Group Actions and Orbits

Let $G$ be a group with identity $e$ and $X$ be a (nonempty) set. A left [right] group action of $G$ on $X$ is a function $\phi : G \times X \to X$ [or $\phi : X \times G \to X$] satisfying for all $x \in X$, $\phi(e, x) = x$ [or $\phi(x, e) = x$] and for all $g, h \in G$ and all $x \in X$, $\phi(gh, x) = \phi(g, \phi(h, x))$ [or $\phi(x, gh) = \phi(\phi(x, g), h)$].

Examples:

1. Let $n \in \mathbb{N}$. $GL_n(\mathbb{R})$ acts on the vector space $\mathbb{R}^n$ as follows: $\phi(A, \mathbf{v}) = A\mathbf{v}$. ELFY: Show this is a (left) group action.

2. Let $n \in \mathbb{N}$. $S_n$ acts on the set $\{1, 2, ..., n\}$ as follows: $\phi(i, \sigma) = (i)\sigma$. ELFY: Show this is a (right) group action.

3. Let $G$ be a group with identity $e$. $G$ acts on itself via $\phi(g, h) = gh$. This can be viewed as either a left or right group action. Let’s justify that it is indeed a left group action: Let $g \in G$. Then $\phi(e, g) = eg = g$. Let $h, k \in G$. Then $\phi(gh, k) = (gh)k = g(hk) = \phi(g, hk) = \phi(g, \phi(h, k))$.

Let $\phi$ be a left group action of a group $G$ on a set $X$. Let $x \in X$. The orbit of $x \in X$ under $\phi$ is the set $\{\phi(g, x) | g \in G\}$. A similar definition works for right group actions.

Example:

Consider the right group action of $H$ on $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$ where $H$ is the cyclic subgroup of $S_8$ generated by $\sigma = (1\ 3\ 6)(2\ 8)(4\ 7\ 5)$ in cycle notation. What are the orbits?

The orbit of 1 or 3 or 6 is $\{1, 3, 6\}$. The orbit of 2 or 8 is $\{2, 8\}$. The orbit of 4 or 5 or 7 is $\{4, 5, 7\}$. Together, these three orbits form a partition of $X$. 
Alternating Groups and Cayley’s Theorem

Let $n \geq 2$ be an integer. Let’s have some more fun with $S_n$:

A cycle of length 2 in $S_n$ is a transposition. So for example $(1 \ 3)$ is a transposition in $S_n$ (for $n \geq 3$) while $(1 \ 2 \ 3)$ is not.

By direct computation we find that a cycle $(i_1 \ i_2 \ldots \ i_\ell) \in S_n$ satisfies $(i_1 \ i_2 \ldots \ i_\ell) = (i_1 \ i_{\ell-1})(i_{\ell-1} \ i_{\ell-2})
\ldots \cdot (i_2 \ i_1)$. So EVERY cycle is a product of transpositions. Since every element of $S_n$ is a product of disjoint cycles, and each cycle is a product of transpositions, it follows that every element of $S_n$ is a product of transpositions!

**Proposition 5.1:** No permutation in symmetric group $S_n$ (where $n \geq 2$ is an integer) can be expressed as a product of an even number and an odd number of transpositions.

**Proof:** Let $P_n$ be the set of $n \times n$ permutation matrices: Every row and column has exactly one 1 and all other entries are zero. (ELFY) Show $P_n$ is a group under matrix multiplication.

Let’s show that $S_n \cong P_n$. Let $\phi : S_n \rightarrow P_n$ be given by $\phi(\sigma) = P_\sigma$ where the $(i, j)$-entry of $P_\sigma$ is 1 if $(i)\sigma = j$ and 0 otherwise.

Since $\sigma$ is function, each row of $P_\sigma$ has one and only one 1. Since $\sigma$ is 1 − 1 and onto, each column of $P_\sigma$ has one and only one 1. So $\phi$ is well-defined.

It should also be clear that for $\sigma, \tau \in S_n$, if $\phi(\sigma) = \phi(\tau) = A$ then $\sigma = \tau$ as for $i = 1, 2, \ldots, n$ we have $(i)\sigma = j_i = (i)\tau$ where the $j_i$th entry in row $i$ of $A$ is the unique non-zero entry (namely a 1) in row $i$ of $A$. Hence $\phi$ is 1 − 1.

Let $A$ be an $n \times n$ permutation matrix. Let $j_i$ be the column of the unique non-zero entry in row $i$. Let $\sigma_A : \{1, 2, \ldots, n\} \rightarrow \{1, 2, \ldots, n\}$ be given by $(i)\sigma_A = j_i$ for $i \in \{1, 2, \ldots, n\}$. First, $\sigma_A$ is well-defined because each row of $A$ has only one non-zero entry. $\sigma_A$ is 1 − 1 because each column of $A$ has at most one non-zero entry. $\sigma_A$ is onto since each column has at least one non-zero entry. Then, by construction, $\sigma_A \in S_n$ and $\phi(\sigma_A) = A$. So $\phi$ is onto.

Finally, let $\sigma, \tau \in S_n$. $\phi(\sigma\tau) = A$ where the $(i, j)$ entry of $A$ is 1 if $i(\sigma\tau) = j$ and 0 otherwise. Let $B = \phi(\sigma)$ and $C = \phi(\tau)$. Let $D = BC$. The $(i, j)$ entry of $D$ is 1 iff there exists an integer $k$ such that the $(i, k)$- and $(k, j)$-entry of $B$ and $C$ respectively are both 1. So the $(i, j)$-entry of $D$ is 1 iff there exists an integer $k$ such that $(i)\sigma = k$ and $(k)\tau = j$. So the $(i, j)$-entry of $D$ is 1 iff $(i)\sigma\tau = j$. Thus $D = A$ and $\phi$ is an isomorphism.

Suppose there is an element $\sigma \in S_n$ that can be written as product of an even number of transpositions and an odd number of transpositions. This means that on one hand, $\sigma = t_1t_2\ldots t_r$ where $t_i$ is a transposition for $i = 1, 2, ..., r$ and $r$ is odd, while on the other hand, $\sigma = t'_1t'_2\ldots t'_s$ where $t'_i$ is a transposition for $i = 1, 2, ..., s$ and $s$ is even.

