Chapter 6 #24. \( G = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \quad H = \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{Q} \right\} \).

Define \( \phi : G \to H \) by \( \phi(a + b\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \).

1. \( \phi \) is 1-1 and onto. (Why?)
2. \( \phi((a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})) = \phi(a_1 + b_1\sqrt{2}) + \phi(a_2 + b_2\sqrt{2}) \) (show!)

By 1 and 2 above \( G \) and \( H \) are isomorphic (when considered as groups under addition).

Closure under multiplication:
1. In \( G \): \((a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = a_1a_2 + 2b_1b_2 + (a_1b_2 + a_2b_1)\sqrt{2} \in G\).
2. In \( H \): \[a \quad 2b \quad x \quad 2y \quad a \quad b \quad x \quad y \] = \[
    \begin{bmatrix}
        ax + 2by \\
        bx + ay \\
        2(ay + bx) \\
        2by + ax
    \end{bmatrix} \in H.
\]

The map \( \phi \) preserves multiplication:
\( \phi((a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})) = \phi(a_1 + b_1\sqrt{2})\phi(a_2 + b_2\sqrt{2}) \) (show!)

Chapter 6 #27. Similar to Chapter 6 problem 24.

Chapter 6 #30. \( G \): finite Abelian group. Define \( f : G \to G \) by \( f(z) = a^2 \) for all \( a \in G \).

If \( f(a) = f(b) \) then \( a^2 = b^2 \). This implies \( a^2b^{-2} = 1 \). Since \( G \) is Abelian, \((ab)^{-1} = e\). If \( a \neq b \) then \(|ab^{-1}| = 2\) which contradicts with \( G \) not having any element of order 2. So \( a = b \). Hence \( f \) is 1-1. Because \( G \) is finite and \( f \) is 1-1, \( f \) is also onto. Also, \( f \) preserves the operation of the group because \( f(ab) = (ab)^2 = a^2b^2 \) since \( G \) is Abelian. So, \( f(ab) = f(a)f(b) \). Hence \( f \) is an automorphism of \( G \).

This result does not hold for infinite groups:

Example 1. Consider \( \mathbb{Q}^+ = \) set of positive rational numbers under multiplication. \( x^2 = 1 \) has only one solution in \( Q^+ \) so there is no element of order 2. However, the map \( f : Q^+ \to Q^+ \) defined by \( f(x) = x^2 \) is not an isomorphism because it it not onto: \( 3 \in Q^+ \) but there is no positive rational number whose square is 3.

Example 2. \( \mathbb{Z} \) under addition. \( x + x = 0 \) implies \( 2x = 0 \) and the only element that satisfies this equation is the identity \( 0 \). However, the map \( f : \mathbb{Z} \to \mathbb{Z} \) defined by \( f(x) = 2x \) is not an isomorphism because \( f \) is not onto: \( 5 \in \mathbb{Z} \) but there is no integer that when doubled gives 5.

Chapter 7 #10. \( G \) is a group and \( |G| = 155 = 5 \times 31 \). By Lagrange’s Theorem order of an
element in $G$ should divide 155, so possible orders for non-identity elements $a$ and $b$ are 5, 31, 155. If $a$ or $b$, say $a$ has order 155, then the group is cyclic and $G$ is the only subgroup that contains $a$. The only other possibility is, W.O.L.O.G., to have $|a| = 5$ and $|b| = 31$. If a subgroup $H$ contains both $a$ and $b$ then both 5 and 31 divide $|H|$. Because 5 and 31 are relatively prime, 155 divides $H$, hence $H = G$.

**Chapter 7 #12.** $\mathbb{C}^*$ is non-zero complex numbers is a group under multiplication. Let $H = \{a + bi|a^2 + b^2 = 1\}$.

Let $z = s + ti \in \mathbb{C}^*$. The norm of $z$ is denoted by $|z|$ and it is the distance of the point from the origin when it is represented on the coordinate plane with one of the axis the real part, and the other axis the imaginary part of $z$. Note that $|z| = \sqrt{s^2 + t^2}$.

Claim: The norm is multiplicative that is $|z_1z_2| = |z_1||z_2|$. (Show this! Hint: Use polar coordinates)

In this representation, the subgroup $H$ is the set of points on the unit circle. Note that the coset $zH$ is \( \{z(a + bi)|a^2 + b^2 = 1\} \) and the norm of an element in this set is $|z(a + bi)|$ which is equal to $|z||a + bi|$ using the multiplicative property. Since $|a + bi| = 1$ we get that the norm of an element in the coset $zH$ is $|z|$. Then $x + iy \in zH$ iff $\sqrt{(x^2 + y^2)} = |z|$ or $x^2 + y^2 = |z|^2$. So the cosets of $H$ in $\mathbb{C}^*$ are the circles with different radii.

**Chapter 7 #14.** Since $K$ is a proper subgroup of $H$, $|K| \neq |H|$ and $|K|$ divides $|H|$. Similarly, $|H| \neq |G|$ and $|H|$ divides $|G|$. So 42 divides $|H|$, $|H|$ divides 420, and $|H| \neq 42, 420$. Therefore, $|H| = 84$ or 210.

**Chapter 7 #20.** Suppose $H$ and $K$ are subgroups of a group $G$ with orders 12 and 35 respectively. $H \cap K$ is a subgroup of both $H$ and $K$ (proved earlier). By Lagrange’s Theorem $|H \cap K|$ divides both 12 and 35. But because 12 and 35 are relatively prime $|H \cap K| = 1$.

