1. Exercises from the book:

- **14. 39**: We define $\phi_*$ so that it sends the left coset of $H$ in $G$ generated by $a$ to the left coset of $H'$ in $G'$ generated by $\phi(a)$ (the only "natural way" that we can define $\phi_*), so if $aH$ is a left coset of $H$ in $G$,

$$\phi_*(aH) := \phi(a)H'.$$

We need to show that this is a well-defined function from the set of left cosets of $H$ in $G$ to the set of left cosets of $H'$ in $G'$. After showing this, we show that $\phi_*$ is a homomorphism.

To show that $\phi_*$ is well-defined, we need to show that if $aH = bH$, then $\phi_*(aH) = \phi_*(bH)$ that is $\phi(a)H' = \phi(b)H'$. Since $aH = bH$, $a^{-1}b \in H$. Since $\phi$ sends elements of $H$ to elements of $H'$, $\phi(a^{-1}b) \in H'$, so $\phi(a)^{-1}\phi(b) \in H'$, so $\phi(a)H' = \phi(b)H'$.

To show that $\phi_*$ is a homomorphism, note that

$$\phi_*(aHbH) = \phi_*(abH)$$
$$= \phi(ab)H'$$
$$= \phi(a)\phi(b)H'$$
$$= (\phi(a)H') (\phi(b)H')$$
$$= \phi_*(aH)\phi_*(bH).$$

- **15. 11**: We show that $\langle \mathbb{Z} \times \mathbb{Z} \rangle / \langle (2,2) \rangle \cong \mathbb{Z} \times \mathbb{Z}_2$ by describing an isomorphism from the first group to the second group. Let $H = \langle (2,2) \rangle$. Then $(a,b) + H = (a',b') + H$ (we use the addition to denote the group operation in $\mathbb{Z} \times \mathbb{Z}$) if and only if $-(a,b) + (a',b') \in H, that is a' - a, b' - b \in 2\mathbb{Z}$.

Let

$$\phi: \langle \mathbb{Z} \times \mathbb{Z} \rangle / H \to \mathbb{Z} \times \mathbb{Z}_2$$

be the function $\phi((a,b) + H) = (a - b, [b]), that is

$$\phi((a,b) + H) = \begin{cases} 
(a - b, 0) & \text{if } b \text{ is even} \\
(a - b, 1) & \text{if } b \text{ is odd.}
\end{cases}$$
This is a well-defined function: if \((a, b) + H = (a', b') + H\), then \((a' - a, b' - b) = (2k, 2k)\) for some \(k \in \mathbb{Z}\). So \(b\) is odd if and only if \(b'\) is odd, and also, \(a' - a = b' - b\) so \(a - b = a' - b'\). Thus
\[
\phi((a, b) + H) = (a - b, [b]) = (a' - b', [b']) = \phi((a', b') + H).
\]

\(\phi\) is one-to-one: we show \(\text{Ker}(\phi)\) is the zero coset \(H\). If \(\phi((a, b) + H) = (0, 0)\), then \(a = b\) and \(b\) is even, so both \(a\) and \(b\) are even, so \((a, b) \in H\), so \((a, b) + H = H\).

\(\phi\) is onto: for \((a, 0) \in \mathbb{Z} \times \mathbb{Z}_2\), \(\phi((a, 0) + H) = (a, 0)\), and for \((a, 1) \in \mathbb{Z} \times \mathbb{Z}_2\), \(\phi((a + 1, 1) + H = (a, 1)\).

\(\phi\) is a group homomorphism:
\[
\phi((a, b) + H + (a', b') + H) = \phi((a + a', b + b') + H)
= (a + a' - b - b', [b + b'])
= ((a - b) + (a' - b'), [b] + [b'])
= (a - b, [b]) + (a' - b', [b'])
= \phi((a, b) + H) + \phi((a', b') + H)
\]

\[\textbf{15. 37:}\] Assume that \(G/Z(G)\) is generated by \(aZ(G)\). If \(a \in Z(G)\), then \(aZ(G)\) the trivial element of \(G/Z(G)\) and hence \(G/Z(G)\) has only one element. So \(G = Z(G)\), and we are done.

Otherwise, \(a \notin Z(G)\), so there is \(b \in G\) such that \(ab \neq ba\). Consider the left coset generated by \(b\), \(bZ(G)\). Since \(G/Z(G)\) is generated by \(aZ(G)\), there is \(i\) such that
\[bZ(G) = (aZ(G))^i.\]
Note that by the definition of the group operation on \(G/Z(G)\), \((aZ(G))^i = a^iZ(G)\), so \(bZ(G) = a^iZ(G)\), so \(a^{-i}b \in Z(G)\). This means that \(a^{-i}b\) commutes with every element of \(G\), in particular
\[a(a^{-i}b) = (a^{-i}b)a,\]
so \(a^{1-i}b = a^{-i}ba\). If we cancel \(a^{-i}\) from the left side of the equality, we get \(ab = ba\) which is contradicting the assumption that \(a\) does not commute with \(b\).

2. Prove that every group \(G\) of order 6 is isomorphic to \(\mathbb{Z}_6\) or \(S_3\).

\[\textbf{Solution:}\] The order of any element other than the identity in \(G\) is 2, 3, or 6. If there is an element of order 6, then \(G \simeq \mathbb{Z}_6\).

