1. Suppose that $G$ is a finite group with subgroups $A$ and $B$. Prove that $o(AB) = o(A)o(B)/o(A \cap B)$. Note that typically, $AB$ will just be a subset of $G$ and not a subgroup. 

**Answer:** We define the function $f : A \times B \to AB$ with $f(a,b) = ab$. The function is trivially surjective. There are $o(A)o(B)$ elements in the domain, and $o(AB)$ elements in the codomain. If $ab \in AB$, we need to find out how many elements there are in the set $f^{-1}(ab)$.

Suppose that $f(c,d) = f(a,b)$. Then we have $cd = ab$, so $a^{-1}c = bd^{-1}$. Because $a^{-1}c \in A$ and $bd^{-1} \in B$, we know that $a^{-1}c = bd^{-1} \in A \cap B$. In other words, every element in $f^{-1}(ab)$ produces an element in $A \cap B$. Can two different elements of $f^{-1}(ab)$ produce the same element of $A \cap B$? In other words, if $f(c,d) = f(a,b) = f(c',d')$, does $a^{-1}c = a^{-1}c'$? Because of cancellation, that can happen only if $c = c'$.

Does every element of $A \cap B$ produce an element of $f^{-1}(ab)$? Yes: If $r \in A \cap B$, then $(ar,r^{-1}b) \in f^{-1}(ab)$.

So there is a one-to-one correspondence between elements of $A \cap B$ and elements of $f^{-1}(ab)$, which shows that $o(A)o(B)/o(A \cap B) = o(AB)$.

2. If $(m,n) = 1$, show that the only group homomorphism $\phi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is the trivial homomorphism. Remember that the group operation is addition.

**Answer:** Choose any element $a \in \mathbb{Z}/m\mathbb{Z}$. We know that $o(\phi(a))|o(a)$. The corollary to Lagrange’s Theorem tells us that $o(\phi(a))|o(\mathbb{Z}/m\mathbb{Z})$, or $o(\phi(a))|m$, implying that $o(\phi(a))|m$. But the corollary to Lagrange’s Theorem also tells us that $o(\phi(a))|n$. Because $(m,n) = 1$, we have $o(\phi(a)) = 1$, meaning that $\phi(a) = 0$. Because $a$ was arbitrary, we can conclude that $\phi$ is trivial.

3. Find a non-trivial group homomorphism $\phi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$.

**Answer:** Remember that $o(\phi(a))|o(a)$. In this case, if $a \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and $a \neq (0,0)$, then $o(a) = 2$, so we have $o(\phi(a)) = 1$ or $2$. There are actually $3$ different non-trivial homomorphisms:

\begin{align*}
\phi_1 : & (0,0) \to 0 & (0,0) \to 0 & (0,0) \to 0 \\
& (1,0) \to 2 & (1,0) \to 2 & (1,0) \to 0 \\
& (0,1) \to 2 & (0,0) \to 0 & (0,1) \to 2 \\
& (1,1) \to 0 & (1,1) \to 2 & (1,1) \to 2
\end{align*}

In each case, it’s easy to see that $\phi(x + y) = \phi(x) + \phi(y)$, which is the requirement that $\phi$ must satisfy.

4. Find a non-trivial group homomorphism $\phi : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

**Answer:** If $\phi(1) = (0,0)$, then $\phi$ is trivial. Each of the other $3$ possibilities gives a homomorphism:

\begin{align*}
\phi_1 : & 0 \to (0,0) & 0 \to (0,0) & 0 \to (0,0) \\
& 1 \to (1,0) & 1 \to (0,1) & 1 \to (1,1) \\
& 2 \to (0,0) & 2 \to (0,0) & 2 \to (0,0) \\
& 3 \to (1,0) & 3 \to (0,1) & 3 \to (1,1)
\end{align*}
5. Remember that the Hamiltonians $H$ are defined by $H = \{x_1 + ix_2 + jx_3 + kx_4 : x_1, x_2, x_3, x_4 \in \mathbb{R}\}$ with $ij = k$, $jk = i$, $ki = j$, and $i^2 = j^2 = k^2 = -1$. Show there are infinitely many elements $x \in H$ satisfying $x^2 = -1$.

