1. Let $a$ and $b$ be distinct elements in a group $G$. Show that there is an automorphism of $G$ that carries $ab$ to $ba$. Why does this prove that $|ab| = |ba|$?

**Solution:** Consider the inner automorphism $\chi : G \to G$ given by $\chi(g) = a^{-1}xa$. Then we have $\chi(ab) = a^{-1}(ab)a = (a^{-1}a)(ba) = ba$. Since for all isomorphisms $\phi : G \to H$ we always have $|\phi(g)| = |g|$, for the inner automorphism $\chi$ above we must have $|ba| = |\chi(ab)| = |ab|$. 

2. Suppose that $K$ is a subgroup of $H$ and $H$ is a subgroup of $G$. If there are six left cosets of $K$ in $H$ and four left cosets of $H$ in $G$, how many left cosets of $K$ are there in $G$?

**Solution:** The number of cosets of $K$ in $G$ is equal to the index of $K$ in $G$, namely

$$|G : K| = |G|/|K| = (|G|/|H|)(|H|/|K|) = |G : H| \cdot |H : K| = 4 \cdot 6 = 24.$$ 

3. If $H$ and $K$ are subgroups of $G$ and $g \in G$, prove that $gH \cap gK = g(H \cap K)$.

**Proof.** Let $H$ and $K$ be subgroups of $G$ and let $g$ be an element of $G$. Then $H \cap K = \{x \in G : x \in H$ and $x \in K\}$, so $gH \cap gK = \{gx \in G : x \in H$ and $x \in K\} = \{y \in G : y \in gH$ and $y \in gK\}$ (where $y = gx$ from before, so $x \in H$ implies $y = gx \in gH$ by multiplying throughout by $g$ on the left). Hence $g(H \cap K) = \{y \in G : y \in gH$ and $y \in gK\} = gH \cap gK$. 

4. Prove that the only subgroup of $D_5$ that contains two reflections is $D_5$ itself.

**Proof.** Suppose $H \leq D_5$ contains distinct reflections $\rho_1$ and $\rho_2$. Then, by closure, the product $\rho_1\rho_2 \in H$, but we know that the product of two reflections in a dihedral group is a rotation. We claim that this rotation is non-trivial, i.e., that $\rho_1\rho_2 \neq R_0$. For, if $\rho_1\rho_2 = R_0$, then $\rho_1 = \rho_2^{-1}$, since $R_0$ is the identity element in $D_5$. However, $\rho_2^{-1} = \rho_2$, since every reflection is its own inverse, so $\rho_1 = \rho_2$, which contradicts our assumption that $\rho_1$ and $\rho_2$ are distinct. Therefore $\rho_1\rho_2$ is a nontrivial rotation in $D_5$, so it is of the form $R_{360k/5} = R_{72k}$ for some $k$ with $1 \leq k \leq 4$, so this $R_{72k} \in H$.

We recall that the set of reflections in $D_5$ is a cyclic subgroup of $D_5$ of order 5, and a cyclic group $(a)$ is generated by any element $a^m$ so long as $m$ is relatively prime to the order of $a$, i.e., gcd$(|a|, m) = 1$. Therefore, the element $R_{72k} \in H$ we found above is a generator for the subgroup of rotations of $D_5$, so all 5 rotations in $D_5$ belong to $H$ and there are also the two reflections $\rho_1$ and $\rho_2$. Hence $|H| \geq 7$, but $|H|$ divides $|D_5| = 10$ by Lagrange’s Theorem. Therefore, $|H| = 10 = |D_5|$, as 10 is the only divisor of 10 that is greater than or equal to 7, so $H = D_5$. 

5. Suppose that $H$ is a subgroup of a group $G$ and that $|G| = 60$ and $|H| = 10$. Prove that for every $a \in G$, there is an integer $k$ with $1 \leq k \leq 6$ so that $a^k \in H$.

