1. **Question:** What is the best approach to formally proving that a function is onto?

   Answer: Say we have a map $\varphi : G \to H$. In this class, we normally have that φ is at least a group homomorphism, and that G and H are groups, but for our purposes here, we need only that G and H are sets (of any sort) and that φ is a function.

   Then, to show that φ is onto, we take an arbitrary element $h \in H$ and then we find a $g \in G$ which has the property that $\varphi(g) = h$.

2. **Question:** How do you formally show that something is one-to-one?

   Answer: To show that a function f from a set S to a set T is one-to-one, we take two arbitrary elements of S, say s_1 and s_2 and we verify that if $f(s_1) = f(s_2)$, then $s_1 = s_2$.

   If our function happens to be a group homomorphism, we have an equivalent definition: a group homomorphism $\phi : G \to H$ is one-to-one if $\phi(g) = e_H$ implies $g = e_G$. To see that this is the same, consider the following progression: Let $g_1, g_2 \in G$ s.t.

$$\begin{aligned}
\phi(g_1) &= \phi(g_2) \text{ then...} \\
\phi(g_1)\phi(g_2)^{-1} &= e_H \\
\phi(g_1)\phi(g_2^{-1}) &= e_H \text{ since } \phi(g)^{-1} = \phi(g^{-1}) \\
\phi(g_1 \cdot g_2^{-1}) &= e_H \text{ since } \phi \text{ is a homomorphism} \\
\phi(g_1 \cdot g_2^{-1}) &= \phi(e_G) \text{ since } \phi(e_G) = e_H
\end{aligned}$$

   So, if ϕ is one-to-one under our normal definition, then this implies $g_1 g_2^{-1} = e_G$, which means that $g_1 = g_2$.

   On the other hand, if ϕ is a group homomorphism and $\phi(g) = e_H$ implies $g = e_G$, then the above calculation shows that if $\phi(g_1) = \phi(g_2)$, then $\phi(g_1 g_2^{-1}) = e_H$, implying that $g_1 g_2^{-1} = e_G$, implying that $g_1 = g_2$.

3. **Question:** I am still confused about proofs by induction.

   Answer: The general idea is: if we know that some statement holds for some integer a and we can show that the same statement is true for an integer n whenever it's true for all the integers i between a and n: $a \leq i < n$, then we've shown that it's true for all integers $n \geq a$. Usually our a is 0 or 1, and we call the proof that the statement holds for a the base-step. The proof that the statement holds for n whenever it holds for the integers less than n is called the inductive step. For examples or help, check out the text book (or the books of proofs in my office!).

4. **Question:** Are there specific instances when we need to do a proof for a finite set and then for an infinite set?

   Answer: Usually, we're able to prove statements about groups in general (as one case), but if our argument depends at all on any theorem that only works for finite groups (or, respectively, only works for infinite groups), then we'll have to treat the cases separately... so inspect the hypotheses of the theorems carefully!

5. **Question:** I don't understand the proof of the one-step subgroup test. How can you assign both $a = b = x$ in the proof.

   Answer: This is actually a common "trick" used in proofs. Here's the idea: If a statement holds for *all values* of a and b, then it had better hold for a particular choice, such as $a = x$ and $b = x$.

   In the proof of the one-step subgroup test, we're assuming that the nonempty subset H has the property that for any $a, b \in H$, $ab^{-1} \in H$. So, if $x \in H$, then we are free to choose both $a = x$ and $b = x$, which gives us that $xx^{-1} = e \in H$.

6. **Question:** What exactly is the group of quaternions? How do you define it?

   Answer: The definition of the group of quaternions given in homework (using which you worked out a Cayley table for this group) is a perfectly good one: Let $Q = \{1, -1, i, -i, j, -j, k, -k\}$ and define a multiplication on it so that 1 is the identity, -1 commutes with all elements, $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$. We saw that these rules imply that $ki = j$, and that reversing the order of a product $ab = -ba$ when a and b are not equal or opposites, nor are they either ± 1.

   The book uses a different notation. On p. 91 it defines the group of quaternions as the set $\{e, a, a^2, a^3, b, ba, ba^2, ba^3\}$ with a given Cayley table to be the quaternions. If you define a map ϕ so that $\phi(a) = i$ and $\phi(b) = j$, and so that ϕ is a homomorphism, you'll find that ϕ is an isomorphism from their description to ours.

   Finally, some people noticed that the multiplication of the i's, j's and k's looked an awful lot like taking the cross products of the standard basis vectors of $\mathbb{R}^3$, $i = \langle 1, 0, 0 \rangle$, $j = \langle 0, 1, 0 \rangle$ and $k = \langle 0, 0, 1 \rangle$. It's true. The multiplication for these works exactly the same - but only for ij, ji, ik, ki, jk, and kj (i.e. for each of these, $ab = a \times b$). The cross product of a vector with itself is 0, so $i^2 \neq i \times i$.

7. **Question:** What does it mean for an element of a group to be a generator?

   Answer: In multiplicative notation: we say that an element $a \in G$ *generates* G if for every element $g \in G$, g is a power of a. That is, there is some integer k with $a^k = g$.