Since for any transposition $(i \ j)$, the permutation matrix $P_{(i \ j)}$ is obtained from $I_n$ by switching two rows, it follows that $P_\sigma$ can obtained by doing an odd number of row switches and by doing an even number of row switches. This means that its determinant is both $−1$ and $1$, which is a contradiction. That completes the proof. □
So a permutation $\sigma \in S_n$ is **even** if it can be written as a product of an even number of transpositions and **odd** if it can be written as a product of an odd number of transpositions. Obviously every permutation is either even or odd; furthermore, we have shown that no permutation in $S_n$ is both even and odd. Hence, the set of even permutations and the set of odd permutations partition $S_n$.

**Proposition 5.2:** Let $n \geq 2$ be an integer. Let $A_n$ and $B_n$ be the partition of $S_n$ into sets of even and odd permutations respectively. Then $|A_n| = |B_n| = \frac{n!}{2}$.

**Proof:** Let’s construct a bijection from $A_n$ to $B_n$. Let $f : A_n \rightarrow B_n$ be given by $f(\sigma) = (1 2)\sigma$. Since $\sigma$ can be written as a product of an even number of transpositions, $f(\sigma)$ can be written as a product of an odd number of transpositions. Hence $f$ is well-defined.

Let $\sigma, \tau \in A_n$. Suppose $f(\sigma) = f(\tau)$. Then $(1 2)\sigma = (1 2)\tau$. By left-cancelation, we get $\sigma = \tau$. Hence $f$ is 1–1.

Now let $\rho \in B_n$. So $\rho$ can be written as a product of an odd number of transpositions. Then $(1 2)\rho$ can be written as a product of an even number of transpositions. Furthermore, $f((1 2)\rho) = (1 2)(1 2)\rho = 1(2)^2\rho = (\text{Id})\rho = \rho$. So $f$ is onto. So $f$ is a bijection from $A_n$ to $B_n$. Consequently the finite sets $A_n$ and $B_n$ have the same number of elements, and since $|A_n| + |B_n| = |S_n| = n!$, we get $|A_n| = |B_n| = \frac{n!}{2}$. $\square$

**Proposition 5.3:** Let $n \geq 2$ be an integer. Let $A_n$ be the set of even permutations in $S_n$. $A_n < S_n$.

**Proof:** Clearly $A_n$ is a proper nonempty subset of $S_n$ as $\text{Id} = (1 2)^2 \in A_n$ and $(1 2) \in S_n \setminus A_n$.

Let $\sigma, \tau \in A_n$. So $\sigma = t_1t_2 \cdots t_r$ where $t_i \in S_n$ is a transposition for $i = 1, 2, ..., r$ and $r$ is even. Also $\tau = t'_1t'_2 \cdots t'_s$ where $t'_i \in S_n$ is a transposition for $i = 1, 2, ..., s$ and $s$ is even. Then $\sigma \tau \in A_n$ as it can be written as an even number of transpositions (namely $r + s$). So $A_n$ is closed under the group operation in $S_n$. Notice that $\tau^{-1} = t'_{s}t'_{s-1} \cdots t'_1$. Hence $\sigma \tau^{-1} \in A_n$ as it can be written as an even number of transpositions (namely $r + s$). So $A_n < S_n$ by the 1-step subgroup test. $\square$

The subgroup $A_n < S_n$ of even permutations is called the alternating group.

Here is $A_3$: $\{\text{Id}, (1 \ 2 \ 3), (1 \ 3 \ 2)\}$. ELFY: Show $A_3 \cong \mathbb{Z}_3$. Hint: $A_3 = \langle (1 \ 2 \ 3) \rangle$.

Here is $A_4$:

$\{\text{Id}, (1 \ 2 \ 3), (1 \ 3 \ 2), (1 \ 2 \ 4), (1 \ 4 \ 2), (1 \ 3 \ 4), (1 \ 4 \ 3), (2 \ 3 \ 4), (2 \ 4 \ 3), (1 \ 2)(3 \ 4), (1 \ 3)(2 \ 4), (1 \ 4)(2 \ 3)\}$. 
Let $G$ be a group. The symmetric group of $G$ is $S_G = \{ f : G \to G | f \text{ is a bijection} \}$ under composition (we don’t bother using the composition symbol, so $f \circ g$ is just written $fg$).

**Proposition 5.4 (Cayley’s Theorem):** Every group $G$ is isomorphic to a subgroup of $S_G$, the symmetric group of $G$.

**Proof:** Let $G$ be a group with identity $e$. For each $g \in G$, let the function $f_g : G \to G$ be defined by $f_g(a) = ga$. Let $g, h, k \in G$. Suppose $f_g(h) = f_g(k)$. Then $gh = gk$ and hence $h = k$. So $f_g$ is 1–1. Furthermore, $f_g(g^{-1}h) = gg^{-1}h = h$, so $f_g$ is onto. So $f_g$ is a bijection from $G$ to itself, and hence an element of $S_G$.

Notice that for all $x \in G$, $(fgf_{g^{-1}})(x) = f_g(f_{g^{-1}}(x)) = f_g(g^{-1}x) = gg^{-1}x = x$ and $(f_{g^{-1}}f_g)(x) = f_{g^{-1}}(f_g(x)) = f_{g^{-1}}(gx) = g^{-1}gx = x$. So $f_{g^{-1}} = f_{g^{-1}}$. Also, notice that $f_e = Id_G$ as for all $a \in G$, $f_e(a) = ea = a = Id_G(a)$.

So far we have established that $K = \{ f_g | g \in G \} \subseteq S_G$ contains the identity in $S_G$ and for each $k \in K$, $k^{-1} \in K$. Let $f_g, f_h \in K$. In particular, $f_gf_{h^{-1}} = f_gf_{h^{-1}}$. Let $x \in G$. Then $(f_gf_{h^{-1}})(x) = (f_gf_{h^{-1}})(x) = f_g(f_{h^{-1}}(x)) = f_g(h^{-1}x) = g(h^{-1}x) = (gh^{-1})x = f_{gh^{-1}}(x)$. So $f_gf_{h^{-1}} = f_{gh^{-1}} \in K$ showing that $K \leq S_G$ by the 1-step subgroup test.

