Solution Outlines for Chapter 8

 # 1: Prove that the external direct product of any finite number of groups is a group.

Proof. Let $G = G_1 \oplus G_2 \oplus \cdots \oplus G_n$, where each G_i is a group, and let the operation $*$ on G be defined component wise (as in the definition of external direct product). Since each operation in G_i is associative, $*$ is associative on G. [This is clear since $a*(b*c) = a*(b_1*c_1, b_2*c_2, \ldots b_n*c_n) = (a_1*(b_1*c_1), a_2*(b_2*c_2), \ldots, a_n*(b_n*c_n)) = ((a_1*b_1)*c_1, (a_2*b_2)*c_2, \ldots, (a_n*b_n)*c_n) = (a_1*b_1, a_2*b_2, \ldots, a_n*b_n)*c = (a*b)*c$.] Similarly, we can see that G is closed since $a*b = (a_1*b_1, a_2*b_2, \ldots, a_n*b_n)$ and $a_ib_i \in G_i$ by closure of G_i. The previous calculation also verifies that the identity in G is $e = (e_1, e_2, \ldots, e_n)$ where e_i is the identity in G_i and that the inverse of a is $a^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$. Since each G_i is a group, both e and a^{-1} is in G. □

 # 2: Show that $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ has seven subgroups of order 2.

First notice that any subgroup of order two must be isomorphic to $\mathbb{Z}_2$ and hence cyclic with an order two generator. Moreover, each subgroup of order two contains one non-identity order two element. Thus the seven subgroups are generated by the seven non-identity order two elements in $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Namely, these groups are:
$<(1,0,0)>$, $<(0,1,0)>$, $<(0,0,1)>$, $<(1,1,0)>$, $<(1,0,1)>$, $<(0,1,1)>$, and $<(1,1,1)>$.

 # 3: Let G be a group with identity e_G and let H be a group with identity e_H. Prove that G is isomorphic to $G \oplus \{e_H\}$ and that H is isomorphic to $\{e_G\} \oplus H$.

Proof. Define $\phi : G \to G \oplus \{e_H\}$ by $g \mapsto (g, e_H)$. Since $\phi(gh) = (gh, e_H) = (gh, e_He_H) = (g, e_H)(h, e_H) = \phi(g)\phi(h)$, the map ϕ is a homomorphism. The kernel of ϕ is simply $\{g|\phi(g) = (e_G, e_H)\} = \{g|(g, e_H) = (e_G, e_H)\} = \{g|g = e_G\} = \{e_G\}$ so ϕ is one-to-one. Finally, let $y \in G \oplus \{e_H\}$. Then $y = (g, e_H)$ for some $g \in G$ by definition of the external direct product. Hence $\phi(g) = y$ and the map is also onto. Since ϕ is an isomorphism, $G \approx G \oplus \{e_H\}$. Using a similar argument, it is clear that $H \approx \{e_G\} \oplus H$. □

 # 4: Show that $G \oplus H$ is Abelian if and only if G and H are Abelian. State the general case.

Let $G \oplus H$ be Abelian. Then $xy = yx$ for all $x, y \in G \oplus H$. By definition of external direct product, $x = (g_1, h_1)$ and $y = (g_2, h_2)$ for $g_1, g_2 \in G$ and $h_1, h_2 \in H$. Thus $xy = yx$ implies $(g_1g_2, h_1h_2) = (g_2g_1, h_2h_1)$. Hence, $g_1g_2 = g_2g_1$ and $h_1h_2 = h_2h_1$. Since x, y are arbitrary, all elements of G commute as do all elements in H, and both groups are Abelian. This argument reverse entirely to show that G and H Abelian implies $G \oplus H$ is Abelian.

In general, the external direct product of a finite number of groups is Abelian if and only if each group in the product is Abelian.

 # 6: Prove, by comparing orders of elements, that $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}_4 \oplus \mathbb{Z}_4$.

Notice that $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ has an element of order 8, namely $(1,1)$, but $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ can not have an element of order 4 since the orders in $\mathbb{Z}_4$ are 1, 2, and 4. (There is no way to get a least common multiple of 8 from 1, 2, and 4.)