   In additive notation: we say that an element $a \in G$ *generates* G if for every element $g \in G$, g is a multiple of a. That is, there is some integer k with $k \cdot a = g$.

   In either case, we write $G = \langle a \rangle$.

8. **Question:** I'm still a little confused about cyclic groups, particularly the Fundamental Theorem of Cyclic Groups and knowing which groups are cyclic.

   Answer: As mentioned above, a group is *cyclic* if it has a *generator*. The Fundamental Theorem of Cyclic Groups states that: (1) Every subgroup of a cyclic group is cyclic. (2) If $|\langle a \rangle| = n$, then the order of every subgroup of $\langle a \rangle$ divides n. (3) For each positive divisor d of n, there is exactly one subgroup of order d, and one generator of this subgroup is $a^{n/d}$ (in additive notation, this is $\frac{n}{d} \cdot a$).

   (1) promises us that if we consider the subgroups $\langle g \rangle$ for each $g \in G$, we will find all of the subgroups of G. In $\mathbb{Z}$, this means that every subgroup has the form $\langle n \rangle = n\mathbb{Z}$ (all the multiples of n).

(2) we now know holds for any group, even if it isn't cyclic (this is Lagrange's Theorem).

(3) says that the converse to Lagrange's Theorem is true **for cyclic groups** (we know this isn't true for general groups), and it tells us how to find that subgroup by giving us a formula for its generator.

9. **Question:** I really don't have a good understanding of what a permutation is. In the way that I can think of Z_{12} as the group: $\{0, 1, \ldots, 11\}$ with an operation of addition $(mod 12)$, I'd like to have a better conceptual idea of what a permuation group is.

   Answer: I know some of you aren't going to like this... but a permutation group is a group of maps. These maps are bijections from the set $\{1, 2, \ldots, n\}$ onto the same set: $\{1, 2, \ldots, n\}$.

   - There is a natural identity map, which takes each element $s \in \{1, 2, \ldots, n\}$ to itself: $\epsilon(s) = s$.
   - Since these permutation [maps] are bijections, the composition of any two is still a bijection (going from the same set onto the same set), so the set of permutation [maps] is closed under the operation of function composition.
   - Function composition is associative: $\alpha \circ \beta \circ \gamma = \alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$.
   - Since these permutation [maps] are bijections, each has an inverse, which is again a permutation [map].

   The notations (array and cycle) are merely shorthand for expressing where these maps send the elements of the set, namely 1,2,... n.

   Sometimes, it is tempting to think of permutations as all the possible *arrangements* of the elements of the set $\{1, 2, \ldots, n\}$, but this isn't quite accurate... what would our identity arrangement be? How would we "multiply" arrangements? Really, these arrangements are images of the set under the permutation maps.

10. **Question:** I don't understand composing permutations.

    Answer: Composing permutations is, admittedly, a little confusing. First, let's remember that permutations are functions. These functions take in the integers 1 to n and spit out integers 1 to n (although not necessarily the same one). If we remember back to calculus, when we had two functions, say $f(x) = x + 1$ and $g(x) = x^2$, then when we compose them, we perform the one inside the parentheses (the one on the right) first: $f \circ g(x) = f(g(x)) = f(x^2) = x^2 + 1$. When we do the composition of the same functions in the opposite order, we have: $g \circ f(x) = g(f(x)) = g(x + 1) = (x + 1)^2 = x^2 + 2x + 1$. So order matters in function composition. Keeping this cautionary tale in mind, let's talk about permutations.

    Think of α and β in S_n as functions. In array notation, the top row has the input, and the bottom row has the output. Using the α and β in S_8 from the second homework set (given below), we think of $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \alpha(1) & \alpha(2) & \alpha(3) & \alpha(4) & \alpha(5) & \alpha(6) & \alpha(7) & \alpha(8) \end{bmatrix}$, where $\alpha(1) = 2$, $\alpha(2) = 3$, $\alpha(3) = 4$, etc. We think of β in a similar way. Then their product, $\alpha\beta$ is defined by:

$$\begin{aligned}
\alpha\beta(1) &= \alpha(\beta(1)) = \alpha(1) = 2\\
\alpha\beta(2) &= \alpha(\beta(2)) = \alpha(3) = 4\\
\alpha\beta(3) &= \alpha(\beta(3)) = \alpha(8) = 6\\
\alpha\beta(4) &= \alpha(\beta(4)) = \alpha(7) = 8\\
\alpha\beta(5) &= \alpha(\beta(5)) = \alpha(6) = 7\\
\alpha\beta(6) &= \alpha(\beta(6)) = \alpha(5) = 1\\
\alpha\beta(7) &= \alpha(\beta(7)) = \alpha(2) = 3\\
\alpha\beta(8) &= \alpha(\beta(8)) = \alpha(4) = 5
\end{aligned}$$

You can verify yourself that this is exactly what we got for the product before, using the notational shortcuts of array or cycle notations.

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 8 & 6 \end{bmatrix} \text{ and } \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 8 & 7 & 6 & 5 & 2 & 4 \end{bmatrix}$$

11. **Question:** What is the usefulness of Theorem 5.5 Always even or always odd?

    Answer: Theorem 5.5 says that if we express a permutation as a product transpositions in two different ways, then either both products have an even number of transpositions or an both have an odd number. So, we can classify permutations as even or odd, depending on whether they require an even or odd number of transpositions.