Now define $\phi : G \to K$ by the rule $\phi(g) = f_g$. It is well-defined and onto by construction. Let $g_1, g_2 \in G$. Suppose that $\phi(g_1) = \phi(g_2)$. Then $f_{g_1} = f_{g_2}$. Thus $g_1 = f_{g_1}(e) = f_{g_2}(e) = g_2$. Therefore $\phi$ is 1–1, and hence a bijection. It only remains to show that $\phi$ has the “morphism” property:

Let $g, h \in G$. Let $x \in G$. Then

$$\phi(gh)(x) = f_{gh}(x) = (gh)x = g(hx) = f_g(hx) = f_g(f_h(x)) = (f_gf_h)(x) = (\phi(g)\phi(h))(x).$$

Therefore $\phi(gh) = \phi(g)\phi(h)$. So $\phi$ is an isomorphism. That completes the proof. $\square$
Cosets and Lagrange’s Theorem

Let $G$ be a group with identity $e$ and $H \leq G$. Define (binary) relations $\sim_1$ and $\sim_2$ on $G$ as follows:

For all $a, b \in G$, $a \sim_1 b$ iff $a^{-1}b \in H$ and $a \sim_2 b$ iff $ab^{-1} \in H$.

Let’s prove that $\sim_1$ and $\sim_2$ are equivalence relations:

Let $a, b, c \in G$.

(i) $a^{-1}a = aa^{-1} = e \in H$ (as $H$ is a subgroup). Hence $a \sim_1 a$ and $a \sim_2 a$. Thus $\sim_1$ and $\sim_2$ are reflexive.

(ii) Assume $a \sim_1 b$. Then $a^{-1}b \in H$. Since $H$ is a subgroup, $(a^{-1}b)^{-1} = b^{-1}(a^{-1})^{-1} = b^{-1}a$ is in $H$. Thus $b \sim_1 a$. Hence $\sim_1$ is symmetric. A similar argument (ELFY) shows that $\sim_2$ is symmetric.

(iii) Assume $a \sim_1 b$ and $b \sim_1 c$. Then $a^{-1}b, b^{-1}c \in H$. Since $H$ is a subgroup, $(a^{-1}b)(b^{-1}c) = a^{-1}(bb^{-1})c = a^{-1}c$ is in $H$. Hence $a \sim_1 c$. Thus $\sim_1$ is transitive. A similar argument (ELFY) shows that $\sim_2$ is transitive.

Therefore $\sim_1$ and $\sim_2$ are equivalence relations! So the equivalence classes of $\sim_i$ partition $G$ for $i = 1, 2$.

These equivalence relations each define a partition of $G$ by their equivalence classes. Let $g \in G$. The equivalence class under $\sim_1$ of $g$ consists of all $x \in G$ such that $g^{-1}x \in H$, that is, $g^{-1}x = h$ (equivalently $x = gh$) for some $h \in H$. In other words, the equivalence class of $g$ consists of $gH = \{gh|h \in h\}$ ($H$-orbit of $g$ where $H$ acts on $G$ on the right). Similarly (ELFY) we have that the equivalence class under $\sim_2$ of $g$ is $Hg = \{hg|h \in H\}$.

Let $G$ be a group and $H \leq G$. Let $g \in G$. The set $gH$ is called the left coset of $H$ containing $g$ and the set $Hg$ is called the right coset of $H$ containing $g$.

Example:

Let $G = S_3 = \{Id, (1 2), (2 3), (1 3), (1 2 3), (1 3 2)\}$. Let $H = < (1 2) >$.

Let’s compute all the left cosets of $H$:

There is $H = (Id)H, (2 3)H = \{(2 3), (1 2 3)\}, (1 3)H = \{(1 3), (1 3 2)\}$.

Let’s compute all the right cosets of $H$:

There is $H = H(Id), H(2 3) = \{(2 3), (1 3 2)\}, H(1 3) = \{(1 3), (1 2 3)\}$.

Notice that the left/right cosets $gH$ and $Hg$ may not be equal!
However, if the $G$ is abelian group then they must be equal: Suppose $G$ is abelian and $H \leq G$. Let $g \in G$. Then $gH = \{gh | h \in H\}$. Since $G$ is abelian, $gH = \{gh | h \in H\} = \{hg | h \in H\} = Hg$.

Let $G$ be a group with identity $e$ and $H \leq G$.

Let’s show that for all $g \in G$ we have $g \in H$ iff $gH = H$: Let $g \in H$. Then $gH \subseteq H$ since for all $h \in H$, $gh \in H$. Let $k \in H$. Then $g^{-1}k \in H$. Then $k = g(g^{-1}k) \in gH$. So $H \subseteq gH$. Thus $gH = H$. Conversely, let $g \in G$ and assume $gH = H$. Since $e \in H$ we have that $g = ge \in gH = H$, so $g \in H$.

Similarly (ELFY) $H = Hg$ iff $g \in H$.

**Lemma 6.1**: Let $G$ be a finite group and $H \leq G$. Let $g_1, g_2 \in G$. Then the left/right cosets are of the same size:

$$|g_1H| = |g_2H| = |Hg_1| = |Hg_2|.$$

**Proof**: Let $\phi : H \to g_1H$ be given by $\phi(h) = g_1h$. This function is well-defined and onto by construction. Let $h_1, h_2 \in H$. Suppose $\phi(h_1) = \phi(h_2)$. Then $g_1h_1 = g_1h_2$, which yields $h_1 = h_2$, so $\phi$ is 1 - 1. So $\phi$ is a bijection between $H$ and $g_1H$. Hence $|H| = |g_1H|$. A similar argument (ELFY) shows that $|H| = |Hg_1|$. Thus $|H| = |g_1H| = |g_2H| = |Hg_1| = |Hg_2|$ □

**Proposition 6.2 (Lagrange’s Theorem)**: Let $G$ be a finite group and $H \leq G$. Then the order $H$ divides the order of $G$.