**Answer:** To avoid the nuisance of typing subscripts, let $x = a + bi + cj + dk$, with $a, b, c, d \in \mathbb{R}$. We compute (or find from the text) that $x^2 = a^2 - b^2 - c^2 - d^2 + 2abi + 2acj + 2adk$. If we set this equal to $-1$, we conclude that

$$a^2 - b^2 - c^2 - d^2 = -1$$

$$2ab = 0$$

$$2ac = 0$$

$$2ad = 0$$

Now, if $a \neq 0$, we are forced to conclude from the final three equations that $b = c = d = 0$, and then $a^2 = -1$ has no solutions.

However, if we set $a = 0$, then the final three equations are automatically satisfied, and we are left with $b^2 + c^2 + d^2 = 1$. This equation has infinitely many solutions—for example, set $b = \cos \theta$ and $c = \sin \theta$ and $d = 0$—and each solution will imply that $x^2 = -1$.

6. If $R$, $S$ are rings, define the **direct sum** of $R$ and $S$, $R \oplus S$, by

$$R \oplus S = \{(r, s) : r \in R, s \in S\}$$

where $(r, s) = (r_1, s_1)$ if and only if $r = r_1$ and $s = s_1$, and where we define

$$(r, s) + (t, u) = (r + t, s + u), \quad (r, s)(t, u) = (rt, su).$$

(a) Show that $R \oplus S$ is a ring.

(b) Show that $\{(r, 0) : r \in R\}$ and $\{(0, s) : s \in S\}$ are ideals of $R \oplus S$.

(c) Show that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ is ring isomorphic to $\mathbb{Z}/6\mathbb{Z}$.

(d) Show that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is not ring isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

**Answer:** (a) First, the identity element for addition is $(0_R, 0_S)$, and the identity element for multiplication is $(1_R, 1_S)$. Second, we see that $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) = (r_2 + r_1, s_2 + s_1) = (r_2, s_2) + (r_1, s_1)$, showing that addition is commutative; the demonstration that addition is associative is similar.

Third, we check the distributive law: $(r_1, s_1)((r_2, s_2) + (r_3, s_3)) = (r_1, s_1)(r_2 + r_3, s_2 + s_3) = (r_1(r_2 + r_3), s_1(s_2 + s_3)) = (r_1r_2, r_1r_3, s_1s_2 + s_1s_3) = (r_1r_2, s_1s_2) + (r_1r_3, s_1s_3) = (r_1, s_1)(r_2, s_2) + (r_1, s_1)(r_3, s_3))$. The distributive law on the right side is checked similarly.

(b) We have $(r_1, 0) + (r_2, 0) = (r_1 + r_2, 0)$, showing that the set is closed under addition. We also have $(r_1, 0)(r_2, s_2) = (r_1r_2, 0s_2) = (r_1r_2, 0)$, which again is in the set. Therefore, the set is an ideal. The demonstration is exactly the same for the other ideal.

(c) Remember that we insist that if $\phi : R_1 \rightarrow R_2$ is a homomorphism, then $\phi(1_{R_1}) = 1_{R_2}$. Therefore, a homomorphism $\phi$ from $\mathbb{Z}/6\mathbb{Z}$ to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ must satisfy $\phi(1) = (1, 1)$. Therefore, the only homomorphism is

$$\phi :$$

$$\begin{align*}
0 &\rightarrow (0, 0) \\
1 &\rightarrow (1, 1) \\
2 &\rightarrow (0, 2) \\
3 &\rightarrow (1, 0) \\
4 &\rightarrow (0, 1) \\
5 &\rightarrow (1, 2)
\end{align*}$$

"
and this is obviously a bijection.

\( d \) Suppose that \( \phi : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \) is a homomorphism. The requirement that \( \phi(1_{R_1}) = 1_{R_2} \) again gives no choice about the function:

\[
\begin{align*}
0 & \to (0,0) \\
1 & \to (1,1) \\
2 & \to (0,0) \\
3 & \to (1,1)
\end{align*}
\]

This is obviously neither an injection nor a surjection, so it is not an isomorphism.