    This might be surprising, considering that there are an endless number of ways to write any permutation as a product of transpositions. It's useful because it turns out that the even permutations form a sub-group!

12. **Question:** I know how to prove that something is an automorphism, but I am still not completely certain about how to always determine the automorphisms of a group or better yet, how to describe the elements of an automorphism group.

    Answer: Just to refresh everyone's memory, an automorphism is a bijective group homomorphism taking a group G onto itself. So, to prove that a map is actually an automorphism, we need to verify the following: (1) In case it's not painfully obvious, we should verify that the map (call it α) takes elements of G to elements of G - so verify $\alpha(g) \in G$ for $g \in G$. (2) Verify that α is a homomorphism - so, for $a, b \in G$, $\alpha(ab) = \alpha(a)\alpha(b)$. (3) Verify that α is 1-1. And finally, (4) verify that α is onto. Remember, we have a few new tricks for these last two: if $|G|$ is finite, then we only need to check one of (3) or (4) (see HW3); second, once we know that α is a homomorphism, in order to show that α is 1-1, we can just show that $\{g \in G \ s.t.\ \alpha(g) = e\} = \{e\}$.

    Now, for a general group G, we don't always have an easy way of specifying all of the automorphisms of G (that is, we don't always know the elements of $Aut(G)$). When G is a finite cyclic group of order n, we know that these correspond to the unit group $U(n)$.

Since the elements of an automorphism group, $Aut(G)$, are maps, we need to specify what these maps do in order to fully describe these elements. That is, we need to either give a general formula (e.g. $\phi(x) = 33x$ $(mod\ 50)$ as in the homework) or list out what exactly $\phi(g)$ is for each $g \in G$.

For example, consider the group $Z_2 \oplus Z_2 = \{(0,0),(0,1),(1,0),(1,1)\}$. We don't have any theorems that tell us what the automorphisms of this group look like, but since it's a small group, it's reasonable to specify automorphisms by listing what they do to the elements. First of all, let α_0 be the identity map, so $\alpha(a,b) = (a,b)$ for any $(a,b) \in Z_2 \oplus Z_2$.

Now, any automorphism $\beta \in Aut(Z_2 \oplus Z_2)$ will have $\beta(0,0) = (0,0)$ since it must preserve the identity. Let $\beta(1,0) = (0,1)$ and $\beta(0,1) = (1,0)$. Then if β is an automorphism, we should have $\beta(1,1) = \beta((1,0)+(0,1)) = \beta(1,0) \oplus \beta(0,1) = (0,1) \oplus (1,0) = (1,1)$. This completely defines an automorphism of $Z_2 \oplus Z_2$ (we haven't fully verified here that β is an automorphism, but we can see it is both 1-1 and onto, and we can check that it is operation preserving by checking a few more "products").

13. **Question:** What is so special about the inner automorphism that it gets its own name and notation?

    Answer: First, note that for Abelian groups, all inner automorphisms give the identity map since $\phi_g(x) = gxg^{-1} = xgg^{-1} = x$. Also, recall that we know all of the automorphisms for cyclic groups. We'll see that all Abelian groups can be viewed as being built out of smaller, cyclic groups, and that we can reconstruct automorphisms of these groups by pasting together automorphisms of the pieces.

    For non-Abelian groups, we aren't so lucky. But, in the non-Abelian case, the inner automorphisms form a much more interesting group. In the non-Abelian setting, inner automorphisms are sometimes the only ones we can easily specify.

14. **Question:** I don't understand why, in the solution for problem 5 (b) in HW3, we are looking for something that equals 1 (mod 50) in order to solve the problem.

    Answer: We know that every automorphism of a cyclic group can be described just by specifying the image of one generator: let G be a cyclic group, a a generator of G (i.e. $G = \langle a \rangle$), and α an automorphism of G. Suppose we know that $\alpha(a) = b$ for some element $b \in G$. If $g \in G$, then $g = a^k$ for some k (this is what it means for a to be a generator of G), and then $\alpha(g) = \alpha(a^k) = \alpha(a)^k = b^k$ (by the homomorphic propertiy of α).

    This same reasoning helps explain why automorphisms of finite cyclic groups ($Aut(Z_n)$) correspond to the elements of the unit groups ($U(n)$): suppose α is an automorphism of Z_n, and that a is a generator of Z_n. Then a must be relatively prime to n, and so $a \in U(n)$. Since $\langle a \rangle = Z_n$, $\langle \alpha(a) \rangle = Z_n$ since $n = |a| = |\alpha(a)|$, so $\alpha(a)$ must also be relatively prime to n, i.e. $\alpha(a) \in U(n)$.

    Now, since an automorphism of a finite cyclic group is specified by where it sends any generator, we can focus on where it sends the generator 1 (since this is the friendliest generator - meaning that it is easiest to determine the k above when $a = 1$). So, now there is one automorphism for each choice of the image of 1, and these choices come from $U(n)$, thus establishing the correspondence. That this correspondence is actually an isomorphism, itself, is proven in the textbook.