**Proof**: Let $n = |G|$ and $m = |H|$. Let $r \in \mathbb{N}$ be the number of left cosets of $H$ in $G$. Since the left cosets of $H$ partition $G$ and they are all of size $m = |H|$, we have that $mr = n$ □

**Corollary 6.3**: Let $G$ be a finite group and of order $p > 1$ where $p$ is a prime. Then $G$ is cyclic (hence isomorphic to $\mathbb{Z}_n$).

**Proof**: Let $g \in G \setminus \{e\}$ where $e$ is the identity. Set $H = \langle g \rangle$. Then $|H| > 1$ as there are at least two distinct elements in $H$, namely $g$ and $e$. By Lagrange’s theorem, $|H| = 1$ or $|H| = p$. Hence $|H| = p$. But then $H = G$. So $g$ generates $G$, showing $G$ is cyclic □

**Corollary 6.4**: Let $G$ be a finite group and $g \in G$. Then the order of $g$ divides the order of $G$.

**Proof**: Just apply to Lagrange’s Theorem to the subgroup $H = \langle g \rangle$ □
Let \( H \leq G \). The index of \( H \) in \( G \), denoted \((G : H)\) is the number of left cosets of \( H \) in \( G \). This could be finite or infinite. If \( G \) is finite then \((G : H)\) is finite and \((G : H) = |G|/|H|\) (see proof of Lagrange’s Theorem). If \( G \) is infinite, then \((G : H)\) could be finite (like \((\mathbb{Z} : n\mathbb{Z})\) under addition) or infinite (like \((\mathbb{R} : \mathbb{Z})\) under addition).

(ELFY) Let \( G \) be a finite group and \( K \leq H \leq G \). Show that \((G : K) = (G : H)(H : K)\).
Homomorphisms

Let $G$ and $G'$ be groups. A function $\phi : G \to G'$ is a homomorphism if for all $g, h \in G$, $\phi(gh) = \phi(g)\phi(h)$.

Note: A homomorphism is an isomorphism if the function is a bijection.

Example:

Let $G = S_n$ and $G' = \mathbb{Z}_2$. Then define $\phi : G \to G'$ by

$$\phi(\sigma) = \begin{cases} 
0 & \text{if } \sigma \in A_n \\
1 & \text{if } \sigma \notin A_n
\end{cases}$$

By construction this function is well-defined. Let $\sigma_1, \sigma_2$ be in $S_n$.

Suppose $\phi(\sigma_1\sigma_2) = 0$. Then $\sigma_1\sigma_2$ can be written as an even number of transpositions. This means that either $\sigma_1$ and $\sigma_2$ are both even or both odd. In the former case, $\phi(\sigma_1) = \phi(\sigma_2) = 0$. In the latter case, $\phi(\sigma_1) = \phi(\sigma_2) = 1$. Either way $\phi(\sigma_1) + \phi(\sigma_2) = 0$.

Suppose $\phi(\sigma_1\sigma_2) = 1$. Then $\sigma_1\sigma_2$ can be written as an odd number of transpositions. So one must be even and the other odd. Assume (WLOG) that $\sigma_1$ is odd and $\sigma_2$ is even. Then $\phi(\sigma_1) = 1$ and $\phi(\sigma_2) = 0$. Hence $\phi(\sigma_1) + \phi(\sigma_2) = 1$.

Either way, $\phi(\sigma_1\sigma_2) = \phi(\sigma_1) + \phi(\sigma_2)$. So $\phi$ is a homomorphism.

Another example:

Let $n \in \mathbb{N}$. Recall that $GL_n(\mathbb{R})$ is the general linear group (invertible $n \times n$ matrices under multiplication) and $\mathbb{R}^*$ is the group of non-zero reals under multiplication.

Since for all $A, B \in GL_n(\mathbb{R})$ we have $\det(AB) = (\det(A))(\det(B))$ it follows that $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$ is a homomorphism.
Let \( \phi : G \to G' \) be a group homomorphism between groups \( G \) and \( G' \) with identities \( e \) and \( e' \) respectively.

The following fundamental facts are left as ELFY:

1. \( \phi(e) = e' \).
2. For all \( g \in G \), \( \phi(g^{-1}) = \phi(g)^{-1} \).
3. For any \( H \leq G \), \( \phi(H) = \{ \phi(h) | h \in H \} \) (the image of \( H \) under \( \phi \)) satisfies \( \phi(H) \leq G' \).
4. For any \( K \leq G' \), \( \phi^{-1}(K) = \{ g \in G | \phi(g) \in K \} \) (the pre-image of \( K \) under \( \phi \)) satisfies \( \phi^{-1}(K) \leq G \).

Let \( \phi : G \to G' \) be a homomorphism of groups \( G \) and \( G' \) with identities \( e \) and \( e' \) respectively. The kernel of \( \phi \) is the set \( \text{Ker}(\phi) = \{ g \in G | \phi(g) = e' \} \) (elements in \( G \) that map to \( e' \) under \( \phi \)).

Let \( T_A : \mathbb{R}^n \to \mathbb{R}^m \) given by \( T_A(x) = Ax \) where \( A \) is an \( m \times n \) matrix. Recall that such a function is called a linear transformation. Since \( \mathbb{R}^n \) and \( \mathbb{R}^m \) are groups under addition, and for all \( x, y \in \mathbb{R}^n \) we have \( T_A(x + y) = T_A(x) + T_A(y) \), \( T_A \) is a group homomorphism. What’s the \( \text{Ker}(T_A) \)? It’s the null space of \( A \) of course.

**Proposition 7.1** : Let \( G \) and \( G' \) be groups with identities \( e \) and \( e' \) respectively. Let \( \phi : G \to G' \) be a homomorphism and \( H = \text{Ker}(\phi) \). Then \( H \leq G \).

**Proof**: Since \( \phi(e) = e' \) we know that \( H \) is a nonempty subset of \( G \). Let \( g, h \in H \). Then \( \phi(g) = e' \) and \( \phi(h) = e' \). Then \( \phi(gh^{-1}) = \phi(g)\phi(h^{-1}) = e'(\phi(h))^{-1} = (e')^{-1} = e' \). Hence \( gh^{-1} \in H \) showing \( H \leq G \). \( \square \)

Consider the function \( f : \mathbb{C}^* \to \mathbb{R}^+ \) (between groups under multiplication) given by \( f(z) = |z| \).

