SOLUTION KEY
Produced by: Kyle Dahlin

<u>Problems:</u>
Chap 10: 31,**32**,41,**42**
Chap 11: 4,8,15,26,28,**30**,36

Problem 10.31. Suppose that ϕ 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.

Solution:
$\phi^{-1}(7) = 7 \ker \phi = \{7, 17\}$. ■

Problem 10.32. Find a homomorphism ϕ from $U(30)$ to $U(30)$ with kernel $\{1, 11\}$ and $\phi(7) = 7$.

Solution:
First note the orders of elements of $U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}$: $|7| = 4$, $|11| = 2$, $|13| = 4$, $|17| = 4$, $|19| = 2$, $|23| = 4$, and $|29| = 2$.

Since $\phi(19) = \phi(7^2) = \phi(7)^2 = 19$ then $\phi(19) = 19$. Similarly $\phi(13) = \phi(19 \cdot 7) = 19 \cdot 7 = 13$. Since $\ker \phi = \{1, 11\}$, $\phi(29) = 19$ and $\phi(23) = 13$.

Any map with the properties above that meets property 2 of Theorem 10.2 must map $1, 11 \mapsto 1$, $7, 17 \mapsto 7$, $13, 23 \mapsto 13$, $19, 29 \mapsto 19$. Hence either this map is a homomorphism or there can be no homomorphism with the listed properties. ■

Problem 10.41. (Second Isomorphism Theorem) If K is a subgroup of G and N is a normal subgroup of G, prove that $K/(K \cap N)$ is isomorphic to KN/N.

Solution:
Let $\phi : K \to KN/N$ be defined by $\phi(k) = kN$. ϕ is clearly well-defined. Now

$$\ker \phi = \{k \in K | \phi(k) = N\} = \{k \in K | k \in N\} = K \cap N.$$

Let $knN \in KN/N$. Since $knN = kN$, then $\phi(k) = knN$. Hence ϕ is onto.

Thus by the First Isomorphism Theorem, $K/(K \cap N) \approx KN/N$. ■

Problem 10.42. (Third Isomorphism Theorem) If M and N are normal subgroups of G and $N \leq M$, prove that $(G/N)/(M/N) \approx G/M$.

Solution:
Define $\phi : G/N \to G/M$ by $\phi(gN) = gM$. To show that ϕ is well-defined, let $g_1N = g_2N$. Then $g_1g_2^{-1} \in N$, hence $g_1g_2^{-1} \in M$ so that $\phi(g_1) = g_1M = g_2M = \phi(g_2)$.

Let $gN \in \ker \phi$. Then $gM = M$, hence $g \in M$. Hence $gN \in M/N$. Now let $mN \in M/N$, then $\phi(mN) = mM = M$. Thus $\ker \phi = M/N$. ϕ is clearly onto since $N \leq M$.

By the First Isomorphism Theorem, $(G/N)/(M/N) \approx G/M$. ■

Problem 11.4. Calculate the number of elements of order 2 in each of $\mathbb{Z}_{16}$, $\mathbb{Z}_8 \oplus \mathbb{Z}_2$, $\mathbb{Z}_4 \oplus \mathbb{Z}_4$, and $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Do the same for elements of order 4.

Solution:

Group	elements of order 2	#
$\mathbb{Z}_{16}$	8	1
$\mathbb{Z}_8 \oplus \mathbb{Z}_2$	$(0,1),(4,0),(4,1)$	3
$\mathbb{Z}_4 \oplus \mathbb{Z}_4$	$(2,2),(0,2),(2,0)$	3
$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	$(2,0,0),(2,1,0),(2,1,1),(2,0,1),(0,1,0),(0,1,1),(0,0,1)$	7

Group	elements of order 4	#
$\mathbb{Z}_{16}$	$4, 12$	2
$\mathbb{Z}_8 \oplus \mathbb{Z}_2$	$(2,0),(2,1),(6,0),(6,1)$	4
$\mathbb{Z}_4 \oplus \mathbb{Z}_4$	all except elements of order 0 or 2	12
$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	all except elements of order 0 or 2	8

■

Problem 11.8. Show that there are two Abelian groups of order 108 that have exactly 13 subgroups of order 3.

Solution:
The only Abelian groups of order 108 are:

1. $\mathbb{Z}_{27} \oplus \mathbb{Z}_4$
2. $\mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4$
3. $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4$
4. $\mathbb{Z}_{27} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$
5. $\mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$
6. $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Since 3 is prime, any subgroup of order 3 must be cyclic. The order of elements in finite Abelian groups is given by the least common multiple of their "components". Thus the "even part" of the element must always be zero. Thus we need only look for which of $\mathbb{Z}_{27}$, $\mathbb{Z}_9 \oplus \mathbb{Z}3$, or $\mathbb{Z}_3 \oplus \mathbb{Z}3 \oplus \mathbb{Z}3$ has 13 subgroups of order 3.