 # 7: Prove that $G_1 \oplus G_2$ is isomorphic to $G_2 \oplus G_1$. State the general case.

Proof. Define $\phi : G_1 \oplus G_2 \to G_2 \oplus G_1$ by $(g_1, g_2) \mapsto (g_2, g_1)$. We claim that ϕ is an isomorphism. By construction it is clear that ϕ maps from $G_1 \oplus G_2$ to $G_2 \oplus G_1$. Now $\phi((g_1, g_2)(h_1, h_2)) = \phi((g_1g_2, h_1h_2)) = (h_1h_2, g_1g_2) = (h_1, g_1)(h_2, g_2) = \phi(g_1, h_1)\phi(g_2, h_2)$ so ϕ is indeed a homomorphism. If we let $\phi((g_1, g_2)) = \phi((h_1, h_2))$ then $(g_2, g_1) = (h_2, h_1)$ so $g_2 = h_2$ and $g_1 = h_1$. Thus $(g_1, g_2) = (h_1, h_2)$ and we know ϕ is one to one. Finally we show ϕ is onto. Let $(g_2, g_1) \in G_2 \oplus G_1$. Then we know that $(g_1, g_2) \in G_1 \oplus G_2$. Moreover, $\phi((g_1, g_2)) = (g_2, g_1)$ and ϕ is indeed onto. $\square$

In general, $G_1 \oplus G_2 \oplus \cdots \oplus G_n \approx G_{\sigma(1)} \oplus G_{\sigma(2)} \oplus \cdots \oplus G_{\sigma(n)}$ for $\sigma \in S_n$.

 # 10: How many elements of order 9 does $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ have?

We know that (a, b) has order 9 if $lcm(|a|, |b|) = 9$. Thus $|b|$ must be 9 and $|a|$ can be 1 or 3. Everything in $\mathbb{Z}_3$ has order 1 or 3, so a can be any element in $\mathbb{Z}_3$. In $\mathbb{Z}_9$, there are $\phi(9) = 3^2 - 3 = 6$ elements of order 9. Thus there are 3*6 = 18 elements of order 9 in $\mathbb{Z}_3 \oplus \mathbb{Z}_9$.

 # 13: For each integer $n > 1$, give two examples of two non isomorphic groups of order n^2.

$\mathbb{Z}_{n^2}$ and $\mathbb{Z}_n \oplus \mathbb{Z}_n$ (Note: we know these are different since n is not relatively prime to n.)

 # 14: The dihedral group D_n of order $2n$ ($n \geq 3$) has a subgroup of n rotations and a subgroup of order 2. Explain why D_n cannot be isomorphic to the external direct product of two such groups.

Suppose D_n is the external direct product of two such groups. Then $D_n \approx < r > \oplus Z_2 \approx \mathbb{Z}_n \oplus \mathbb{Z}_2$. But, $\mathbb{Z}_n \oplus \mathbb{Z}_2$ is Abelian and D_n is not. Thus D_n can not be the external direct product of two such groups. (Note: It is actually the semi direct product of two such groups.)

 # 15: Prove that the group of complex numbers under addition is isomorphic to $\mathbb{R} \oplus \mathbb{R}$.

Proof. Define $\phi : (\mathbb{C}, +) \to \mathbb{R} \oplus \mathbb{R}$ by $a + bi \mapsto (a, b)$. The calculation $\phi((a + bi) + (c + di)) = \phi((a + c) + (b + d)i) = (a + c, b + d) = (a, b) + (c, d) = \phi(a + bi) + \phi(c + di)$ shows that ϕ is indeed a homomorphism. Suppose that $\phi(a + bi) = \phi(c + di)$. Then $(a, b) = (c, d)$ so $a = c$ and $b = d$. Hence, $a + bi = c + di$ showing one-to-one. For onto, let (a, b) be any element of $\mathbb{R} \oplus \mathbb{R}$. Then it is clear that $a + bi \in \mathbb{C}$ and $\phi(a + bi) = (a, b)$ as desired. $\square$

 # 19: If r is a divisor of m and s is a divisor of n, find a subgroup of $\mathbb{Z}_m \oplus \mathbb{Z}_n$ that is isomorphic to $\mathbb{Z}_r \oplus \mathbb{Z}_s$.