Since for all \( z_1, z_2 \in \mathbb{C}^* \) we know that \( f(z_1z_2) = |z_1z_2| = |z_1||z_2| = f(z_1)f(z_2) \) it follows that \( f \) is a homomorphism. What’s the kernel of \( f \)? It’s a subgroup we have already encountered! It’s the circle group, \( U = \{ a \in \mathbb{C} : |a| = 1 \} \).
**Proposition 7.2:** Let $G$ and $G'$ be groups with identities $e$ and $e'$ respectively. Let $\phi : G \to G'$ be a homomorphism and $H = \text{Ker}(\phi)$. Let $g \in G$. Then the pre-image set $\phi^{-1}(\phi(g)) = \{x \in G | \phi(x) = \phi(g)\}$ is both the left coset $gH$ and the right coset $Hg$. Consequently, the partition of $G$ into left cosets of $H$ in $G$ is the same as the partition of $G$ into right cosets of $H$ in $G$.

**Proof:** Let $x \in \phi^{-1}(\phi(g))$. Then $\phi(x) = \phi(g)$. Then $\phi(x)\phi(g)^{-1} = e'$ and $\phi(g)^{-1}\phi(x) = e'$. Thus $\phi(x)\phi(g)^{-1} = e'$ and $\phi(g)^{-1}\phi(x) = e'$ and hence $\phi(xg^{-1}) = e'$ and $\phi(g^{-1}x) = e'$. So $g^{-1}x \in H$ and $xg^{-1} \in H$. This means that $x = gh_1$ and $x = h_2g$ for some $h_1, h_2 \in H$. Thus $x \in gH \cap Hg$. So $\phi^{-1}(\phi(g)) \subseteq gH$ and $\phi^{-1}(\phi(g)) \subseteq Hg$.

Now let’s show that the reverse containments hold. Let $x \in gH$ Then $x = gh$ for some $h \in G$. Then $\phi(x) = \phi(gh) = \phi(g)\phi(h) = \phi(g)e' = \phi(g)$ implies $x \in \phi^{-1}(\phi(g))$. So $gH \subseteq \phi^{-1}(\phi(g))$. A similar argument (ELFY) shows that $Hg \subseteq \phi^{-1}(\phi(g))$. Consequently, $gH = \phi^{-1}(\phi(g)) = Hg$. □

A $1-1$ homomorphism is called a **monomorphism**. An onto homomorphism is called an **epimorphism**.

**Proposition 7.3:** Let $G$ and $G'$ be groups with identities $e$ and $e'$ respectively. Let $\phi : G \to G'$ be a homomorphism. $\phi$ is a monomorphism iff $\text{Ker}(\phi) = \{e\}$.

**Proof:** Assume $\phi$ is a monomorphism. Then for all $a, b \in G$, $\phi(a) = \phi(b)$ implies $a = b$. We already know that $\phi(e) = e'$ and so $\{e\} \subseteq \text{Ker}(\phi)$. Let $x \in \text{Ker}(\phi)$. Then $\phi(x) = e' = \phi(e)$. Since $\phi$ is $1-1$ we get that $x = e$. Hence $\text{Ker}(\phi) \subseteq \{e\}$ and so $\text{Ker}(\phi) = \{e\}$.

Conversely, assume $\text{Ker}(\phi) = \{e\}$. Let $g, h \in G$. Suppose $\phi(g) = \phi(h)$. Then (following steps we’ve seen before) $\phi(gh^{-1}) = e'$. This means that $gh^{-1} \in \text{Ker}(\phi) = \{e\}$. So $gh^{-1} = e$ which implies $g = h$. Since that means $\phi$ is $1-1$, we have that $\phi$ is a monomorphism. □

If $\phi$ is a group monomorphism and in addition is onto, then it is an isomorphism! This suggests a straightforward procedure for showing that a function $\phi : G \to G'$ (where $G, G'$ are groups) is a group isomorphism:

(i) Show that $\phi$ is a homomorphism.  
(ii) Show that $\text{Ker}(\phi) = \{e\}$ (where $e$ is the identity in $G$).  
(iii) Show that $\phi$ is onto.

Example:

Let $n \geq 2$ be an integer. Let’s show that $\mathbb{Z} \cong n\mathbb{Z}$ as groups under addition.

Define $\phi : \mathbb{Z} \to n\mathbb{Z}$ by the rule $\phi(k) = nk$. This is a well-defined function by construction.
Let’s show $\phi$ is a homomorphism:

Let $k_1, k_2 \in \mathbb{Z}$. Then $\phi(k_1 + k_2) = n(k_1 + k_2) = nk_1 + nk_2 = \phi(k_1) + \phi(k_2)$. So $\phi$ is a homomorphism.

Let’s show that $\ker(\phi) = \{0\}$:

We know that $0 \in \ker(\phi)$ since $\phi$ is an homomorphism (or by direct calculation). Let $k \in \mathbb{Z}$. Suppose $k \in \ker(\phi)$. Then $\phi(k) = 0$ which means that $nk = 0$. Since $n \neq 0$ it follows that $k = 0$. Thus $\ker(\phi) = \{0\}$. So $\phi$ is $1 - 1$ (a monomorphism).

Let’s show that $\phi$ is onto:

Let $m \in n\mathbb{Z}$. Then $m = nk$ for some $k \in \mathbb{Z}$. Hence $\phi(k) = m$ showing that $\phi$ is onto (an epimorphism).

Putting all this together we get that $\phi$ is an isomorphism and $\mathbb{Z} \cong n\mathbb{Z}$. 
Normal Subgroups and Factor Groups

Let $G$ be a group. $N \leq G$ is a normal subgroup if for all $g \in G$, $gN = Ng$ (that is, if the left and right cosets of $N$ containing $g$ coincide).

Notation for a normal subgroup: $N \trianglelefteq G$. We write $N \vartriangleleft G$ if it is a proper normal subgroup. Any group is always a normal subgroup of itself. The trivial subgroup is also obviously a normal subgroup.

So by proposition 7.2 we already have an important example of a normal subgroup of any group $G$: The kernel of any group homomorphism $\phi : G \to G'$ is a normal subgroup of $G$.