$\mathbb{Z}_3 \oplus \mathbb{Z}3 \oplus \mathbb{Z}3$ has $27 - 1 = 26$ elements of order 3 which generate 13 unique subgroups of order 3 (since some overlap). Hence any Abelian group of order 108 with exactly 13 subgroups of order 3 is isomorphic to either $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4$ or $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. ■

Problem 11.15. How many Abelian groups (up to isomorphism) are there

a. of order 6?

b. of order 15?

c. of order 42?

d. of order pq, where p and q are distinct primes?

e. of order pqr, where p, q, and r are distinct primes?

f. Generalize parts d and e.

Solution:

a. There is one Abelian group of order 6 (up to isomorphism): $\mathbb{Z}_6 \approx \mathbb{Z}_3 \oplus \mathbb{Z}_2$, since 3 and 2 are relatively prime and prime.

b. Similarly, there is one Abelian group of order 15 (up to isomorphism): $\mathbb{Z}_{15} \approx \mathbb{Z}_5 \oplus \mathbb{Z}_3$

c. There is one Abelian group of order 42 (up to isomorphism): $\mathbb{Z}_{42} \approx \mathbb{Z}_7 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$, since 7, 3, and 2 are relatively prime and prime.

d. There is one Abelian group of order pq (up to isomorphism): $\mathbb{Z}_{pq} \approx \mathbb{Z}_p \oplus \mathbb{Z}_q$, since p and q are relatively prime and prime.

e. There is one Abelian group of order pqr (up to isomorphism): $\mathbb{Z}_{pqr} \approx \mathbb{Z}_p \oplus \mathbb{Z}_q \oplus \mathbb{Z}_r$, since p, q, and r are relatively prime and prime.

f. If p_1, p_2, …, p_n are distinct primes, then there is exactly one Abelian group up to isomorphism: $\mathbb{Z}_{p_1 p_2 \cdots p_n} \approx \mathbb{Z}_{p_1} \oplus \cdots \oplus \mathbb{Z}_{p_n}$.

■

Problem 11.26. Let $G = \{1, 7, 17, 23, 49, 55, 65, 71\}$ under multiplication modulo 96. Express G as an external and internal direct product of cyclic groups.

Solution:
We calculate the order of elements on G:

Element	Order
1	0
7	4
17	2
23	4
49	2
55	4
65	2
71	4

Since G has order 8 with 4 elements of order 4, $G \approx \mathbb{Z}_4 \oplus \mathbb{Z}_2$. Let ϕ be the isomorphism between G and $\mathbb{Z}_4 \oplus \mathbb{Z}_2$. Then $G = \phi^{-1}(\mathbb{Z}_4 \oplus \{0\}) \times \phi^{-1}(\{0\} \oplus \mathbb{Z}_2)$. ■

Problem 11.28. The set $G = \{1, 4, 11, 14, 16, 19, 26, 29, 31, 34, 41, 44\}$ is a group under multiplication modulo 45. Write G as an external and an internal direct product of cyclic groups of prime-power order.

Solution:
We calculate the order of elements on G:

Element	Order
1	0
4	6
11	6
14	6
16	3
19	2
26	2
29	6
31	3
34	6
41	6
44	2

Hence $G \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$ since it has order 12 and 6 elements of order 6. Let ϕ be the isomorphism between G and $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$. Then $G = \phi^{-1}(\mathbb{Z}_2 \oplus \{0\} \oplus \{0\}) \times \phi^{-1}(\{0\} \oplus \mathbb{Z}_2 \oplus \{0\}) \times \phi^{-1}(\{0\} \oplus \{0\} \oplus \mathbb{Z}_3)$. ■

Problem 11.30. Suppose that G is an Abelian group of order 16, and in computing the order of its elements, you come across an element of order 8 and two elements of order 2. Explain why no further computations are needed to determine the isomorphism class of G.

Solution:
An Abelian group of order 16 is isomorphic to one of: $\mathbb{Z}_{16}$, $\mathbb{Z}_8 \oplus \mathbb{Z}_2$, $\mathbb{Z}_4 \oplus \mathbb{Z}_4$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

If there is an element of order 8, then only $\mathbb{Z}_{16}$ or $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ are possible candidates. Since $\mathbb{Z}_{16}$ has only one element of order 2, namely 8, then G must be isomorphic to $\mathbb{Z}_8 \oplus \mathbb{Z}_2$. ■

Problem 11.36. Suppose that G is a finite Abelian group. Prove that G has order p^n, where p is prime, if and only if the order of every element of G is a power of p.

Solution:
Let G be a finite Abelian group.

Suppose that G has order p^n, where p is a prime. Then if $g \in G$, $|g|$ divides p^n and since p is prime, $|g| = p^k$ for $0 \leq k \leq n$.

Now suppose that the order of every element of G is a power of p. Suppose that $|G| = p^k m$ where p does not divide m. By the Corollary on page 230, G has a subgroup of order m, call it H. Let $h \in H$. Then $|h| = p^l$ divides $|H| = m$. But since p^l does not divide m for $k > 0$, we must have that $k = 0$ and $H = \{e\}$ and $m = 1$. Hence $|G| = p^k$. ■