$< \frac{m}{r} > \oplus < \frac{n}{s} >$

 # 20: Find a subgroup of $\mathbb{Z}_{12} \oplus \mathbb{Z}_{18}$ that is isomorphic to $\mathbb{Z}_9 \oplus \mathbb{Z}_4$.

First notice that $\mathbb{Z}_9 \oplus \mathbb{Z}_4$ is isomorphic to $\mathbb{Z}_4 \oplus \mathbb{Z}_9$. This second presentation is, by the previous problem, isomorphic to $< 3 > \oplus < 2 >$.

 # 23: What is the order of any nonidentity element of $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$? Generalize.

Let $e \neq (a, b, c) \in \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$. Since (a, b, c) is not the identity, at least one of a, b, or c is not the identity. Every non-identity element in $\mathbb{Z}_3$ has order 3 and so each of these non-identity elements has order 3. Hence $lcm(|a|, |b|, |c|) = 3$ and the order of the element is 3.

In general, the order of any element in $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \mathbb{Z}_p$, where p is prime, is p.

 # 26: The group $S_3 \oplus \mathbb{Z}_2$ is isomorphic to one of the following groups: $\mathbb{Z}_{12}$, $\mathbb{Z}_6 \oplus \mathbb{Z}_2$, A_4, D_6. Determine which one by elimination.

Since $S_3 \oplus \mathbb{Z}_2$ is not Abelian (since S_3 is not), $S_3 \oplus \mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}_{12}$ or $\mathbb{Z}_6 \oplus \mathbb{Z}_2$. Now, A_4 is the set of even permutation of S_4 and contains elements of order 1, 2, and 3, as seen on page 111 of the text. But $S_3 \oplus \mathbb{Z}_2$ contains the element $((123), 1)$ which has order $lcm(3, 2) = 6$. Thus the group is not A_4, and $S_3 \oplus \mathbb{Z}_3$ is actually isomorphic to D_6.

 # 30: Find all subgroups of order 4 in $\mathbb{Z}_4 \oplus \mathbb{Z}_4$.

Recall that there are two groups of order 4, $\mathbb{Z}_4$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. The subgroups isomorphic to $\mathbb{Z}_4$ are the cyclic ones generated by (a, b) where $lcm(|a|, |b|) = 4$. These are: $< (1, 0) >=< (3, 0) >, < (1, 1) >=< (3, 3) >, < (1, 2) >=< (3, 2) >, < (1, 3) >=< (3, 1) >$ $, < (0, 1) >=< (0, 3), < (2, 1) >=< (2, 3) >$. The other subgroups are isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ and are, by our previous theorem, $< 2 > \oplus < 2 >= \{(0, 0), (0, 2), (2, 0), (2, 2)\}$.

 # 36: Find a subgroup of $\mathbb{Z}_{12} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{15}$ that has order 9.

$< 4 > \oplus \{0\} \oplus < 5 >= \{(0, 0, 0), (4, 0, 0), (8, 0, 0), (0, 0, 5), (0, 0, 10), (4, 0, 5), (4, 0, 10), (8, 0, 5), (8, 0, 10)\}$
Note: This is not the same as $< (4, 0, 5) >= \{(4, 0, 5), (8, 0, 10), (0, 0, 0)\}$.

 # 38: Let $H = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \middle| a, b \in \mathbb{Z}_3 \right\}$. Show that H is an Abelian group of order 9. Is H isomorphic to $\mathbb{Z}_9$ or to $\mathbb{Z}_3 \oplus \mathbb{Z}_3$?

First we show that H is an abelian group. Since $\begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & c & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+c & b+d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, which is of the desired form, we know that H is closed. Associativity is known for matrix multiplication and we know that I is the standard identity matrix. Now, $A^{-1} = \begin{bmatrix} 1 & -a & -b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ by the previous calculation. Finally we observe that $\begin{bmatrix} 1 & c & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+c & d+b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ so H is Abelian since addition in $\mathbb{Z}_3$ is Abelian.

Now, we know that H has order 9 because there are three options for a and three for b or $3 * 3 = 9$ total possible matrices.

We know H can not be isomorphic tho $\mathbb{Z}_9$ since it is not cyclic. But we can clearly see that $H \approx to\mathbb{Z}_3 \oplus \mathbb{Z}_3$ using the map $\begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \mapsto (a, b)$.

