Definition 1. The *order* of a group element x, denoted by $|x|$, is the size of its orbit $\langle x \rangle$. Note: If the size of $\langle x \rangle$ is finite, then the order of x is the smallest positive integer k such that $x^k = e$.
The *order* of a group G, denoted by $|G|$, is the number of elements in G.

Remark 2. Let J be a subset of a group G. To show that J is a subgroup of G, show the following:

(a) J contains the identity of G

(b) for all $x, y \in J$, the product xy is also in J (closure under the group operation)

(c) for all $x \in J$, the inverse x^{-1} is also in J (closure under taking inverses)

Theorem 3. If a permutation σ can be expressed as the product of an even number of transpositions, then any other product of transpositions equaling σ must also contain an even number of transpositions. Similarly, if σ can be expressed as the product of an odd number of transpositions, then any other product of transpositions equaling σ must also contain an odd number of transpositions.

Proposition 4. For any $\sigma \in S_n$, we have $\sigma\ (a_1\ a_2\ \ldots\ a_k)\ \sigma^{-1} = (\,\sigma(a_1)\ \sigma(a_2)\ \ldots\ \sigma(a_k)\,)$.

Definition 5. Let $H \leq G$. If $x \in G$, the set $xH := \{xh \mid h \in H\}$ is a *left coset* of H.

Lemma 6. Let H be a subgroup of G and let that $a, b \in G$. The following conditions are equivalent.

(1) $aH = bH$

(2) $b \in aH$

(3) $b\ a^{-1} \in H$

Theorem 7 (Lagrange's Theorem)**.** If G is a finite group and $H \leq G$, then $[G : H] = \frac{|G|}{|H|}$. In particular, $|H|$ divides $|G|$.

Theorem 8. Let H be a subgroup of G. Then the following are all equivalent.

(1) $gH = Hg$ for all $g \in G$ (that is, H is normal in G) ("left cosets are right cosets")

(2) $ghg^{-1} \in H$ for all $h \in H, g \in G$ ("closed under conjugation")

(3) $gHg^{-1} = H$ for all $g \in G$ ("only one conjugate subgroup")

Definition 9. Let $H \leq G$. The set $G/H = \{xH : x \in G\}$ is the set of all left cosets of H in G.
If $H \trianglelefteq G$, then G/H forms a group (called the *quotient group of G by H*) under coset multiplication $(xH)(yH) = (xy)H$.

Definition 10. A group *homomorphism* is a function $\phi\colon (G_1, *) \to (G_2, \circ)$ satisfying

$$\phi(a * b) = \phi(a) \circ \phi(b), \qquad \text{for all } a, b \in G_1\,.$$

Proposition 11. Let $f : G_1 \to G_2$ be a homomorphism of groups. Then

i. If e_1 is the identity of G_1, then $f(e_1)$ is the identity of G_2.

ii. For any element $g \in G_1$, $f(g^{-1}) = [f(g)]^{-1}$.

iii. If H_1 is a subgroup of G_1, then $f(H_1)$ is a subgroup of G_2.

iv. If H_2 is a subgroup of G_2, then $f^{-1}(H_2) = \{g \in G_1 : f(g) \in H_2\}$ is a subgroup of G_1.

Definition 12. A group G is said to *act* on a set X if there is a homomorphism $\phi : G \to \mathrm{Perm}(X)$.

Definition 13 (Ideal test)**.** A subset I of a ring R is called an *ideal* of R if it satisfies the following properties:

- I is an additive subgroup of R
- I "absorbs" all elements of R, that is, for all $a \in I$ and $r \in R$, we have $ar \in I$ and $ra \in I$.

Theorem 14. Let R be a commutative ring with unity and M an ideal in R. Then M is a maximal ideal of R if and only if the quotient ring R/M is a field.

Theorem 15. Let R be a commutative ring with unity and P an ideal in R. Then P is a prime ideal of R if and only if the quotient ring R/P is an integral domain.