem.

**# 66: Let $p$ be a prime. Determine the number of homomorphisms from $\mathbb{Z}_p \oplus \mathbb{Z}_p$ into $\mathbb{Z}_p$.**

Let $\phi : \mathbb{Z}_p \oplus \mathbb{Z}_p \to \mathbb{Z}_p$ be a homomorphism. Then $\phi((a, b)) = a\phi((1, 0)) + b\phi((0, 1))$. So to determine the number of homomorphisms, we only need to know the number of possible choices for $\phi((1, 0))$ and $\phi((0, 1))$. But $p$ is prime, so we can send each of these to any element in $\mathbb{Z}_p$ (everything except 0 will be a generator so the image will automatically have order $p$ or 1). Thus there are $p^2$ homomorphisms.