Let $g \in G$. Define the set \( gNg^{-1} = \{ gng^{-1} | n \in N \} \). ELFY: Show that $gNg^{-1} \leq G$.

The following are equivalent:

1. $N$ is a normal subgroup of $G$.
2. $N = gNg^{-1}$ for all $g \in G$.
3. $N \supseteq gNg^{-1}$ for all $g \in G$.
4. $gng^{-1} \in N$ for all $n \in N$ and $g \in G$.

It’s clear that (2) implies (3) and that (3) implies (4).

Let’s show that (4) implies (1):

Let $G$ be a group, $N \trianglelefteq G$, and assume $gng^{-1} \in N$ for all $n \in N$ and $g \in G$. Let $g \in G$.

Suppose $x \in gN$. Then $x = gn_1$ for some $n_1 \in N$. Then $xg^{-1} = gn_1g^{-1}$ is an element of $N$. So $xg^{-1} = n_2$ for some $n_2 \in N$. Thus $x = n_2g$ showing that $x \in Ng$. So $gN \subseteq Ng$.

Now suppose $x \in Ng$. Then $x = n_1g$ for some $n_1 \in N$. Then $g^{-1}x = g^{-1}n_1g = (g^{-1})n_1(g^{-1})^{-1}$ is in $N$. So $g^{-1}x = n_2$ for some $n_2 \in N$. Thus $x = gn_2$ showing that $x \in gN$. So $Ng \subseteq gN$. Hence $gN = Ng$ thereby showing that $N$ is a normal subgroup of $G$.

Let’s show that (1) implies (2):

Let $G$ be a group and $N \trianglelefteq G$. Let $g \in G$ and $n \in N$.

Let $x = gng^{-1}$. Then $xg = gn$ is in $gN$. Since $gN = Ng$ there exists $n' \in N$ such that $xg = n'g$. Hence $x = n'g$. This shows that $gNg^{-1} \subseteq N$ for all $g \in G$.

Notice that $n = g ((g^{-1})n (g^{-1})^{-1}) g^{-1}$ and $(g^{-1})n (g^{-1})^{-1} \in N$ by our argument above (since $g^{-1} \in G$). Therefore $N \subseteq gNg^{-1}$ for all $g \in G$. So $N = gNg^{-1}$.

So one can use any of the other three conditions as an equivalent reformulation of the definition of a normal subgroup.
Consider the group \( G = S_3 = \{Id, (1 \, 2), (2 \, 3), (1 \, 3), (1 \, 2 \, 3), (1 \, 3 \, 2)\} \). Let \( H = \langle (1 \, 2) \rangle \).

Let \( K = A_3 = \langle (1 \, 2 \, 3) \rangle \).

Consider that \((2 \, 3)(1 \, 2)(2 \, 3)^{-1} = (1 \, 2 \, 3)(2 \, 3) = (1 \, 3) \not\in H\). Hence \( H \) is not a normal subgroup of \( G \). However, \( K \) is a normal subgroup of \( G \) by applying the following proposition:

**Proposition 8.1** : Let \( G \) be a finite group and \( H \leq G \) be of index \([G : H] = 2\) (i.e. \(|G|/|H| = 2\)). Then \( H \triangleleft G \).

**Proof** : Since \([G : H] = 2\) there are two left cosets (and two right cosets) of \( H \) in \( G \). Since \([G : H] \neq 1\) we know that \( H \neq G \). Let \( g \in G \).

Suppose \( g \in H \). Then \( H = gH = Hg \).

Suppose \( g \not\in H \), then \( gH = G \setminus H \) as there are only two left cosets of \( H \) in \( G \) and those cosets partition \( G \). For the same reason, \( Hg = G \setminus H \).

Either way, \( gH = Hg \). Therefore \( H \triangleleft G \). 

Let \( G \) be a group and \( H \leq G \). Let \( x \in gH \). Then \( x = gh \) for some \( h \in G \). So \( g^{-1}x \in H \) and hence \((g^{-1}x)^{-1} = x^{-1}g \in H\). So \( x^{-1}g = h' \) for some \( h' \in H \). Thus \( g = xh' \in xH \).

Let’s show that \( gH = xH \):

Let \( a \in gH \). Then \( a = gh_a \) for some \( h_a \in H \). Then \( a = (xh')h_a = x(h'h_a) \in xH \). Thus \( gH \subseteq xH \). Now let \( b \in xH \). Then \( b = xh_b \) for some \( h_b \in H \). So \( b = (gh)h_b = g(hh_b) \in gH \). Thus \( xH \subseteq gH \). This implies \( xH = gH \).

ELFY: Show that for any \( y \in Hg \) we get \( Hy = Hg \).

(One could just appeal to the general proof of this for equivalence classes: If \( a \) is in the equivalence class of \( b \) then the equivalence class of \( a \) is the same as for \( b \).)
**Proposition 8.2**: Let $G$ be a group and $H \leq G$. Let $S$ be the set of left cosets of $H$ in $G$. We have that $(g_1H)(g_2H) = (g_1g_2)H$ is a well-defined binary operation on $S$ (meaning that if $g_1' H = g_1 H$ and $g_2' H = g_2 H$ then $(g_1' g_2')H = (g_1 g_2)H$) iff $H \trianglelefteq G$.

**Proof**: Assume that $(g_1H)(g_2H) = (g_1g_2)H$ is a well-defined binary operation on $S$.

We need to show that for all $g \in G$, $gH = Hg$.

Let $x \in gH$. Then $xH = gH$ and $H = (gg^{-1})H = (gH)(g^{-1}H) = (xH)(g^{-1}H) = (xg^{-1})H$. Hence $xg^{-1} \in H$. So $xg^{-1} = h$ for some $h \in H$. This means that $x = hg \in Hg$. So $gH \subseteq Hg$.

Now let $x \in Hg$. So $x = hg$ for some $h \in H$. Then $x^{-1} = g^{-1}h^{-1} \in g^{-1}H$ since $h^{-1} \in H$. Then $x^{-1}H = g^{-1}H$ and $H = (g^{-1}g)H = (g^{-1}1H)(gH) = (x^{-1}1H)(gH) = (x^{-1}g)H$. Hence $x^{-1}g \in H$. So $(x^{-1}g)^{-1} = g^{-1}x \in H$. This means that $g^{-1}x = h'$ for some $h' \in H$. So $x = gh' \in gH$. Thus $Hg \subseteq gH$ and so $gH = Hg$.

