(1) Show any group of order 4 is abelian.

Hint: We know cyclic groups are abelian.

Proof: Assume \( G \) is a group of order 4. Since cyclic groups are abelian, we assume \( G \) is not cyclic. That means \( G \) consists of the identity element \( e \) and three order two elements. Let \( a, b \in G \). Then each of \( a, b \) and \( ab \) has order 1 or 2. So \( a^2 = b^2 = (ab)^2 = e \) implying \( (ab)^2 = a^2b^2 \), which, as shown on a previous homework, is enough to conclude that \( G \) is abelian. □

(2) Let \( G, H \) be groups. Prove that if \( \phi : G \to H \) is a homomorphism then the image of \( G \) under \( \phi \), that is \( \phi(G) = \{ \phi(x) | x \in G \} \), is a subgroup of \( H \).

Proof: Let \( \phi : G \to H \) be a homomorphism. Clearly \( \phi(G) \) is non-empty. Let \( a, b \in \phi(G) \). Then \( a = \phi(g) \) and \( b = \phi(k) \) for some \( g, k \in G \). Consider that \( \phi(gk^{-1}) = \phi(g)\phi(k)^{-1} = ab^{-1} \). Thus \( ab^{-1} \in \phi(G) \), showing that \( \phi(G) \) a subgroup of \( H \). □

(3) Suppose \( G \) is a group with normal subgroups \( M, N \) such that \( M \cap N = \{ e \} \) where \( e \) is the identity of \( G \). Show that for any \( m \in M \) and for any \( n \in N \), \( mn = nm \).

Proof: Let \( m \in M \) and \( n \in N \). Consider the element \( x = mnm^{-1}n^{-1} \). Since \( M \) is a normal subgroup of \( G \) it follows that \( x = m(nm^{-1}n^{-1}) \) is in \( M \). Since \( N \) is a normal subgroup of \( G \) it follows that \( x = (mnm^{-1})n^{-1} \) is in \( N \). Hence \( x \in M \cap N \). So \( x = e \). Then by right multiplication by \( nm \) we get \( nm = mn \). □

(4) Let \( G \) be a group and \( Z(G) = \{ z \in G | zg = gz \ \forall g \in G \} \) (called the center of \( G \)). Show that \( Z(G) \leq G \) and if \( G/Z(G) \) is a cyclic group then \( G \) is abelian.

Proof: Clearly \( e \in Z(G) \) as \( eg = ge = g \) for all \( g \in G \). Let \( a, b \in Z(G) \) and \( g \in G \). Since \( bg^{-1} = g^{-1}b \) it follows \( gb^{-1} = b^{-1}g \) that by taking the inverse of both sides. Then \( ab^{-1}g = agb^{-1} = gab^{-1} \). Hence \( ab^{-1} \in Z(G) \). That shows \( Z(G) \leq G \). Consider \( gag^{-1} = agg^{-1} = a \in Z(G) \). Hence \( Z(G) \leq G \).

Suppose \( G/Z(G) \) is cyclic and generated by \( xZ(G) \). Let \( g, h \in G \). Then there exists integers \( i, j \) such that \( gZ(G) = x^iZ(G) \) and \( hZ(G) = x^jZ(G) \). Then \( g = x^iy \) and \( h = x^jy \) for some \( y, z \in Z(G) \). Then

\[
gh = x^iyx^jz = zx^ix^jy = zx^jx^iy = x^jzx^iy = hg,
\]

which proves that \( G \) is abelian. □
5) Consider the additive quotient group $G = \mathbb{Q}/\mathbb{Z}$.

(a) Show every element of $G$ can be represented by $r + \mathbb{Z}$ where $r \in \mathbb{Q}$ and $0 \leq r < 1$.

Let $q \in \mathbb{Q}$. The coset $q + \mathbb{Z}$ is equal to $r + \mathbb{Z}$ for $r = q - n$ where $n$ is the greatest integer less than or equal to $q$ (called the floor of $q$) since $q - r$ is an integer. Hence every element of $G$ can be represented by $r + \mathbb{Z}$ where $r \in \mathbb{Q}$ and $0 \leq r < 1$.

(b) Show that every element of $G$ has finite order, but there is no upper bound on the orders of all the elements.