**Proof.** Suppose $H \leq G$ where $|H| = 10$ and $|G| = 60$. Thus, by Lagrange’s Theorem, there are $|G : H| = |G|/|H| = 60/10 = 6$ left cosets of $H$ in $G$. Now let $a \in G$ and consider the cosets $aH, a^2H, a^3H, a^4H, a^5H, a^6H, a^7H$. This is a listing of seven left cosets of $H$, but there are exactly 6 distinct left cosets of $H$ in $G$. Therefore, at least two of the cosets we have listed must be the same. Let’s call them $a^iH$ and $a^jH$, where we assume that $i < j$. Thus $a^iH = a^jH$, so $H = a^{-i}a^jH = a^{-i}H$, which implies that $a^{j-i} \in H$. Yet $1 \leq i < j \leq 7$, so $1 \leq j - i \leq 7 - 1 = 6$, so for $k = j - i$, which satisfies $1 \leq k \leq 6$, we have $a^k \in H$. 


6. Suppose that $H$ is a proper subgroup of $S_4$ and that $H$ contains $(12)(34)$ and $(234)$. Prove that $H = A_4$.

**Proof.** Let $H$ be a proper subgroup of $S_4$, which means that $H \neq S_4$, and assume that $(12)(34), (234) \in H$. We claim that $H = A_4$ is the alternating group of degree 4, which has order $|A_4| = 4!/2 = 24/2 = 12$. Now $H$ contains the element $(12)(34)$, so $H$ contains the cyclic subgroup $\langle (12)(34) \rangle$, whose order is 2. Similarly, $H$ contains the cyclic subgroup generated by $(234) \in H$, and we know $|\langle (234) \rangle| = |(234)| = 3$. Hence $H$ contains a subgroup of order 2 and a subgroup of order 3. By Lagrange’s Theorem, the order $|H|$ of $H$ must then be divisible by both 2 and by 3, and hence by $6 = \text{lcm}(2,3)$. That is, 6 divides $|H|$ and $|H|$ divides $|S_4| = 4! = 24$, so $|H|$ is either 6 or 12 or 24. However, $H$ is a proper subgroup of $S_4$, so $|H| < 24$. That means $|H|$ is either 6 or 12.

Now $(12)(34)$ and $(234)$ are both even permutations, so both belong to $A_4$ and the subgroup $E$ generated by them must also be a subgroup of $A_4$ and $|E| \geq 6$ by the argument above. Yet $A_4$ contains no subgroups of order 6, so $E \leq A_4$ and $6 \leq |E|$ imply that $E = A_4$. Therefore, as $H$ contains $E = A_4$, we have $A_4 \leq H \leq S_4$. Now $|S_4 : A_4| = 2$, so there are no proper subgroups of $S_4$ strictly between $A_4$ and $S_4$, so $H = A_4$ since it must be a proper subgroup of $S_4$. \[\square\]

7. What is the order of the element $6 + \langle 8 \rangle$ in the factor group $\mathbb{Z}_{48}/\langle 8 \rangle$?

**Solution:** The order of $6 + \langle 8 \rangle \in \mathbb{Z}_{48}/\langle 8 \rangle$ is the least positive integer $k$ such that $k(6 + \langle 8 \rangle) = 6k + \langle 8 \rangle$ is equal to the identity element, 0 + $\langle 8 \rangle$ = $\langle 8 \rangle$ in the factor group. Thus, the order is the least positive integer $k$ such that $6k \in \langle 8 \rangle = \{0, 8, 16, 24, 32, 40\}$, from which we can see that $k = 4$ is the order. Hence $|6 + \langle 8 \rangle| = 4$.

8. Let $G = GL(2, \mathbb{R})$ and let $H = \{A \in GL(2, \mathbb{R}) : \det(A) \text{ is rational} \}$. Prove that $H$ is a normal subgroup of $G$.

**Proof.** We will use the Normal Subgroup Test, so let $x \in G$ and $A \in H$ and consider $xAx^{-1}$. In particular, $\det(xAx^{-1}) = \det(x) \det(A) \det(x^{-1}) = \det(x) \det(x^{-1}) \det(A) = \det(xx^{-1}) \det(A) = \det(I_2) \det(A) = \det(A)$, which is rational since $A \in H$. Therefore $xAx^{-1} \in H$ as well, so $xHx^{-1} \subseteq H$ since the element $A \in H$ was arbitrary. So, by the Normal Subgroup Test, $H$ is normal in $G$. \[\square\]