 # 40: Let $(a_1, a_2, \ldots, a_n) \in G_1 \oplus G_2 \oplus \cdots \oplus G_n$. Give a necessary and sufficient condition for $|(a_1, a_2, \ldots, a_n)| = \infty$.

Since the order of $(a_1, a_2, \ldots, a_n)$ is just the least common multiple of the component orders, the necessary and sufficient condition is for $|a_i| = \infty$ for some $1 \leq i \leq n$.

 # 49: Express $Aut(U(25))$ in the form $\mathbb{Z}_m \oplus \mathbb{Z}_n$.

First, notice that $U(25)$ has $\phi(25) = 5^2 = 5 = 20$ elements and is cyclic (one generator is 2) so $U(25) \approx \mathbb{Z}_{20}$. Thus $Aut(U(25)) \approx Aut(\mathbb{Z}_{20})$.

Now, $Aut(\mathbb{Z}_{20}) \approx U(20)$ from our previous work and $U(20) \approx U(4) \oplus U(5)$. But $U(4)$ and $U(5)$ are both cyclic and of orders 2 and 4 respectively. Thus, $U(4) \oplus U(5) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_4$.

 # 52: Is $\mathbb{Z}_{10} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6 \approx \mathbb{Z}_{60} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2$?

Yes! $\mathbb{Z}_{10} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6 \approx \mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \approx (\mathbb{Z}_5 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3) \oplus (\mathbb{Z}_3 \oplus \mathbb{Z}_2) \oplus \mathbb{Z}_2 \approx \mathbb{Z}_{60} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2$.

 # 53: Is $\mathbb{Z}_{10} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6 \approx \mathbb{Z}_{15} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{12}$?

No! $\mathbb{Z}_{10} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6 \approx \mathbb{Z}_5 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ but $\mathbb{Z}_{15} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{12} \approx \mathbb{Z}_5 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

Alternately, $\mathbb{Z}_{10} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6$ has more than three elements of order 2 [(5,6,3), (0,6,3), (5,6,0), (5,0,3)] while $\mathbb{Z}_{15} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{12}$ only has three such elements [(0,0,6), (0,2,0), (0,2,6)].

 # 55: How many isomorphisms are there from $\mathbb{Z}_{12}$ to $\mathbb{Z}_4 \oplus \mathbb{Z}_3$?

We know that isomorphisms map generators to generators. So the isomorphisms are completely determined by where 1 maps. The generators of $\mathbb{Z}_4 \oplus \mathbb{Z}_3$ (the elements with order 12) are: (1,1), (3,1), (1,2), and (3,2). Thus there are four isomorphisms.

 # 56: Suppose that ϕ is an isomorphism form $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ to $\mathbb{Z}_{15}$ and $\phi(2,3) = 2$. Find the element in $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ that maps to 1.

Let $\phi : \mathbb{Z}_3 \oplus \mathbb{Z}_5 \to \mathbb{Z}_{15}$ be defined by $\phi((2,3)) = 2$. Then $1 \equiv 8 * 2 = 8 * \phi((2,3)) = \phi(8 * (2,3))$. This last step is the additive version of $\phi(a)^n = \phi(a^n)$. Now, $\phi(8 * (2,3)) = \phi((16,24)) = \phi((1,4))$. Thus, $(1,4)$ maps to 1.

 # 67: Express $U(165)$ as an external direct product of U-groups in four different ways.

First note that 165 = 3*5*11. Then $U(165) \approx U(3) \oplus U(55) \approx U(5) \oplus U(33) \approx U(11) \oplus U(15) \approx U(3) \oplus U(5) \oplus U(11)$

 # 68: Without doing any calculations in $Aut(\mathbb{Z}_{20})$, determine how many elements of $Aut(\mathbb{Z}_{20})$ have order 4. How many have order 2?

First we notice that $Aut(\mathbb{Z}_{20}) \approx U(20) \approx U(4) \oplus U(5)$. Further, both $U(4)$ and $U(5)$ are cyclic with orders 2 and 4 respectively. So, $Aut(\mathbb{Z}_{20}) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_4$. Now, for an element here to have order 4, the second coordinate must be 1 or 3, and the first can be either 0 or 1. Thus there are four elements of order 4.