Chapter 6. Problem 10. Let \( G \) be a group. Prove that the mapping \( \alpha(g) = g^{-1} \forall g \in G \) is an automorphism if and only if \( G \) is Abelian.

**Solution:** (\( \Rightarrow \)) Let \( G \) be a group and let \( a \) and \( b \in G \). Assume that the map \( \alpha \) such that \( \alpha(g) = g^{-1} \forall g \in G \) is an automorphism. Then we know \( \alpha(ab) = \alpha(a)\alpha(b) \). But since \( ab \in G \), we can write \( \alpha(ab) = (ab)^{-1} = b^{-1}a^{-1} = \alpha(b)\alpha(a) \). Hence, \( \alpha(a)\alpha(b) = \alpha(b)\alpha(a) \), so by Theorem 6.2 (part 3), \( G \) is Abelian.

(\( \Leftarrow \)) Let \( G \) be an Abelian group and let \( a \) and \( b \in G \). Let \( \alpha : G \to G \) be the map \( \alpha(g) = g^{-1} \forall g \in G \). The existence property of inverses in a group guarantees that the map \( \alpha \) is onto and the uniqueness property guarantees that the map \( \alpha \) is one-to-one. Now, consider \( \alpha(ab) \). Since \( G \) is Abelian, \( ab = ba \) so \( \alpha(ab) = \alpha(ba) = (ba)^{-1} = a^{-1}b^{-1} = \alpha(a)\alpha(b) \). So we have \( \alpha(ab) = \alpha(a)\alpha(b) \). Hence, \( \alpha \) is an automorphism.

Chapter 6. Problem 12. Find two groups \( G \) and \( H \) such that \( G \not\approx H \), but \( \text{Aut}(G) \cong \text{Aut}(H) \).

**Solution:** Consider the groups \( Z \) (the integers under addition) and \( Z_3 \). We see immediately that \( Z \not\approx Z_3 \) since \( Z \) has an infinite number of elements while \( Z_3 \) has only 3. However, since these are both cyclic groups, we know that generators must be mapped to generators, and each of these groups has exactly two generators, hence there are exactly two automorphisms on each. Under addition, \( Z = \langle 1 \rangle = \langle -1 \rangle \), and under addition modulo 3, \( Z_3 = \langle 1 \rangle = \langle 2 \rangle \). So the automorphisms on \( Z \) are the maps \( \alpha_1 : Z \to Z : x \mapsto x \) and \( \alpha_2 : Z \to Z : x \mapsto -x \) for \( x \in Z \).

The automorphisms on \( Z_3 \) are the maps \( \beta_1 : Z_3 \to Z_3 : y \mapsto y \) and \( \beta_2 : Z_3 \to Z_3 : y \mapsto -y \) for \( y \in Z_3 \) (that is, \( 0 \mapsto 0; 1 \mapsto 2; 2 \mapsto 1 \)).

So we can compare the Cayley tables of the automorphism groups:

<table>
<thead>
<tr>
<th></th>
<th>( \alpha_1 )</th>
<th>( \alpha_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \alpha_1 )</td>
<td>( \alpha_1 )</td>
<td>( \alpha_2 )</td>
</tr>
<tr>
<td>( \alpha_2 )</td>
<td>( \alpha_2 )</td>
<td>( \alpha_1 )</td>
</tr>
</tbody>
</table>

We can see from these that \( \text{Aut}(G) \cong \text{Aut}(H) \).

Chapter 6. Problem 22. Prove or disprove that \( U(20) \) and \( U(24) \) are isomorphic.

**Solution:** These groups are not isomorphic. In \( U(24) \) every element other than the identity has order 2 (since \( 5^2 = 25 = 1 \mod 24 \), etc.). However, in \( U(20) \), the order of the element 3 is 8. Since Theorem 6.2 part 5. tells us that isomorphisms preserve order, there cannot be an isomorphism between these two groups.

Chapter 7. Problem 22. 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.
Theorem 0.2). So, to see that $\phi |$ must divide $n e$ let $\phi |$ must verify that it is a bijection that preserves the group operation. To see that

Solution 1: Let’s suppose $G$ is an infinite group. Take some $g \in G$, $g \neq e$. If $|g|$ is finite, then $\langle g \rangle$ is a proper, non-trivial subgroup of $G$, and we have a contradiction. So, suppose $|g|$ is infinite. Now, consider the subgroup $\langle g^2 \rangle$. We see that $g \notin \langle g^2 \rangle$ (since $g \in \langle g^2 \rangle \Rightarrow g = g^{2n} \Rightarrow e = g^{2n-1}$, which cannot be since $|g|$ is infinite) and $\langle g^2 \rangle \subseteq G$. Hence $\langle g^2 \rangle$ is a non-trivial, proper subgroup of $G$, which contradicts our original constraints on $G$. Therefore, $G$ must be a finite group.

