1.) A *simple* group is one whose only normal subgroups are the trivial group and the whole group. Let \( G \) be a simple group and suppose \( \varphi : G \to H \) is a group homomorphism. Prove that \( \varphi \) is either the trivial homomorphism or injective.

Let \( \varphi : G \to H \) be a homomorphism. Then \( \ker \varphi \triangleleft G \). Since \( G \) is assumed to be simple, we know \( \ker \varphi \) is trivial or the whole group. In the first case, \( \varphi \) is injective. In the second case, \( \varphi \) is the trivial map.

2.) Prove that \( S_4 \) has no normal subgroup of order 3.

Suppose \( H \leq S_4 \) has order 3. Because 3 is a prime number, \( H \) is cyclic. Therefore \( H \) is generated by some three cycle \( \sigma \). For example, we might have \( H = \langle (123) \rangle \). Let \( \sigma = (abc) \). Then \( H = \{(), (abc), (acb)\} \). Let \( d \) be the remaining number in \( \{1, 2, 3, 4\} \) after \( a, b, c \) are taken away. Let \( \tau = (ad) \), a transposition. Note that \( \tau \) is self-inverse. Conjugating \( \sigma \) by \( \tau \), we have

\[
\tau^{-1}\sigma\tau = (ad)(abc)(ad) = (a)(bcd) = (bcd).
\]

Therefore \( \tau^{-1}\sigma\tau \notin H \), and so \( H \) is not normal in \( S_4 \).

3.) Let \( \text{GL}_n(\mathbb{R}) \) denote the (multiplicative) group of invertible \( n \times n \) matrices with real entries. Let \( \text{SL}_n(\mathbb{R}) \) be the subset of matrices with determinant 1. Show that \( \text{SL}_n(\mathbb{R}) \) is a normal subgroup of \( \text{GL}_n(\mathbb{R}) \) and identify the quotient group \( \text{GL}_n(\mathbb{R})/\text{SL}_n(\mathbb{R}) \) with something we’ve previously studied.

Consider the map \( \det : \text{GL}_n(\mathbb{R}) \to \mathbb{R}^\times \). Note that \( \det \) is a group homomorphism because \( \det(AB) = \det(A)\det(B) \). Moreover, \( \det \) is onto. To see this, suppose \( a \) is a nonzero real number. Let \( A \) be the matrix with the entry \( a \) in the upper left-hand corner, 1’s down the rest of the diagonal, and 0’s everywhere else. Then \( \det(A) = a \), which shows \( \det \) is onto. Moreover, we have \( \ker \det = \text{SL}_n(\mathbb{R}) \). By the isomorphism theorem, we have

\[
\text{GL}_n(\mathbb{R})/\text{SL}_n(\mathbb{R}) \cong \mathbb{R}^\times.
\]

4.) Let \( Q \) denote the quaternion group of order 8. Let \( N = Z(Q) \) be its center, a normal subgroup of \( Q \).

(a) Find \( N \) and its index \([Q : N] \).
By definition, 1 and \(-1\) commute with everything, so \(\{\pm 1\} \subset N\). On the other hand, \(ij = k \neq -k = ji\), so neither \(i\) nor \(j\) is contained in \(N\). In the same vein, no other element is contained in \(N\). So \(N = \{\pm 1\}\). By Lagrange, \([Q : N] = |Q|/|N| = 8/2 = 4\).

(b) **Find coset representatives for the left coset space \(Q/N\).**

We have

\[
1N = \{\pm 1\} \quad iN = \{\pm i\} \quad jN = \{\pm j\} \quad kN = \{\pm k\}.
\]

Since these four cosets are disjoint and \([Q : N] = 4\), these must be all the left cosets of \(N\). Therefore \(1, i, j, k\) are coset representatives.

(c) **What is the order of the quotient group \(Q/N\)? You know that up to isomorphism, there are exactly two groups of this order. Which of the two isomorphism classes contains \(Q/N\)?**

The quotient group \(Q/N\) has order 4, as we already discovered in part (a). We see that

\[
(iN)^2 = i^2N = -1N = N,
\]

and so the coset \(iN\) has order 2 in \(Q/N\). Similarly, the cosets \(jN\) and \(kN\) also have order 2. If a group of order 4 has three elements of order 2, then the group is isomorphic to the mattress group (aka the Klein 4 group). Therefore \(Q/N \cong \mathbb{Z}_2 \times \mathbb{Z}_2\).