Let $r + \mathbb{Z} \in G$. Then $r = p/q$ for some integers $p, q$ such that $q \neq 0$. Then $q(r + \mathbb{Z}) = \mathbb{Z}$ implies the order of $r + \mathbb{Z}$ is finite (a divisor of $q$). To yield a contradiction, suppose there exists a real number $B > 0$ such that the order of $q + \mathbb{Z}$ is less than $B$ for any $q \in \mathbb{Q}$. Let $n$ be an integer such that $n > B$. Then $1/n < 1/B$ implies that the order is more than $B$, which is a contradiction. So there is no upper bound on the orders of the cosets.

6) Let $G, G'$ be groups with normal subgroups $H, H'$ respectively. Show that if $\phi : G \to G'$ is a homomorphism and $\phi(H) \subseteq H'$ then $\phi_* : G/H \to G'/H'$ given by $\phi_*(gH) = \phi(g)H'$ is a homomorphism.

Proof: Let $\phi : G \to G'$ be a homomorphism and assume $\phi(H) \subseteq H'$. Define $\phi_* : G/H \to G'/H'$ by $\phi_*(gH) = \phi(g)H'$. First let’s show $\phi_*$ is well-defined. Let’s make sure the definition does not depend on the choice of coset representative. Suppose $a, b \in G$ and $aH = bH$. Then $a^{-1}b \in H$ and

$$\phi_*(aH) = \phi(a)H' = \phi(a)\phi(a^{-1}b)H' = \phi(aa^{-1}b)H' = \phi(b)H' = \phi_*(bH)$$

since $\phi(a^{-1}b) \in H'$ as $\phi(H) \subseteq H'$. So $\phi_*$ is well-defined.

Now let $gH, kH \in G/H$. Consider that

$$\phi_*(gHkH) = \phi_*(gkH) = \phi(gk)H' = \phi(g)\phi(k)H' = \phi(g)H' \phi(k)H' = \phi(gH)\phi(kH).$$

Thus $\phi_*$ is a homomorphism.

7) We know that $\mathbb{C}^*$, $\mathbb{R}^+$ and $U = \{z \in \mathbb{C} : |z| = 1\}$ are groups under multiplication. Prove that $\mathbb{C}^*/U \cong \mathbb{R}^+$.

Hint: Use the First Isomorphism Theorem!

Proof: Let $\phi : \mathbb{C}^* \to \mathbb{R}^+$ be given by $\phi(z) = |z|$ (where for $z = a + bi$ with $a, b \in \mathbb{R}$, $|z| = \sqrt{a^2 + b^2}$). Let $z_1, z_2 \in \mathbb{C}^*$ so $z_1 = a + bi$ and $z_2 = c + di$ for some $a, b, c, d \in \mathbb{R}$ where $i = \sqrt{-1}$. $|z_1z_2|^2 = |z_1|^2|z_2|^2 = (a^2 + b^2)(c^2 + d^2) = a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 = a^2(c^2 + d^2) + b^2(c^2 + d^2) = (a^2 + b^2)(c^2 + d^2) = |z_1|^2|z_2|^2$. So $|z_1z_2| = |z_1||z_2|$. Hence $\phi$ is a homomorphism. Let $r \in \mathbb{R}^+$. Then $r \in \mathbb{C}^*$ and $\phi(r) = r$. So $\phi$ is onto. The kernel is $\ker(\phi) = \{z \in \mathbb{C}^* : \phi(z) = 1\} = \{z \in \mathbb{C}^* : |z| = 1\} = U$. Therefore, by the First Isomorphism Theorem, $\mathbb{C}^*/U \cong \mathbb{R}^+$. □
Let $G$ be a group and $H \leq G$. The normalizer of $H$ in $G$ is $N(H) = \{ g \in G | ghg^{-1} = H \}$.

Prove the following:

(a) $N(H) \leq G$.

Proof: Clearly $N(H) \subseteq G$ and $e \in N(H)$ as $eHe^{-1} = eHe = H$. Let $a, b \in N(H)$. Then $aHa^{-1} = H$ and $bHb^{-1} = H$, which also implies $b^{-1}Hb = H$. Let’s show that $ab^{-1} \in N(H)$:

$$(ab^{-1})H(ab^{-1})^{-1} = ab^{-1}Hba^{-1} = aHa^{-1} = H.$$ 

So $ab^{-1} \in N(H)$. Thus $N(H)$ is a subgroup of $G$. □

(b) $H$ is a normal subgroup of $N(H)$.

Hint: First show that $H \subseteq N(H)$.