In problem 5 (b), we are given that ϕ is an automorphism of Z_{50} and that $\phi(11) = 13$. Since 11 is relatively prime to 50, 11 is a generator of Z_{50}, so the automorphism ϕ is entirely specified by the fact that $\phi(11) = 13$: for any element $m \in Z_{50}$, $m = k \cdot 11\ (mod\ 50)$, and so $\phi(m) = \phi(k \cdot 11) = k \cdot \phi(11) = k \cdot 13\ (mod\ 50)$. But it is difficult to see a general formula for this, since it is difficult to find k. It would be nice if we knew $\phi(1)$, since then it would be easy to specify $\phi(m)$ (since $\phi(m) = m \cdot \phi(1)\ (mod\ 50)$).

We use the fact that $41 \cdot 11 \equiv 1\ (mod\ 50)$: $\phi(41 \cdot 11) \equiv 41 \cdot \phi(11) \equiv 41 \cdot 13 \equiv 33\ (mod\ 50)$. Thus, $\phi(m) = m \cdot 33\ (mod\ 50)$ for any $m \in Z_{50}$.

15. **Question:** I had trouble understanding the centralizer question (problem 7 in HW3). I did not understand why we needed to prove anything about commutativity in order to show that the two (sub)groups were isomorphic.

    Answer: Problem 7 asked you to prove that $C(a) \cong C(gag^{-1})$, for group elements a and g. In general, since $C(a) \leq G$ (the centralizer is a subgroup), we know that it's image under any automorphism of G, say α, will also be a subgroup: $\alpha(C(a)) \leq G$. We also know, since α is an isomorphism, that $C(a) \cong \alpha(C(a))$.

    In this problem, the automorphism in question, α, is really the inner automorphism ϕ_g, so we know that $C(a) \cong \phi_g(C(a)) = gC(a)g^{-1}$. So, if we show that $\phi_g(C(a)) = C(gag^-1)$, then we will have shown $C(a) \cong C(gag^{-1})$.

    In order to show that $\phi_g(C(a))$ (which is just the subgroup containing elements of the form gcg^{-1} where $c \in C(a)$) is the same as the subgroup $C(gag^{-1})$ (which is the subgroup of elements which commute with gag^{-1}), we'll show that each set contains the other.

    First, $\phi_g(C(a)) \subseteq C(gag^{-1})$ means exactly that the elements in $\phi_g(C(a))$ commute with the element gag^{-1}, since this is how we define the set $C(gag^{-1})$. Since elements of $\phi_g(C(a))$ are of the form gcg^{-1} where $c \in C(a)$ (i.e. c commutes with a), this means we must show $(gcg^{-1})(gag^{-1}) = (gag^{-1})(gcg^{-1})$.

    Once we have shown this first containment, we'll show the other: $C(gag^{-1}) \subseteq \phi_g(C(a))$. That is, we will show that all elements which commute with gag^{-1} have the form gcg^{-1} for some $c \in C(a)$. This is the same as saying that ϕ_g maps $C(a)$ *onto* $C(gag^{-1})$, and so we go about proving this as we generally do: take an arbitrary element $z \in C(gag^{-1})$, find a $c \in C(a)$ so that $\phi_g(c) = z$. But we know the unique preimage of z is $\phi_g^{-1}(z) = g^{-1}zg$, so we need only verify that this element is the c we were looking for - that is, we need to verify that $c = g^{-1}zg$ is, indeed, a member of $C(a)$. But this just means we need to show that $c = g^{-1}zg$ commutes with a.

16. **Question:** For the isomorphism between D_3 and S_3, how do we know which element in D_3 maps to which element in S_3?

    Answer: The short answer here is: by the process of elimination, primarily using the fact that we know that the order of an element should be the same as the order of it's image under an isomorphism, and that isomorphisms preserve the operation.

Let's say $\psi : D_3 \to S_3$. Then, first of all, we know that the identity has to go to the identity, so $\psi(R_0) = (1)(2)(3) = \epsilon \in S_3$. Next, we know that the elements R_{120} and R_{240} each have order 3, so their images should also have order 3. There are two such elements of S_3: $(1, 2, 3)$ and $(1, 3, 2)$. Similarly, the images of F, F', and F'' should be the elements of order 2 in S_3, which are $(1, 2)$, $(1, 3)$, and $(2, 3)$.

The final step of determining specifically $\psi(R_{120})$, $\psi(R_{240})$, $\psi(F)$, $\psi(F')$ and $\psi(F'')$ requires making use of the homomorphism property of isomorphisms (the preservation of the operation). That is, we need to make sure that our choices agree with the operation in each group... but there is a choice involved (that is, there is more than one isomorphism between these groups!).

So, let's say we choose $\psi(R_{120}) = (1, 2, 3)$. Then this forces $\psi(R_{240}) = \psi(R_{120} \cdot R_{120}) = \psi(R_{120}) \circ \psi(R_{120}) = (1, 2, 3) \circ (1, 2, 3) = (1, 3, 2)$.