**Chapter 7 #21.** Let $G$ be Abelian group with $2n + 1$ elements, that is $G = \{e, a_1, a_2, \ldots, a_{2n}\}$. Since $|G|$ is odd, by Lagrange’s Theorem, there is no element of order 2 in $G$. Then for each $a_i \in G$, $a_i^{-1} = a_j$ for some $j \in \{1, \ldots, 2n\}$. W.O.L.O.G. let $a_i^{-1} = a_{i+n}$ for $i = 1, 2, \ldots, n$. Because $G$ is Abelian, $ea_1a_2 \ldots a_n a_{n+1} \ldots a_2n = ea_1 a_{n+1}a_2 a_{n+2} \ldots a_n a_{2n}$ and by our discussion above, this is equal to $ee \ldots e = e$.

**Chapter 7 #26.** Let $G$ be a group with 8 elements. Show that $G$ has an element of order 2. Similar to Chapter 7 problem 34.

**Chapter 7 #33.** Let $G$ be a group of order $p^n$ where $p$ is prime. Suppose the center $Z(G)$ has order $p^{n-1}$. Then there exists $a \in G$ that is not in $Z(G)$. The centralizer of $a$, denoted by $C(a)$,
contains $Z(G)$ and it is strictly larger than $Z(G)$. This is because $a$ is in $C(a)$ but not in $Z(G)$. We proved in class that $C(a)$ is a subgroup of $G$. Since $|C(a)| < |Z(G)|$, we have to have $C(a) = G$ which implies $C(a) = G$. This means $a$ commutes with every element in $G$, that is $a \in Z(G)$ which is contradicts with our assumption that $a \notin Z(G)$. Therefore $|Z(G)| \neq p^{n-1}$.

Chapter 7 #34. Let $G$ be a group with $|G|=12$. Possible orders of non-identity elements in $G$, by Lagrange’s Theorem are, 2,3,4,6, and 12.

Let $a \in G$. If $a$ has an element of order 2 we are done.

If $a$ has order 4 then, $a^2$ has order 2. (Think about why?)

If $a$ has order 8, then $a^4$ has order 2.

If $a$ has order 12, then $a^6$ has order 2.

Next, we will prove that not all elements can have order 3 in $G$. For sake of contradiction suppose that all elements in $G$ have order 3. Then $G = \{e, a_1, a_1^2, a_2, a_2^2 \ldots a_5, a_5^2, b\}$. Notice that there isn’t enough room for all elements to have order 3.

So $G$ contains an element of order 4,8, or 12, hence an element of order 2.

Chapter 7 #36. Let $G$ be a finite Abelian group, and $n \in \mathbb{Z}^+$ that is relatively prime to $|G|$. Let $f : G \rightarrow G$ be defined by $f(a) = a^n$ for all $a \in G$.

Suppose $f(a) = f(b)$. This means $a^n = b^n$ which implies $(ab^{-1})^n = e$ because $G$ is Abelian. Because $n$ and $|G|$ are relatively prime, $ab^{-1} = e$, that is $a = b$. This says that $f$ is 1-1.

Because $G$ is finite, and $f$ is a 1-1 map from $G$ to itself, $f$ is also onto.

Also, $f(ab) = (ab)^n = a^n b^n$ because $G$ is Abelian. So, $f(ab) = f(a)f(b)$, hence $f$ is an automorphism of $G$.

Chapter 7 #38. Let $G$ be a group of order $pq r$ where $p, q, r$ are distinct primes. Let $H$ and $K$ are subgroups of $G$ with orders $pq$ and $qr$ respectively. $H \cap K$ is a subgroup of both $H$ and $K$ (proved earlier). So $|H \cap K|$ divides both $pq$ and $qr$. So $|H \cap K| = 1$ or $q$.

We will prove that it can’t be 1.

For sake of contradiction suppose $H \cap K = \{e\}$.

Then $H = \{e, a_2, \ldots, a_{pq}\}$ and $H = \{e, b_2, \ldots, b_{qr}\}$ where $a_i \neq b_j$ for $i = 2, \ldots, pq$ and $j = 2, \ldots, b_{qr}$.

Let $a_i, a_j \in H$ and $b_k, b_l \in K$, all distinct, non-identity elements. Then $a_i b_k = a_j b_l$ only if $a_i = a_j^{-1}$ and $b_l = b_k^{-1}$ because, if they were equal, then we would have $a_i a_j^{-1} = b_l b_k^{-1}$ and hence $a_i a_j^{-1}$ and $b_l b_k^{-1}$ in $H \cap K = \{e\}$. But $a_i a_j^{-1} = e$ implies $a_i = a_j$ which contradicts with our assumption that $a_i$’s are distinct.

Now consider the set $\{a_i b_k | a_i \in H, b_k \in K\}$. The number of distinct elements in this set is greater then $|G| = pq r$ (Why?). This is a contradiction. Therefore $|H \cap K| = q$.

Chapter 7 #43. $G = GL(2, \mathbb{R})$, $H = \{\text{matrices with determinant 1 or -1}\}$ subgroup of $G$. Let
$a, b \in G$.

If $aH = bH$ then $ah_1 = bh_2$ for some $h_1, h_2 \in H$.

Then $det(ah_1) = det(ah_2)$. Since determinant is multiplicative, we get $det(a)det(h_1) = det(b)det(h_2)$. This implies $det(a) = \pm det(b)$ because $det(h_1)$ and $det(h_2)$ are $\pm 1$.

For the converse, if $det(a) = \pm det(b)$ then $det(ab^{-1}) = \pm 1$. So $ab^{-1}$ is in $H$. This implies $aH = bH$. 