9. Let $H = \{\beta \in S_4 : \beta(4) = 4\}$. Is the subgroup $H$ normal in $G$? Justify your answer.

**Solution:** The subgroup $H$ is not normal in $G = S_4$.

**Proof.** Let $\sigma = (34) \in S_4$ and let $\beta = (123) \in S_4$. Then $\beta(4) = 4$, so $\beta \in H$. Consider the permutation $\sigma \beta \sigma = (34)(123)(34) = (124)(3) = (124)$. Therefore $(\sigma \beta \sigma)(4) = 1 \neq 4$, so $\sigma \beta \sigma \notin H$, so $\sigma H \sigma^{-1} \not\subseteq H$, so $H$ is not normal in $G = S_4$. \[\square\]

10. Suppose that $H$ is a normal subgroup of $G$ with $|G : H| = 24$ and $|H| = 11$. If $x \in G$ and $x^{11} = e$, prove that $x \in H$.

**Proof.** Since $H$ is normal in $G$ and $x^{11} = e$, we have $x^{11} \in H$. Therefore, $x = x^{11}x^{-1} \in H$ since $H$ is normal in $G$. \[\square\]
Proof. Let $H \leq G$ be a normal subgroup of $G$ such that $|G : H| = 24$ and $|H| = 11$. Let $x \in G$ be an element such that $x^{11} = e$. As $H$ is normal in $G$, $G/H$ is a factor group of order $|G : H| = 24$. Consider the coset $xH \in G/H$. Since $|G/H| = 24$, $(xH)_{G/H} = (xH)^{24} = (x^{24})H$ must be the identity element by Corollary 4 to Lagrange’s Theorem. Hence $x^{24} \in H$, as $x^{24}H = eH$. Yet $x^{24} = x^{22} \cdot x^2 = (x^{11})^2 \cdot x^2 = e^2 \cdot x^2 = x^2$, so $x^2 \in H$. As $x^2 \in H$, $x^{2n} \in H$ for all $n \in \mathbb{Z}$. In particular, $x^{12} \in H$. But we already know that $x^{11} = e$, so $x = x \cdot e = x \cdot x^{11} = x^{12} \in H$ implies that $x \in H$, which is what we needed to prove. \qed

11. If $H$ is a normal subgroup of $G$ and $K$ is any subgroup of $G$, prove that the subgroup $H \cap K$ is normal in $K$.

Proof. We will apply the Normal Subgroup Test to $N = H \cap K$, viewed as a subgroup of $K$ (we know that $N \leq K$ from previous work). Suppose $x \in K$ and $y \in N$. Since $N = H \cap K$, $y \in N$ implies that $y \in H$ and $y \in K$. Thus, since $K$ is a subgroup of $G$, the product $xyx^{-1} \in K$ since both $x, y \in K$. Since $H$ is normal in $G$, the product $xyx^{-1} \in H$ as $y \in H$ and $x \in K \leq G$. Therefore, $xyx^{-1} \in H \cap K = N$, so $xNx^{-1} \subseteq N$. Hence $N$ is normal in $K$ since the element $x \in K$ was arbitrary. \qed

12. Let $G$ be a group with more than one element. Is it ever the case that the set of all homomorphisms from $G$ to $G$ is a group under function composition? Justify your answer.

Solution: No.

Proof. First of all, under function composition, the “identity element” must be the identity function, $id_G : G \rightarrow G$ given by $id_G(g) = g$ for all $g \in G$.

We know that for any pair of groups $G_1$ and $G_2$, there is always the trivial homomorphism $\varepsilon : G_1 \rightarrow G_2$ defined by $\varepsilon(g) = e_2$ for all $g \in G_1$, where $e_2$ is the identity element of $G_2$. We claim that the homomorphism $\varepsilon : G \rightarrow G$ is not invertible in the set of all homomorphisms from $G$ to $G$ under function composition. For, suppose to the contrary that there is a homomorphism $\varphi : G \rightarrow G$ such that $\varphi \circ \varepsilon = id_G$. Let $g \in G$ be an element other that $e$, which exists since we are assuming that $G$ is a group with more than one element. Consider $\varphi(\varepsilon(g)) = \varphi(e) = e \neq g = id_G(g)$, so $\varphi \circ \varepsilon \neq id_G$. Hence the homomorphism $\varepsilon$ has no inverse, so the set of all homomorphisms from $G$ to $G$ under function composition is not a group. \qed