We still have a choice for $\psi(F)$, $\psi(F')$ and $\psi(F'')$, but as soon as we choose one of these, the other two will be specified. For example, if we choose $\psi(F) = (1, 2)$. Then $\psi(F') = \psi(R_{120} \cdot F) = \psi(R_{120}) \circ \psi(F) = (1, 2, 3) \circ (1, 2) = (1, 3)$, and $\psi(F'') = \psi(F \cdot R_{120}) = \psi(F) \circ \psi(R_{120}) = (1, 2) \circ (1, 2, 3) = (2, 3)$.

17. **Question:** Are we expected to know how to come up with formulas for homomorphisms, isomorphism, and automorphisms?

    Answer: Not from scratch, no. But, if I give you some information, and I tell you that it is enough information to specify an entire map, you should know how to use the properties of that map (be it a homomorphism, isomorphism or automorphism) to either give a general formula for the map or to specify the image of each group element.

    For example, if I give you: $\alpha : S_3 \to D_3$ is an isomorphism and I tell you that $\alpha((1, 2)) = F$ and $\alpha((1, 2, 3)) = R_{120}$, you should be able to use the fact that α is an isomorphism to specify $\alpha((1, 3))$, $\alpha((2, 3))$, $\alpha((1, 3, 2))$ (and of course, you should always know what $\alpha(\epsilon)$ is).

    Similarly, if I tell you that $\beta : Z_{12} \to Z_4$ is a homomorphism, and $\beta(1) = 3$, you should be able to describe $\beta(x)$ generally or even specify $\beta(2)$, $\beta(3)$, $\beta(4)$, etc.

    Similarly, if I tell you that $\gamma : Z_{12} \to Z_4$ is a homomorphism, and $\gamma(5) = \bar{3}$, you should be able to describe $\gamma(x)$ generally. Since this example is a little more complicated than the last, I'll do the whole thing here:

$$\begin{aligned}
\gamma(5) &= \bar{3} \\
\gamma(10) = \gamma(5+5) &= \gamma(5)+\gamma(5)\ (mod\ 4) = \bar{3}+\bar{3}\ (mod\ 4) = \bar{2} \\
\gamma(3) = \gamma(5+10\ (mod\ 12)) &= \gamma(5)+\gamma(10)\ (mod\ 4) = \bar{3}+\bar{2}\ (mod\ 4) = \bar{1} \\
\gamma(8) = \gamma(5+3) &= \gamma(5)+\gamma(3)\ (mod\ 4) = \bar{3}+\bar{1}\ (mod\ 4) = \bar{0} \\
\gamma(1) = \gamma(5+8\ (mod\ 12)) &= \gamma(5)+\gamma(8)\ (mod\ 4) = \bar{3}+\bar{0} = \bar{3} \\
\gamma(6) = \gamma(5+1) &= \gamma(5)+\gamma(1)\ (mod\ 4) = \bar{3}+\bar{3}\ (mod\ 4) = \bar{2} \\
\gamma(11) = \gamma(5+6) &= \gamma(5)+\gamma(6)\ (mod\ 4) = \bar{3}+\bar{2}\ (mod\ 4) = \bar{1} \\
\gamma(4) = \gamma(5+11\ (mod\ 12)) &= \gamma(5)+\gamma(11)\ (mod\ 4) = \bar{3}+\bar{1}\ (mod\ 4) = \bar{0} \\
\gamma(9) = \gamma(5+4) &= \gamma(5)+\gamma(4)\ (mod\ 4) = \bar{3}+\bar{0}\ (mod\ 4) = \bar{3} \\
\gamma(2) = \gamma(5+9\ (mod\ 12)) &= \gamma(5)+\gamma(9)\ (mod\ 4) = \bar{3}+\bar{3}\ (mod\ 4) = \bar{2} \\
\gamma(7) = \gamma(5+2) &= \gamma(5)+\gamma(2)\ (mod\ 4) = \bar{3}+\bar{2}\ (mod\ 4) = \bar{1} \\
\gamma(0) = \gamma(5+7\ (mod\ 12)) &= \gamma(5)+\gamma(7)\ (mod\ 4) = \bar{3}+\bar{1}\ (mod\ 4) = \bar{0}
\end{aligned}$$

Note: Numbers with bars over them, $\bar{0}$, $\bar{1}$, $\bar{2}$, and $\bar{3}$ are elements of Z_4. Numbers without bars over them are elements of Z_{12}.

18. **Question:** Could you explain Example 4 in Chapter 8? (pg 157)

Answer: The text in red below is an excerpt from Joseph Gallian's Contemporary Abstract Algebra, 7^{th} ed., page 157:

Example 4: We determine the number of elements of order 5 in $Z_{25} \oplus Z_5$. By Theorem 8.1, we may count the number of elements (a, b) in $Z_{25} \oplus Z_5$ with the property that $5 = |(a, b)| = lcm(|a|, |b|)$. Clearly this requires that either $|a| = 5$ and $|b| = 1$ or 5, or $|b| = 5$ and $|a| = 1$ or 5. We consider two mutually exclusive cases.

Case 1: $|a|$=5 and $|b| = 1$ or 5. Here there are four choices for a (namely 5, 10, 15 and 20) and five choices for b. This gives 20 elements of order 5.