Suppose $|G|$ is not prime, then for some integers $p$ and $q$ (with $p, q \neq 1$), $|G| = pq$. Let $g$ be an arbitrary non-identity element in $G$. We know $g^{|G|} = e$, by Corollary 4 of Theorem 7.1. Then $g^{pq} = e$ and $(g^p)^q = e$. Hence, $|g^p| \leq q$. If $g^p \neq e$, then $|\langle g^p \rangle| \leq q < |G|$, hence $\langle g^p \rangle$ is a proper, non-trivial subgroup of $G$. If $g^p = e$, then $|\langle g \rangle| \leq p < |G|$, hence $\langle g \rangle$ is a proper, non-trivial subgroup of $G$. In either case, we have a contradiction, because $G$ has no proper, non-trivial subgroups. Hence, $|G|$ must be prime.

Solution 2: Let $G$ be a group with more than one element such that $G$ has no proper, nontrivial subgroups. Since $G$ has more than one element, there is an element $a \in G$ such that $a \neq e$. Consider the cyclic subgroup $H = \langle a \rangle$ of $G$ generated by $a$. Since $a \neq e$, $H \neq \langle e \rangle$ is nontrivial. Therefore, $H = G$, so $G$ must be a cyclic group.

If $|G|$ is infinite, then $G$ is isomorphic to $\mathbb{Z}$, the group of integers under addition (see Example 2 of Chapter 6 on page 123). As the group of integers under addition has proper, nontrivial subgroups (e.g., $2\mathbb{Z}$), so must $G$ by Theorem 6.3 Part 4. This, however, contradicts our assumption regarding the subgroups of $G$, or rather the lack thereof. Hence $G$ cannot be infinite.

Thus $G$ is a finite cyclic group generated by the element $a \neq e$. Suppose $|G| = n$. By the Fundamental Theorem of Cyclic Groups, for each divisor $k$ of $n$, there is exactly one subgroup $\langle a^{n/k} \rangle$ of $G$ of order $k$. If order for $G$ is not prime, then there is a divisor $k$ of $n$, $1 < k < n$, and hence there is a subgroup $K$ of $G$ of order $k$. However, since $k \neq 1$, $K$ is not the trivial subgroup. Also, since $k \neq n$, $K$ is not the improper subgroup, so $K$ is a proper, nontrivial subgroup of $G$. This contradicts our assumption concerning $G$, so we conclude that the order $n$ of $G$ must be prime.

Chapter 7. Problem 36. Let $G$ be a finite Abelian group and let $n$ be a positive integer that is relatively prime to $|G|$. Show that the mapping $a \mapsto a^n$ is an automorphism of $G$.

Solution: To show that this mapping, $\varphi : G \to G : a \mapsto a^n$, is an automorphism, we must verify that it is a bijection that preserves the group operation. To see that $\varphi$ is 1-1, let $a, b \in G$ with $\varphi(a) = \varphi(b)$. Then $a^n = b^n$. We can multiply both sides on the left by $(a^n)^{-1} = a^{-n} = (a^{-1})^n$ to get $e = (a^{-1})^n b^n$. Since $G$ is an Abelian group, we can rewrite this as $e = (a^{-1}b)^n$. Since $|a^{-1}b|$ must divide $|G|$ (by Corollary 2 of Theorem 7.1), $|a^{-1}b|$ must divide $n$ (by Corollary 2 of Theorem 4.1), and $gcd(|G|, n) = 1$, we may conclude that $|a^{-1}b| = 1$. That is, $a^{-1}b = e$, and by the uniqueness of inverses, $a = b$. Therefore, $\varphi$ is 1-1.

Now, recall that since $gcd(|G|, n) = 1$, we can find integers $s$ and $t$ such that $s \cdot |G| + t \cdot n = 1$ (Theorem 0.2). So, to see that $\varphi$ is onto, we let $g \in G$, and we will find an element $a$ of $G$
with \( \varphi(a) = g \). Consider \( g^1 \). We can re-write this as

\[
g = g^{s \cdot |G| + t \cdot n} = g^{s \cdot n} = (g^{|G|})^s (g^t)^n = e^s (g^t)^n = (g^t)^n.
\]

So for any element \( g \) of \( G \), \( g = \varphi(g^t) \), for the particular \( t \) we found above. Hence, \( \varphi \) is onto.

Finally, to see that \( \varphi \) preserves the operation, we will consider \( \varphi(ab) \), for \( a \) and \( b \) \( \in G \).

\( \varphi(ab) = (ab)^n \) which we can re-write as \( (ab)^n = a^n b^n \), since \( G \) is Abelian. So then, \( \varphi(ab) = a^n b^n = \varphi(a) \varphi(b) \). So \( \varphi \) preserves the operation. Hence, \( \varphi \) is an automorphism.