Now assume that there is no element of order 6. We show that it is not possible that every element of \(G\) other than the identity has order
2. Recall from a previous homework problem that if \( a^2 = e \) for all elements in a group, then the group should be abelian. Now assume to the contrary that every element of \( G \) other than the identity has order 2, and pick elements \( a \neq b \) in \( G \) such that \( a \neq e \) and \( b \neq e \). Then \( H := \{e, a, b, ab\} \) should be a subgroup of \( G \) since it is closed under group operation \((a^2 = e, b^2 = e, (ab)^2 = e, ab \in H, ba = ab \in H, a(ab) = b \in H, b(ab) = (ab)b = a \in H)\). But this is not possible since a group of order 6 cannot have a subgroup of order 4.

Pick now an element \( a \) of order 3 in \( G \) and an element \( b \notin \langle a \rangle = \{e, a, a^2\} \). Then \( e, a, a^2, b, ba, ba^2 \) are all distinct, and therefore they should be all the elements of \( G \). To see this, note that clearly \( e, a, a^2, b \) are all distinct. \( ba \neq b, ba \neq a, ba \neq e \) (since otherwise \( b \) would be the inverse of \( a \) which is \( a^2 \), but we assumed \( b \notin \{e, a, a^2\} \)), and \( ba \neq a^2 \) (since \( b \neq a \)). Similarly \( ba^2 \) is not equal to any of the other 5 elements, so \( G = \{e, a, a^2, b, ba, ba^2\} \).

We now show that \( b \) has order 2. We assumed \( G \) does not have any element of order 6. If \( b^3 = e \), then 
\[
\begin{align*}
b^2 &\in \{a, a^2, b, ab, ab^2\}. \end{align*}
\]
Clearly, \( b^2 \) cannot be equal to \( b, ab, \) or \( ab^2 \). If \( b^2 = a \), then 
\[
\begin{align*}
e = b^3 = b(b^2) = ba
\end{align*}
\]
which is not possible. Similarly, if \( b^2 = a^2 \), then 
\[
\begin{align*}
b = be = b(b^3) = b^4 = a^4 = e
\end{align*}
\]
which is not possible. So the only possibility is that \( b^2 = e \), that is \( b \) has order 2.

Now \( ab \) is either equal to \( ba \) or \( ba^2 \). This is because \( ab \neq e, a, a^2 \) or \( b \). If \( ab = ba \), then the order of \( ab \) should be 6: if \( (ab)^2 = e \), then 
\[
\begin{align*}
a^2 = a^2b^2 = (ab)^2 = e
\end{align*}
\]
which is not possible. If \( (ab)^3 = e \), then 
\[
\begin{align*}
e = (ab)^3 = a^3b^3 = eb = b
\end{align*}
\]
So \( ab \) has order 6, but we assumed there is no element of order 6, so \( ab = ba^2 \).

Now we have the complete multiplication table in \( G \) and we can use that to show that \( G \) is isomorphic to \( S_3 \). We can also give an isomorphism explicitly. We define 
\[
\phi : G \rightarrow S_3
\]
by \( \phi(a) = (1\ 2\ 3), \phi(a^2) = (1\ 3\ 2), \phi(b) = (1\ 2), \phi(ba) = (3\ 2), \) and 
\( \phi(ba^2) = (1\ 3). \)

3. Suppose that \( G \) is a group (not necessarily finite) and \( H \) is a subgroup of \( G \) of index 2. Show that \( H \) is a normal subgroup of \( G \).

- **Solution:** We show that \( aH = Ha \) for every \( a \in G \). If \( a \in H \), then \( aH = H \) and \( Ha = H \).

Assume now \( a \notin H \). Then \( aH \cap H = \emptyset \), and every left coset of \( H \) is either equal to \( H \) or \( aH \). If \( b \notin H \), then \( bH \neq H \), so \( bH = aH \), so \( b \in aH \). This means that \( aH \) contains every element of \( G \) which is not in \( H \). So \( aH \) is the complement of \( H \) in \( G \). Similarly, \( Ha \) is the complement of \( H \) in \( G \). Thus \( aH = Ha \).

4. If \( G \) is a cyclic group of order \( n \), then find \( |\text{Aut}(G)| \).

- **Solution:** We first show that if \( \phi : G \to G' \) is a homomorphism, and if \( G \) is cyclic, then every generator of \( G \) is mapped to a generator of \( G' \) (in particular \( G' \) is also cyclic). Let \( a \) be a generator of \( G \), then for every \( a' \in G' \), \( a' = \phi(b) \) for some \( b \in G \), and \( b = a^i \) for some \( i \), so

\[ a' = \phi(b) = \phi(a^i) = \phi(a)^i. \]

This shows that \( \phi(a) \) generates \( G' \).

We now show that if \( G \) is a cyclic group of order \( n \) generated by \( a \), and if \( b \) is any other generator of \( G \), then there is a unique homomorphism \( \phi : G \to G \) such that \( \phi(a) = b \). Uniqueness is clear: if \( \phi(a) = b \), then \( \phi(a^i) \) should be equal to \( b^i \), so there is only one possibility for \( \phi \). It remains to show that \( \phi(a^i) = b^i \) defines a homomorphism which is one-to-one and onto.

\( \phi \) is well defined: if \( a^i = a^j \), then \( i - j \) is a multiple of \( n \), so \( b^{i-j} = e \), so \( b^i = b^j \). \( \phi \) is clearly an onto homomorphism, and if \( \phi(a^i) = \phi(a^j) \), then \( b^i = b^j \), so \( i - j \) is a multiple of \( n \), so \( a^i = a^j \). This shows \( \phi \) is one-to-one.

So the number of automorphisms of \( G \) is exactly the number of generators of \( G \) which is \( \phi(n) \): the number of integers \( 1 \leq i \leq n \) which are relatively prime to \( n \).