5.) Let \(G\) be a finite group. From a previous problem set, we have an equivalence relation \(\sim\) on \(G\), where \(x \sim y\) if there exists \(g \in G\) with \(x = g^{-1}yg\). The equivalence classes \([x] = \{y \in G : x \sim y\}\) are called the **conjugacy classes of \(G\).**

(a) **Suppose \(x \sim y\). Show that \(|x| = |y|\).**

If \(x \sim y\), then there is some \(g \in G\) with \(x = g^{-1}yg\). Suppose \(|y| = n\). Then

\[
x^n = (g^{-1}yg)^n = (g^{-1}yg)(g^{-1}yg) \cdots (g^{-1}yg) = g^{-1}y^n g = g^{-1}eg = e,
\]

\(n\) times

which shows that the order of \(x\) divides \(n\). But \(\sim\) is symmetric, so \(y \sim x\). The same argument then shows \(|y|\) divides \(|x|\). Therefore \(|x| = |y|\).

(b) **Suppose \([x]\) contains exactly one element. Show that \(x \in Z(G)\).**

If \([x]\) contains exactly one elements, then \([x] = \{x\}\). Let \(g \in G\). Because \(g^{-1}xg \sim x\), we have \(g^{-1}xg \in [x]\). Thus \(g^{-1}xg = x\), and so \(xg = gx\). This shows that \(x\) commutes with \(g\). Because \(g\) was arbitrary, \(x\) commutes with every \(g \in G\). Hence \(x \in Z(G)\).

(c) **Find the conjugacy classes of \(S_3\).**

For any group \(G\), the identity makes up its own conjugacy class.

We have \((12)^{-1}(123)(12) = (12)(123)(12) = (132)\). Therefore \((123) \sim (132)\). By part (a), the class \([123]\) only contains elements of order 3. Since \(S_3\) has exactly two elements of order 3, we have found the whole conjugacy class.
Also, $(13)^{-1}(12)(13) = (13)(12)(13) = (23)$, so $(12) \sim (23)$. Similarly, $(12)^{-1}(23)(12) = (12)(23)(12) = (13)$, so $(23) \sim (13)$. Using the same reasoning as before, we have found the whole conjugacy class.

To summarize, the conjugacy classes of $S_3$ are

\[
\begin{align*}
\{()\} & = \{()\} \quad \{12\} = \{(12), (13), (23)\} \\
\{12\} & = \{(12), (13), (23)\} \quad \{13\} = \{(13), (12)\}
\end{align*}
\]

9.) Let $G$ be a group. If $N \triangleleft G$ and $M \triangleleft G$, you’ve already proved that $N \cap M \leq G$. Show that $N \cap M \triangleleft G$.

Consider the map $\pi : G \rightarrow G/N \times G/M$ where $\pi(g) = (gN, gM)$. Because

\[
\pi(ab) = (abN, abM) = ((aN)(bN), (aM)(bM)) = (aN, aM)(bN, bM) = \pi(a)\pi(b),
\]

it follows that $\pi$ is a homomorphism. We have $x \in \ker \pi$ if and only if $(xN, xM) = (N, M)$. This is equivalent to $x \in N$ and $x \in M$, in other words, $x \in N \cap M$. This shows $\ker \pi = N \cap M$. Because kernels of homomorphisms are normal subgroups, $N \cap M \triangleleft G$.

10.) Let $G$ be a group, $N \triangleleft G$, and $H \leq G$. Suppose $\gcd([G : N], |H|) = 1$. Prove that $H \leq N$.

There are several variations on the same proof idea. Here is one version of the proof. Because $N \triangleleft G$, we have the quotient homomorphism $\pi : G \rightarrow G/N$. To show that $H \subset N$, we must show that $h \in N$ for every $h \in H$. Formulating this in terms of $\pi$, we must show $\pi(h) = N$ for every $h \in H$.

Because $\gcd([G : N], |H|) = 1$, there exist integers $a, b$ with $a[G : N] + b|H| = 1$. After proving Lagrange’s theorem, we showed that any group element raised to (a multiple of) the order of the group equals the identity. Applying this theorem to the quotient group $G/N$, if $g$ is any element of $G$, then $\pi(g)^{[G : N]} = (gN)^{[G : N]} = N$. Applying this theorem to the group $H$, if $h$ is any element of $H$, we have $h^{[H]} = e$. Applying all of these ideas in unison, if $h \in H$, we have

\[
\pi(h) = \pi(h)^1 = \pi(h)^{a[G : N]+b[H]} = \pi(h)^a\pi^{[G : N]}(h^b)=N\pi(e) = (N)(N) = N,
\]

which is what we wanted to show.