I'll pause for a moment to explain their reasoning. Since Z_{25} is a cyclic group and $|a| = 5$ is a divisor of its order, the Fundamental Theorem of Cyclic Groups tells us there are $\phi(5) = 4$ elements of Z_{25} of order 5. We know one of these elements is $25/5 = 5$, and the others are the multiples $k \cdot 5$ where k is relatively prime to 25. So, these multiples are $5, 10, 15, 20$. The elements of Z_5 all have order 1 or 5 ($|0| = 1$ and $|1| = |2| = |3| = |4| = 5$), so this is why there are 5 elements of Z_5 with orders 1 or 5. There are $4 \times 5 = 20$ ways of combining these possibilities for a and b to obtain elements of $Z_{25} \oplus Z_5$: $(5, 0)$, $(5, 1)$, $(5, 2)$, $(5, 3)$, $(5, 4)$, $(10, 0)$, $(10, 1)$, $(10, 2)$, $(10, 3)$, $(10, 4)$, $(15, 0)$, $(15, 1)$, $(15, 2)$, $(15, 3)$, $(15, 4)$, $(20, 0)$, $(20, 1)$, $(20, 2)$, $(20, 3)$, and $(20, 4)$. Now we continue with the second case:

Case 2: $|a| = 1$ and $|b| = 5$. This time there is one choice for a and four choices for b, so we obtain four more elements of order 5.

Thus, $Z_{25} \oplus Z_5$ has 24 elements of order 5.

Again, they appeal to the Fundamental Theorem of Cyclic Groups to count how many elements of order 5 are in Z_5. There are, once again, $\phi(5) = 4$ of them: 1,2,3, and 4. And, as always, there is only one element of order 1 - the identity. So the elements $(0,1)$, $(0,2)$, $(0,3)$, and $(0,4)$ in $Z_{25} \oplus Z_5$ have order 5. Now our list has 24 elements.

19. **Question:** Could you explain Example 5 in Chapter 8? (pg 157)

    Answer: For this example, I won't reproduce the entire thing since the first part of it is very similar to the last example. Instead, I'll focus on the last part, which is copied below:

    Thus $Z_{100} \oplus Z_{25}$ has 24 elements of order 10. Because each cyclic subgroup of order 10 has four elements of order 10 and no two of the cyclic subgroups can have an element of order 10 in common, there must be 24/4=6 cyclic subgroups of order 10. (This method is analogous to determining the number of sheep in a flock by counting the legs and dividing by 4.)

    So, the point of the example is to use what we know about the orders of elements in direct products to help us count the number of cyclic subgroups of a given order in the direct product $Z_{100} \oplus Z_{25}$. Once we have counted, and find that there are 24 elements of order 10, the book asks us to notice that if (a, b) is an element of order 10, so is $(3a, 3b)$, $(7a, 7b)$ and $(9a, 9b)$ (each multiple $k \cdot (a, b)$ for k relatively prime to 10). Furthermore, we know that each of these elements generates the *same* subgroup of order 10. So, since we want to count the number of distinct cyclic subgroups of order 10, and we know there is one distinct group for every four elements of order 10, we conclude that there are 24/4=6, total.

20. **Question:** If p is a prime other than 2, why is $U(2p)$ isomorphic to Z_{p-1}?

    Answer: By Theorem 8.3, $U(2p) \cong U(2) \oplus U(p)$. But, $U(2) = \{1\}$ and $U(p)$ is cyclic of order $p - 1$, so $U(p) \cong Z_{p-1}$. But, the direct product of the trivial group with another group is just that other group: $\{e\} \oplus G \cong G$ (via the isomorphism taking (e, g) to g). Thus, $U(2p) \cong U(2) \oplus U(p) \cong \{1\} \oplus Z_{p-1} \cong Z_{p-1}$.

21. **Question:** In class, we saw some examples of direct products of finite cyclic groups. Sometimes these direct products were not cyclic, but other times they were, and for these we found another cyclic group to which they were isomorphic. For instance, $Z_{12} \oplus Z_6$ wasn't cyclic but $Z_3 \oplus Z_8$ was cyclic, and was isomorphic to Z_{24}. I understand that $Z_3 \oplus Z_8$ is cyclic because $gcd(3, 8) = 1$, and we have a therorem about that, but I'm not quite sure I understand how we know that it's isomorphic to Z_{24}.

    Answer: Theorem 8.2 is the one which tells us when a direct product of finite cyclic groups is again cyclic. It says, if G and H are finite cyclic groups, $G \oplus H$ is cyclic if and only if $\gcd(|G|, |H|) = 1$. It doesn't specify that $G \oplus H \cong Z_{|G|\cdot|H|}$, but this is the case. We know that the order of a direct product is the product of the orders of the component groups: $|G \oplus H| = |G| \cdot |H|$. So, if $G \oplus H$ is cyclic, then it is a cyclic group of order $|G| \cdot |H|$, and this is isomorphic to $Z_{|G|\cdot|H|}$.

    To see why this last statement is true, I'll prove something more general: Let G be a finite cyclic group of order n, then $G \cong Z_n$. Since G is cyclic, we know there is at least

1 generator of the group, so let $a \in G$ be a generator (i.e. $\langle a \rangle = G$). Then, for every element $g \in G$, there is a $k \in \mathbb{Z}$ s.t. $a^k = g$. Now, let $\gamma : G \to Z_n$ via $\gamma(g) = k\ (mod\ n)$.

