**SOLUTION KEY**
Produced by: Kyle Dahlin

Problems:
Chap 7: 22, 26, 40, 44
Chap 8: 2, 8, 10, 54

**Problem 7.22.** Suppose $H$ and $K$ are subgroups of a group $G$. If $|H| = 12$ and $|K| = 35$, find $|H \cap K|$. Generalize.

*Solution:*
Let $a \in H \cap K$. Then $|a|$ divides $|H| = 12$ and $|K| = 35$, by Corollary 2 of Lagrange's Theorem. Hence $|a| = 1$ so that $a = e$ and $|H \cap K| = 1$. In general, if $H$ and $K$ are subgroups and $\gcd(|H|, |K|) = 1$, then $|H \cap K| = 1$. ■

**Problem 7.26***.** Suppose that $G$ is a group with more than one element and $G$ has no proper, nontrivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that $G$ is finite.)

*Solution:*
Let $a \neq e$ be an element of $G$. Then $\langle a \rangle = G$ since otherwise $\langle a \rangle$ would be a proper subgroup. If $G$ were not finite, then, for example, $\langle a^2 \rangle$ would be a proper subgroup. Hence $G$ is finite. Let $m$ be any divisor of $|a|$. Then $\langle a^m \rangle \subseteq G$, so that either $m = 1$ or $m = |a|$. Hence $|a| = |G|$ is prime. ■

**Problem 7.40.** Prove that a group of order 63 must have an element of order 3.

*Solution:*
Let $G$ be a group with $|G| = 63$. Let $a \neq e$ be an element of $G$. Then $|a|$ divides 63, by Corollary 2 of Lagrange's Theorem. Hence $|a| \in \{3, 7, 9, 21, 63\}$. If $|a| = 3$, we are done. If $|a| = 63$, then $|a^{21}| = 3$. If $|a| = 21$, then $|a^7| = 3$. If $|a| = 9$, then $|a^3| = 3$.

Hence we need only deal with case that **all** 62 non-identity elements of $G$ have order 7. By the Corollary to Theorem 4.4, the number of elements of order 7 must be a multiple of $\phi(7) = 6$. But 6 does not divide 62. Thus there must be at least one element of $G$ with order 3, 9, 21, or 63, and we are done by our previous work. ■

**Problem 7.44.** Prove that every subgroup of $D_n$ of odd order is cyclic.

*Solution:*
Recall that $|D_n| = 2n$. Let $H \leq D_n$ with $|H| = m$ odd. We know that elements of $D_n$ are made up of combinations of reflections and rotations. Since any reflection has order 2 and $m$ is odd, there can be no reflections in $H$. Let $K$ be the subgroup of $D_n$ made up of all rotations. Then $K = \left\langle R_{360/n} \right\rangle$ is cyclic. Since $H$ must be entirely made up of rotations, $H \leq K$. Every subgroup of a cyclic group is cyclic, hence $H$ is cyclic. ■

**Problem 8.2***.** Show that $Z_2 \oplus Z_2 \oplus Z_2$ has seven subgroups of order 2.

*Solution:*
Each subgroup must be cyclic since 2 is prime.

1. $\langle(1,0,0)\rangle$
2. $\langle(0,1,0)\rangle$
3. $\langle(0,0,1)\rangle$
4. $\langle(1,1,0)\rangle$
5. $\langle(1,0,1)\rangle$
6. $\langle(0,1,1)\rangle$
7. $\langle(1,1,1)\rangle$

Each of these have order 2 since $|(a_1,a_2,a_3)| = \text{lcm}(|a_1|,|a_2|,|a_3|)$. ■

**Problem 8.8.** Is $Z_3 \oplus Z_9$ isomorphic to $Z_{27}$? Why?

*Solution:*
Since 9 and 3 are not relatively prime these are not isomorphic (by Corollary 2 to Theorem 8.2). ■

**Problem 8.10***.** How many elements of order 9 does $Z_3 \oplus Z_9$ have?

*Solution:*
The elements of order 9 of $Z_3 \oplus Z_9$ are elements of the form $(a,b)$ where $\text{lcm}(|a|,|b|) = 9$. Elements of $Z_3$ have orders of 1 or 3 and elements of $Z_9$ have orders of 1, 3, or 9. Hence the only way to get $\text{lcm}(|a|,|b|) = 9$ is if $|b| = 9$. There are $\phi(9) = 6$ elements of order 9 in $Z_9$. Each of these elements of $Z_9$ can be paired with any element of $Z_3$, hence there are $3 \times 6 = 18$ elements of order 9 in $Z_3 \oplus Z_9$. ■

**Problem 8.54.** Find an isomorphism from $Z_{12}$ to $Z_4 \oplus Z_3$.

*Solution:*
Let $\phi : Z_{12} \to Z_4 \oplus Z_3$ be defined by $\phi(a) = (a \bmod 4, a \bmod 3)$. Then since

$$\begin{aligned}\phi(a+b) &= (a+b \bmod 4, a+b \bmod 3)\\ &= (a \bmod 4, a \bmod 3) + (b \bmod 4, b \bmod 3)\\ &= \phi(a) + \phi(b),\end{aligned}$$

$\phi$ is a homomorphism.

Suppose that $\phi(a) = \phi(b)$. Then $a \bmod 4 = b \bmod 4$ and $a \bmod 3 = b \bmod 3$, that is, $a + 4k = b + 4l$ and $a + 3i = b + 3j$ for some $i,j,k,l \in \mathbb{Z}$. Hence $a - b = 4(l-k) = 3(j-i)$. If $l = k$ or $i = j$ then $a = b$. Otherwise if $l \neq k$ and $i \neq j$, then both 4 and 3 divide $a - b$, and hence 12 divides $a - b$. But if 12 divides $a - b$, then $a = b$ in $Z_{12}$. Hence $\phi$ is one-to-one.

Since $|Z_{12}| = |Z_4 \oplus Z_3|$ is finite, $\phi$ being one-to-one implies that it is also onto. ■