Thus $H \trianglelefteq G$.

Conversely, assume that $H \trianglelefteq G$. Let $a, b \in G$. We need to show that $(aH)(bH) = (ab)H$ is a well-defined binary operation on the set of cosets of $H$ in $G$ (no need to say left or right cosets as they are the same since $H$ is normal).

Let $x \in aH$ and $y \in bH$. So $aH = xH$ and $bH = yH$. Then $(ab)H = (aH)(bH)$ and $(xH)(yH) = (xy)H$. It must be shown that $(ab)H = (xy)H$. It suffices to show that $xy \in (ab)H$.

Well, $x = ah_1$ and $y = bh_2$ for some $h_1, h_2 \in H$. Then $xy = ah_1bh_2$. Since $H$ is a normal subgroup of $G$ we have that $h_1b \in Hb$, and thus $h_1b = bh_3$ for some $h_3 \in H$ since $Hb = bH$. Then $xy = abh_3h_2 \in (ab)H$ as $h_3h_2 \in H$. So the binary operation is well-defined (independent of the choice of “representatives of the cosets”) \(\square\)

**Proposition 8.3**: Let $G$ be a group with identity $e$ and $H \trianglelefteq G$. Then the set

\[ G/H = \{gH \mid g \in G\} \]

of cosets of $H$, forms a group under the well-defined binary operation $(aH)(bH) = (ab)H$, called the quotient group (aka factor group) of $G$ by $H$.

**Proof**: Let $aH, bH, cH \in G/H$.

First let’s show the binary operation is associative:

\[ [(aH)(bH)](cH) = [(ab)H](cH) = ((ab)c)H = (a(bc))H = (aH)((bc)H) = (aH)((bH)(cH)) \]

So associativity is inherited from the group $G$. 
Let’s show that there is an identity element in $G/H$:

$$(eH)(aH) = (ea)H = aH \text{ and } (aH)(eH) = (ae)H = aH.$$  So $eH = H$ is the identity element in $G/H$.

Let’s show every element of $G/H$ has an inverse in $G/H$:

$$(aH)(a^{-1}H) = (aa^{-1})H = eH = H \text{ and } (a^{-1}H)(aH) = (a^{-1}a)H = eH = H.$$  So the inverse of $aH$ is $a^{-1}H \in G/H$. This completes the proof $\square$

Examples:

1. Let $G = \mathbb{Z}$. Since $G$ is cyclic (and hence abelian) we have that any subgroup is normal. Let $n \geq 2$ be an integer. Let $H = n\mathbb{Z}$. Then the quotient group

$$G/H = \{n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, ..., (n - 1) + n\mathbb{Z}\}$$

is cyclic (as $G/H = \langle 1 + n\mathbb{Z} \rangle$) and hence is isomorphic to $\mathbb{Z}_n$. ELFY: Define an isomorphism $\phi : G/H \to \mathbb{Z}_n$.

2. Let $G = S_4$ and $H = A_4$. $H$ is a normal subgroup of $G$ because it is of index two. Then

$$G/H = \{H, (1 2)H\}.$$

3. Let $G = S_4$ and $H = \{\text{Id}, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)\}$ (the Klein 4-group up to isomorphism). $H$ is a normal subgroup of $G$:

$$(\text{Id})H = H = \{\text{Id}, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)\} = H(\text{Id})$$

$$(1 2)H = \{(1 2), (3 4), (1 4 2 3), (1 3 2 4)\} = H(1 2),$$

$$(1 3)H = \{(1 3), (1 4 3 2), (2 4), (1 2 3 4)\} = H(1 3),$$

$$(2 3)H = \{(2 3), (1 2 4 3), (1 3 4 2), (1 4)\} = H(2 3),$$

$$(1 2 3)H = \{(1 2 3), (2 4 3), (1 4 2), (1 3 4)\} = H(1 2 3),$$

$$(1 3 2)H = \{(1 3 2), (1 4 3), (2 3 4), (1 2 4)\} = H(1 3 2).$$

Then

$$G/H = \{H, (1 2)H, (1 3)H, (2 3)H, (1 2 3)H, (1 3 2)H\}.$$  

So it turns out that $G/H \cong S_3$.

ELFY: Show that if $G$ is cyclic and $N \trianglelefteq G$ then $G/N$ is cyclic.

Hint: If $G$ is cyclic then $G = \langle g \rangle$ for some $g \in G$. Then $G/N = \{aN | a \in G\}$. Use the fact that $\forall a \in G, a = g^i$ for some integer $i$. 

Proposition 8.4 (First Isomorphism Theorem): Let $G, H$ be groups with identities $e_G, e_H$ respectively and 
\[ \phi : G \to H \]
be a homomorphism. Then 
\[ G/\ker(\phi) \cong \phi(G). \]

Proof: Let $N = \ker(\phi) = \{ g \in G | \phi(g) = e_H \}$. Define $\alpha : G/N \to \phi(G)$ by the rule $\alpha(gN) = \phi(g)$.

If $gN = g'N$ in $G/N$ then $g' = gn$ for some $n \in N$. So $\phi(g') = \phi(gn) = \phi(g)\phi(n) = \phi(g)$ since $\phi(n) = e_H$. So $\alpha(gN) = \phi(g) = \phi(g') = \alpha(g'N)$. That makes $\alpha$ well-defined.

Let $g_1, g_2 \in G$. Then $\alpha((g_1N)(g_2N)) = \alpha((g_1g_2N)) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = \alpha(g_1N)\alpha(g_2N)$.

So $\alpha$ is a homomorphism.

Let's calculate the kernel of $\alpha$. We have that $N \subseteq \ker(\alpha)$ as $\alpha(N) = \ker(e_GN) = \phi$. Let $x \in G$ and assume $xN \neq N$. So $x \notin N$ and $\phi(x) \neq e_H$. Therefore $xN \notin \ker(\alpha)$ as $\alpha(xN) = \phi(x) \neq e_H$. This means that $\ker(\alpha) = \{N\}$ which tells us that $\alpha$ is 1 - 1.