13. Show that there are infinitely many homomorphisms from $\mathbb{Z}$ to itself.

Solution: For each integer $n \geq 0$, define the function $\varphi_n : \mathbb{Z} \rightarrow \mathbb{Z}$ by $\varphi_n(a) = na$. Then $\varphi_n$ is a function from $\mathbb{Z}$ to itself which is operation-preserving, since

$$\varphi_n(a + b) = n(a + b) = na + nb = \varphi_n(a) + \varphi_n(b).$$

Hence, $\varphi_n$ is a group homomorphism from $\mathbb{Z}$ to itself for each integer $n \geq 0$. We claim that if $n$ and $m$ are distinct non-negative integers, then $\varphi_n$ and $\varphi_m$ are distinct homomorphisms. To see this, it is enough to compare $\varphi_n(1) = n1 = n$ with $\varphi_m(1) = m1 = m$. As $n \neq m$, $\varphi_n(1) \neq \varphi_m(1)$, so $\varphi_n \neq \varphi_m$. Thus there are infinitely many group homomorphisms from $\mathbb{Z}$ to itself.

14. Given that $m$ divides $n$, show that $\mathbb{Z}/m\mathbb{Z}$ is a homomorphic image of $\mathbb{Z}/n\mathbb{Z}$.
Proof. Let $m, n$ be integers such that $m$ divides $n$. Define a map $\varphi : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ by $\varphi(a) = a \mod m$. We need to show that $\varphi$ is well-defined, is a homomorphism, and is onto.

Suppose $a = b \mod n$. Then $n$ divides $a - b$, say $a - b = nq$ for some integer $q$. Since $m$ divides $n$, we may write $n = mp$ for some $p \in \mathbb{Z}$. Therefore, $a - b = nq = mpq$ and $pq \in \mathbb{Z}$, so $m$ divides $a - b$. Hence $a = b \mod m$. Therefore, $\varphi(a) = a \mod m = b \mod m = \varphi(b)$, so $\varphi : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ is well-defined.

Now suppose $a, b \in \mathbb{Z}/n\mathbb{Z}$ and consider $\varphi(a+b) = (a+b) \mod m = (a \mod m) + (b \mod m) \mod m = \varphi(a) + \varphi(b)$, so $\varphi$ is a homomorphism.

Finally, suppose $c \in \mathbb{Z}/m\mathbb{Z}$. Then there is an integer $a$ such that $0 \leq a < m$ and $c = a \mod m$. Consider $a$ in $\mathbb{Z}/n\mathbb{Z}$. Then $\varphi(a) = a \mod m = c$, so $\varphi$ is onto. Thus $\mathbb{Z}/m\mathbb{Z}$ is a homomorphic image of $\mathbb{Z}/n\mathbb{Z}$ as claimed. 

15. Suppose that $\varphi$ is a homomorphism from a group $G$ to an Abelian group $H$ and $N$ is a subgroup of $G$ that contains $\ker \varphi$. Prove that $N$ is normal in $G$.

Proof. Suppose that $\varphi : G \rightarrow H$ is a homomorphism, where $H$ is an Abelian group. Let $N \leq G$ be a subgroup such that $\ker \varphi \subseteq N$. Let $x \in G$ and $y \in N$ and consider $xyx^{-1} \in G$. In particular, consider $\varphi(xyx^{-1}) = \varphi(x)\varphi(y)\varphi(x^{-1})$ in $H$, which is Abelian. Thus $\varphi(x)\varphi(y)\varphi(x^{-1}) = \varphi(x)\varphi(x^{-1})\varphi(y) = \varphi(xx^{-1})\varphi(y) = \varphi(y)$. Thus $\varphi(xyx^{-1}) = \varphi(y)$, so $\varphi(xyx^{-1})\varphi(y)^{-1} = \varphi(xyx^{-1}y^{-1}) = e_H$. Therefore, $xyx^{-1}y^{-1} \in \ker \varphi$, which is contained in $N$ and $y \in N$, so $xyx^{-1} = (xyx^{-1}y^{-1})y \in N$. Hence $xNx^{-1} \subseteq N$ since $y \in N$ was arbitrary. So, by the Normal Subgroup Test, $N$ is normal in $G$, since $x \in G$ was arbitrary.