Let $g = a^k$ and $g' = a^l$ be elements of G. Then $\gamma(gg') = \gamma(a^{k+l}) = k + l\ (mod\ n)$. But, $\gamma(g) + \gamma(g')\ (mod\ n) = k + l\ (mod\ n)$, so we see that γ is a homomorphism. Now, suppose that $\gamma(g) = \gamma(g')$, then $k \equiv l\ (mod\ n)$, which means that $k = mn + l$ for some $m \in \mathbb{Z}$. But then $g = a^k = a^{mn+l} = a^{mn}a^l = (a^n)^m a^l = e^m a^l = a^l = g'$, so γ is one-to-one. Now, since γ is a map from a finite set to another finite set of the same size, we could stop here, but instead, we'll show that it's onto, as well.

Let $k \in Z_n$. Then $a^k \in G$ and $\gamma(a^k) = k$. So, now we have shown that every cyclic group of order n is isomorphic to Z_n.

22. **Question:** I understand more or less how external direct products work when only Z_n groups or $U(m)$ groups are involved. Though I have trouble visualizing how to do the products of two different types of group (such as D_3 and S_4 for example). Can this even be done?

    Answer: Yes! Let's consider the elements $(R_{120}, (1,2,3,4))$ and $(F, (1,2)(3,4))$ in the direct product $D_3 \oplus S_4$. Their product is: $(R_{120}, (1,2,3,4))(F, (1,2)(3,4)) = (R_{120}F, (1,2,3,4)(1,2)(3,4)) = (F', (1,3)(2)(4)) = (F', (1,3)) \in D_3 \oplus S_4$.

    While we're on the subject, let's compute the order of each of these elements: $|(R_{120}, (1,2,3,4))| = lcm(|R_{120}|, |(1,2,3,4)|) = lcm(3,4) = 12$ (recall that $|R_{120}| = 3$ in D_3 and the order of a cycle is it's length). $|(F, (1,2)(3,4))| = lcm(|F|, |(1,2)(3,4)|) = lcm(2, lcm(2,2)) = 2$ (recall that the order of a product of disjoint cycles, like $(1,2)(3,4)$, is the lcm of the cycle lengths).

23. **Question:** I don't really understand theorem 8.3 (specifically the line where it says that $U_s(st) \cong U(t)$ and $U_t(st) \cong U(s)$).

    Answer: In the general direct product setting, if we have $G \cong H \oplus K$, then by Theorem 6.3, there are subgroups $\widetilde{H} \leq G$ and $\widetilde{K} \leq G$ with $H \cong \widetilde{H}$ and $K \cong \widetilde{K}$ since $K \cong \{e_H\} \oplus K \leq H \oplus K \cong G$ and $H \cong H \oplus \{e_K\} \leq H \oplus K \cong G$.

    The book introduces the notation $U_k(n)$ and then uses this notation in Theorem 8.3 to specify that in the case of $U(st) \cong U(s) \oplus U(t)$, we can identify these subgroups $\widetilde{U(s)}$ and $\widetilde{U(t)}$. Namely, $U_t(st) \leq U(st)$ and $U_t(st) \cong U(s)$ (i.e. $U_t(st) = \widetilde{U(s)}$). A similar statement holds for $U_s(st)$.

24. **Question:** When we did the example in class on left cosets, we had $G = Z_{12}$ and $H = \langle 4 \rangle$. We listed the cosets of H in G as: $4 + H$, $3 + H$, $2 + H$, and $1 + H$. Are these the only cosets? can't we have $x + H$ for $0 \leq x < 12$? I wasn't sure if we just didn't list them all in class, or if you can't actually have them all.

    Answer: These are all of the *distinct* cosets. Let's calculate them all here to see what that means:

$$\begin{aligned}
0+H=\{0+0,0+4,0+8\} &= \{0,4,8\}=H\\
1+H=\{1+0,1+4,1+8\} &= \{1,5,9\}\\
2+H=\{2+0,2+4,2+8\} &= \{2,6,10\}\\
3+H=\{3+0,3+4,3+8\} &= \{3,7,11\}\\
4+H=\{4+0,4+4,4+8\} &= \{4,8,0\}=H\\
5+H=\{5+0,5+4,5+8\} &= \{5,9,1\}=1+H\\
6+H=\{6+0,6+4,6+8\} &= \{6,10,2\}=2+H\\
7+H=\{7+0,7+4,7+8\} &= \{7,11,3\}=3+H\\
8+H=\{8+0,8+4,8+8\} &= \{8,0,4\}=4+H=H\\
9+H=\{9+0,9+4,9+8\} &= \{9,1,5\}=5+H=1+H\\
10+H=\{10+0,10+4,10+8\} &= \{10,2,6\}=6+H=2+H\\
11+H=\{11+0,11+4,11+8\} &= \{11,3,7\}=7+H=3+H
\end{aligned}$$

So, yes, there is a coset $x+H$ for each $x \in \{0,1,\dots 11\}$, but even if $x \neq 1,2,3,4$, the coset $x+H$ will be the same as one of $1+H$, $2+H$, $3+H$ or $4+H$.

25. **Question:** How do we determine the cosets for more complicated groups, of which we do not know all the elements?

