Definition of Groups

Binary Operation	Let G be a set. A binary operation on G is a function that assigns each ordered pair of elements of G an element of G.
Group	Let G be a set together with a binary operation (usually called multiplication) that assigns to each ordered pair (a, b) of elements of G an element in G denoted by ab. We say G is a group under this operation if the following three properties are satisfied.
Properties to Satisfy (Group)	1. Closure 2. Associativity 3. Identity 4. Inverses
Abelian group	If a group has the property that ab = ba for every pair of elements a and b, we say the group is Abelian.
Associativity	The operation is associative; that is, (ab)c = a(bc) for all a, b, c in G.

Definition of Groups (cont)

Identity	There is an element e (called the identity) in G such that ae = ea = a for all a in G.
Inverses	For each element a in G, there is an element b in G (called an inverse of a) such that ab = ba = e.
Modular Arithmetic	When a = qn + r, where q is the quotient and r is the remainder upon dividing a by n, we write a mod n = r.

Elementary Properties of Groups

Theorem 2.1 Uniqueness of the Identity	In a group G, there is only one identity element.
Theorem 2.2 Cancellation	In a group G, the right and left cancellation laws hold; that is, ba = ca implies b = c, and ab = ac implies b = c.
Theorem 2.3 Uniqueness of Inverses	For each element a in a group G, there is a unique element b in G such that ab = ba = e.
Theorem 2.4 Socks--Shoes Property	For group elements a and b, $(ab)^{-1} = b^{-1}a^{-1}$.

Subgroup Tests

One-Step Subgroup Test	Let G be a group and H a nonempty subset of G. If ab^{-1} is in H whenever a and b are in H, then H is a subgroup of G. (In additive notation, if a - b is in H whenever a and b are in H, then H is a subgroup of G.)
Two-Step Subgroup Test	Let G be a group and let H be a nonempty subset of G. If ab is in H whenever a and b are in H (H is closed under the operation), and a^{-1} is in H whenever a is in H (H is closed under taking inverses), then H is a subgroup of G.
Theorem 3.3 Finite Subgroup Test	Let H be a nonempty finite subset of a group G. If H is closed under the operation of G, then H is a subgroup of G.

Examples of Subgroups

Theorem 3.4 <a> Is a Subgroup	Let G be a group, and let a be any element of G. Then, <a> is a subgroup of G.
Center of a Group	The center, Z(G), of a group G is the subset of elements in G that commute with every element of G. In symbols, **Z(G) = {a ∈ G | ax = xa for all x in G}**.
Theorem 3.5 Center Is a Subgroup	The center of a group G is a subgroup of G.
Centralizer of a in G	Let a be a fixed element of a group G. The centralizer of a in G, C(a), is the set of all elements in G that commute with a. In symbols, **C(a) = {g ∈ G | ga = ag}**.
Theorem 3.6 C(a) Is a Subgroup	For each a in a group G, the centralizer of a is a subgroup of G.

Terminology and Notation

Order of a Group	The number of elements of a group (finite or infinite) is called its order. We will use |G| to denote the order of G.

Terminology and Notation (cont)

Order of an Element	The order of an element g in a group G is the smallest positive integer n such that $g^n = e$. (In additive notation, this would be ng = 0.) If no such integer exists, we say that g has infinite order. The order of an element g is denoted by |g|.
Subgroup	If a subset H of a group G is itself a group under the operation of G, we say that H is a subgroup of G.