Group Theory, Gun and Camera in Hand

Historical Note. Group theory originates with Galois' 1832 generalizations over algebraic structures. Lagarange (in Paris) and Klein (in Bonn) represent the two main historical roots of modern group theory.

Klein's work stemmed from Plüker's 1865 "New Geometry of Space," wherein it's argued that a geometrical space need not be conceived as a plenum of points, but lines. This shows, on Plüker's view, that ordinary 3-space, if conceived as a cosmic agglomeration of infinitely small birdshot, is equivalent to a 4-space conceived as "a cosmic haystack of infinitely thin, infinitely long straight straws." Klein used the contact transformations developed by Lie to establish the requisite 1-1 correspondences.

Lagrange's work stemmed from problems in algebra concerning the approximation of roots of polynomial equations. Lagrange considered the solvability of equations via permutations of their roots, and from this work formulated what is now regarded as the **fundamental theorem** of modern group theory: if o is the order of a subgroup g of group G of order O, then o is a factor of O.

Informal Definition: A set, S, of elements forms a group with respect to a given operation O, if
(1) S is closed under O,
(2) S contains an identity element with respect to O,
(3) for every element there is an inverse element with respect to O, and
(4) O is associative.

Elements can be numbers (arithmetic), points (geometry), transformations (algebra), or anything at all; group theory is fully general. Klein used it to unify geometry, which becomes the study of those properties of figures that remain invariant under a particular group of transformations, like rotation in the plane.

Apparatus. Nowadays, group theory is investigated via axiomatic methods. The apparatus includes:

Definition: Let (G, o) be an algebraic structure such that

(1) G is closed under o,

(2) o is associative in G,
(3) there exists an element $z \in G$ such that $z \, o \, a = a \, o \, z = a$ for all $a \in G$, and
(4) for each element $a \in G$, there exists an element $a^* \in G$, such that
$a \, o \, a^* = a^* \, o \, a = z$,
Then (G,o) is a **group**, z is the **identity** element and a^* is is the **inverse** of a.

Definition: If (G,o) is a group and o is commutative in G, then (G,o) is an **Abelian group**.

Theorem 1: *A group has only one identity element.*

Proof: Let (G,o) be a group, and assume z and z' are two identity elements in G. By definition of identity, $z \, o \, z' = z$, and also $z \, o \, z' = z'$, implying $z = z'$. QED.

Definition: Let (G,o) be a group. If $S = G$ such that (S,o) is a group, then (S,o) is a **subgroup** of (G,o).