Let $h \in \phi(G)$. Then there exists $g \in G$ such that $h = \phi(g)$. Hence $\alpha(gN) = \phi(g) = h$. So the map is onto (by construction).

Thus $\alpha$ is an isomorphism $\Box$

For a positive integer $n$, we have seen that $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$ is a homomorphism. ELFY: Show it is onto (and so an epimorphism).

$SL_n(\mathbb{R}) = \ker(\det)$ so by the first isomorphism theorem, $GL_n/SL_n \cong \mathbb{R}^+$.

Proposition 8.5 (Second Isomorphism Theorem): Let $G$ be a group with $H \leq G$ and $K \leq G$. Then $K \trianglelefteq HK$, $H \cap K \trianglelefteq H$ and $HK/K \cong H/(H \cap K)$ where $HK = \{hk | h \in H, k \in K\}$.

Proof: ELFY: Show $HK$ is a group and $K \leq HK$.

$K$ is normal in $HK$ because for all $g \in HK$ and $k \in K$ we have $gkg^{-1} \in K$ as $g \in G$ and $K \trianglelefteq G$.

ELFY: Show $H \cap K \leq H$.

$H \cap K$ is normal in $H$ because for all $h \in H$ and $k \in H \cap K$ we have $hhk^{-1} \in H \cap K$ since $hkh^{-1} \in K$ as $h \in G$ and $K \trianglelefteq G$ and since $hhk^{-1} \in H$ as $h, k \in H$.

Now we know that $HK/K$ and $H/(H \cap K)$ are groups. Define $\phi : H \to HK/K$ by the rule $\phi(h) = hK$ (which is an element of $HK/K$ because $h \in HK$).

For all $h, h' \in H$ we have $\phi(hh') = hh'K = (hK)(h'K) = \phi(h)\phi(h')$. So $\phi$ is a homomorphism. Let $x \in HK$. Then $x = hk$ where $h \in H$ and $k \in K$. Then $h^{-1}xK = K$ since $h^{-1}x = k \in K$. Hence $xK = hK$. Therefore $\phi(h) = hK = xK$ which shows that $\phi$ is onto, that is, $\phi(H) = HK/K$. 
Finally by applying the first isomorphism theorem we get that $H/\text{Ker}(\phi) \cong HK/K$. We finish the proof by calculating the kernel. $\text{Ker}(\phi) = \{h \in H|\phi(h) = K\} = \{h \in H|hK = K\} = \{h \in H|h \in K\} = H \cap K$ as required  

**Proposition 8.6 (Third Isomorphism Theorem):** Let $G$ be a group with $N \trianglelefteq K \trianglelefteq G$ and $N \trianglelefteq G$. Then $K/N \trianglelefteq G/N$ and $(G/N)/(K/N) \cong G/K$.

**Proof:** $K/N \leq G/N$ as $K/N$ is a group and is clearly contained in $G/N$. Let $g \in G$ and $k \in K$. Then $(gN)(kN)(gN)^{-1} = [(gk)N][g^{-1}N] = (gkg^{-1})N \in K/N$ since $gkg^{-1} \in K$ as $K$ is normal in $G$. So $K/N$ is normal in $G/N$.

Define $\phi : (G/N) \to G/K$ by the rule $\phi(gN) = gK$. $\phi$ is well-defined as if $gN = g'N$ then $g^{-1}g' \in N$ and $N$ is in $K$ (as a subgroup) so $gK = g'K$.

Let $g, g' \in G$. $\phi((gN)(g'N)) = \phi((gg')N) = (gg')K = (gK)(g'K) = \phi(gN)\phi(g'N)$ so $\phi$ is a homomorphism.

The map is (obviously) onto because for all $gK \in G/K$ we have $\phi(gN) = gK$.

So by the first isomorphism theorem, we get $(G/N)/\text{Ker}(\phi) \cong G/K$.

So we finish by calculating the kernel. $\text{Ker}(\phi) = \{gN \in G/N|\phi(gN) = K\} =$

$= \{gN \in G/N|gK = K\} = \{gN \in G/N|g \in K\} = K/N$ as required  

One might think that because of Lagrange’s Theorem, for any group $G$ of order $n$ and any divisor $d$ of $n$ there is a subgroup of $G$ of order $d$. This isn’t true. Let’s explore a counterexample.

Let $G = A_4$, which is order 12. Let’s show that there is no subgroup of $A_4$ of order 6.

To yield a contradiction, assume there is a subgroup $N$ of order 6 in $A_4$. Then since $[A_4 : N] = 2$ we have that $N$ must be a normal subgroup. Then $A_4/N = \{N, \sigma N\}$ where $\sigma \in A_4 \setminus N$. Then $A_4/N = \langle \sigma N \rangle$ and $(\sigma N)^2 = \sigma^2 N = N$.

In particular, for any $\tau \in A_4$ we have that $\tau \in N$ or $\tau \in \sigma N$. If $\tau \in N$ then $\tau^2 \in N$ as $N$ is a subgroup. If $\tau \in \sigma N$ we have that $\tau N = \sigma N$ and hence $(\tau N)^2 = \tau^2 N = N$. So in either case, $\tau^2 \in N$.

$A_4$ contains all cycles of length three in $S_4$ because $(i \ j \ k) = (i \ j)(i \ k)$. Let $c \in A_4$ be a cycle of length three. Then $c = (Id)c = c^3c = (c^3)^2 \in N$. So every cycle of length 3 in $A_4$ is in $N$. There are $8 = (4)(2)$ cycles of length three (4 choices for which 3 elements $i, j$, and $k$ of the elements 1, 2, 3, and 4 are involved, and 2 cycles that can be made from those three elements, $(i \ j \ k)$ and $(i \ k \ j)$).

Hence $|N| > 8$ which is a contradiction. So no such group $N$ exists, meaning that $A_4$ is a group of order 12 with no subgroup of order 6.
We state an important definition and an associated theorem, but we skip the proof to save time.

A group $G$ is simple if it is non-trivial (not of order 1) and if the only proper normal subgroup is the trivial subgroup $\{e\}$.

**Proposition 8.7:** $A_n$ is simple for all $n \geq 5$. 