Proof: Let $x \in H$. Then for all $h \in H$ we have that $xhx^{-1} \in H$ as $H$ is a subgroup. So $xHx^{-1} \subseteq H$. We also have that for all $h \in H$, $h = x(x^{-1}hx)x^{-1}$ is in $xHx^{-1}$ since $x^{-1}hx \in H$ as $H$ is a subgroup. Thus $H \subseteq xHx^{-1}$. So $xHx^{-1} = H$. Hence $x \in N(H)$. Thus $H \subseteq N(H)$ implying $H \leq N(H)$. By definition, $nHn^{-1} = H$ for all $n \in N(H)$, so $H \leq N(H)$. □

(c) If $H$ is a normal subgroup of $K \leq G$ then $K \leq N(H)$. Conclude that $N(H)$ is the largest subgroup of $G$ in which $H$ is normal.

Proof: Assume $H \leq K$ and $K \leq G$. Let $k \in K$. Then $kHk^{-1} = H$ since $H$ is normal in $K$. Thus $k \in N(H)$. Hence $K \subseteq N(H)$. Therefore $N(H)$ is the largest subgroup of $G$ in which $H$ is normal. □

(d) $H$ is a normal subgroup of $G$ iff $G = N(H)$.

Proof: Assume $H \leq G$. Applying part (c) we get $G \leq N(H)$ and hence $N(H) = G$. Now assume $G = N(H)$. Just apply part (b) to get $N \leq G$. □
One presentation of the Dihedral Group of order 8 (symmetries of a square) is $D_8 = \{ \text{Id}, \sigma, \sigma^2, \sigma^3, \tau, \tau \sigma, \tau \sigma^2, \tau \sigma^3 \}$ with the relations $\sigma^4 = \text{Id}$, $\tau^2 = \text{Id}$ and $\sigma \tau = \tau \sigma^3$.

(9) Consider the subgroup $H = \langle \tau \rangle$ of $D_8$. Determine $N(H)$, the normalizer of $H$ in $D_8$.

We already know that $H$ is in $N(H)$. Let’s consider element not in $H$. $\sigma \tau \sigma^{-1} = \sigma \tau \sigma^3 = \tau \sigma^3 = \tau \sigma^2$ so $\sigma \not\in N(H)$. A similar analysis shows that $\sigma^3$ is not in $N(H)$. $\sigma^2 \tau (\sigma^2)^{-1} = \sigma \tau \sigma^2 = \sigma \tau \sigma = \tau$ implies $\sigma^2 \in N(H)$. Then $\tau \sigma^2 \in N(H)$ as $N(H)$ is a subgroup. At that point we know $N(H)$ is a group of order 4 and have the 4 elements. That is enough to conclude that $N(H) = \{ \text{Id}, \sigma^2, \tau, \tau \sigma^2 \}$.

(10) Let $G$ be a group and $a, b \in G$ and assume $b$ is NOT the identity element.

(a) Show that if $aba^{-1} = b^i$ for some $i \in \mathbb{N}$ then $a^r ba^{-r} = b^{ir}$ for all $r \in \mathbb{N}$.

Hint: Use induction!

Proof: Assume $aba^{-1} = b^i$ for some $i \in \mathbb{N}$. We shall use induction on $r$. Clearly $a^r ba^{-r} = b^{ir}$ holds for $r = 1$. Suppose $r \in \mathbb{N}$ and $a^r ba^{-r} = b^{ir}$. Then

$$a^{r+1}ba^{-(r+1)} = a(a^r ba^{-r})a^{-1} = a(b^{ir})a^{-1} = (aba^{-1})(aba^{-1}) \cdots (aba^{-1}) = b^{ir} \cdots b^{i},$$

where there are $i^r$ factors. Thus $a^{r+1}ba^{-(r+1)} = (b^i)^{ir} = b^{ir+1}$, completing the proof by induction □

(b) If the order of $a$ is 5 and $aba^{-1} = b^2$ then determine the order of $b$.

Since the order of $a$ is 5, $a^5 = a^{-5} = e$ where $e$ is the identity of $G$. So by the previous part of this exercise, we have that $b = a^5ba^{-5} = b^{25} = b^{32}$. By cancelation we get $b^{31} = e$. So the order of $b$ is a divisor of 31, which are 1 and 31. Since $b \neq e$, the order of $b$ is equal to 31.