    Answer: We will never work with any groups whose elements are unknown. Even if the group is infinite - or just very large - so that it would be impossible (or impractical) to write down all of the group elements, we will at least always have some description of a typical element (as in matrix groups), and using this, we could write down descriptions of the cosets.

    For example, consider the group S_8. Then we know that $A_8 \leq S_8$ (the even permutations form a subgroup). Since $|A_8| = |S_8|/2$, we know there are two cosets of A_8 in S_8. We also know that if a permutation is not in A_8, this means it is odd. So the two cosets of A_8 are the even permutations and the odd permutations. One coset representative of the odd permutations is $(1,2)$ (since $(1,2)$ is an odd permutation), so we can write the two cosets as A_8 and $(1,2)A_8$.

26. **Question:** When we were proving the Normal Subgroup Test, we went from $xhx^{-1} \in H$, to $xh \in Hx$. Also, just to be clear, Hx means "the right coset containing x," right?

    Answer: First, if $xhx^{-1} \in H$, this means $xhx^{-1} = h'$ for some $h' \in H$. But then, $xh = h'x$, which means exactly that $xh \in Hx$. Secondly, yes, Hx is the right coset containing x. So, the following statements are equivalent:

    (a) H is a normal subgroup of G

    (b) $xH = Hx$ for all $x \in G$ (read: the left coset containing x is the same set as the right coset containing x)

    (c) $xhx^{-1} \in H$ for any $h \in H$ and any $x \in G$

(d) $xh \in Hx$ (the element xh is an element of the right coset containing x for any $x \in G$ and $h \in H$)

Note: this is not an exhaustive list of equivalent statements.

27. **Question:** For normal subgroups, why does $aH = Ha$ not imply that $ah = ha$ for all h? Can we possibly do an example that shows that?

Answer: Consider the example in class where $G = D_4$ and $R = \{R_0, R_{90}, R_{180}, R_{270}\}$. There are only two left cosets of this subgroup, the rotations and the reflections: R and $HR = VR = DR = D'R = \{H, V, D, D'\}$. The right and left cosets computations are given below:

$$\begin{aligned}
R_0R = \{R_0R_0, R_0R_{90}, R_0R_{180}, R_0R_{270}\} &= \{R_0, R_{90}, R_{180}, R_{270}\} \\
RR_0 = \{R_0R_0, R_{90}R_0, R_{180}R_0, R_{270}R_0\} &= \{R_0, R_{90}, R_{180}, R_{270}\} = R_0R \\
R_{90}R = \{R_{90}R_0, R_{90}R_{90}, R_{90}R_{180}, R_{90}R_{270}\} &= \{R_{90}, R_{180}, R_{270}, R_0\} \\
RR_{90} = \{R_0R_{90}, R_{90}R_{90}, R_{180}R_{90}, R_{270}R_{90}\} &= \{R_{90}, R_{180}, R_{270}, R_0\} = R_{90}R \\
R_{180}R = \{R_{180}R_0, R_{180}R_{90}, R_{180}R_{180}, R_{180}R_{270}\} &= \{R_{180}, R_{270}, R_0, R_{90}\} \\
RR_{180} = \{R_0R_{180}, R_{90}R_{180}, R_{180}R_{180}, R_{270}R_{180}\} &= \{R_{180}, R_{270}, R_0, R_{90}\} = R_{180}R \\
R_{270}R = \{R_{270}R_0, R_{270}R_{90}, R_{270}R_{180}, R_{270}R_{270}\} &= \{R_{270}, R_0, R_{90}, R_{180}\} \\
RR_{270} = \{R_0R_{270}, R_{90}R_{270}, R_{180}R_{270}, R_{270}R_{270}\} &= \{R_{270}, R_0, R_{90}, R_{180}\} = R_{270}R \\
HR = \{HR_0, HR_{90}, HR_{180}, HR_{270}\} &= \{H, D, V, D'\} \\
RH = \{R_0H, R_{90}H, R_{180}H, R_{270}H\} &= \{H, D', V, D\} = HR \\
VR = \{VR_0, VR_{90}, VR_{180}, VR_{270}\} &= \{V, D', H, D\} \\
RV = \{R_0V, R_{90}V, R_{180}V, R_{270}V\} &= \{V, D, H, D'\} = VR \\
DR = \{DR_0, DR_{90}, DR_{180}, DR_{270}\} &= \{D, V, D', H\} \\
RD = \{R_0D, R_{90}D, R_{180}D, R_{270}D\} &= \{D, H, D', V\} = DR \\
D'R = \{D'R_0, D'R_{90}, D'R_{180}, D'R_{270}\} &= \{D', H, D, V\} \\
RD' = \{R_0D', R_{90}D', R_{180}D', R_{270}D'\} &= \{D', V, D, H\} = D'R
\end{aligned}$$

So, we can see that for each $a \in D_4$, $aR = Ra$ (so, $R \lhd D_4$), *but* if we take an isolated element of R, say R_{90}, we don't have $aR_{90} = R_{90}a$ for any a which is not a rotation. In particular, if $a = H$, $HR_{90} = D$ but $R_{90}H = D'$. So elements of normal subgroups do not have to commute with all elements of the group.