Some Definitions Useful for Group Theory

1. A group G is a set together with a map $\varphi: G \times G \to G$ such that for all $a, b, c \in G$

a.) $\varphi(a,b) \in G$, {closure},

b.) $\varphi[\varphi(a,b),c] = \varphi[a,\varphi(b,c)]$, {associativity},

c.) $\exists!\, e \in G$ such that $\varphi(e,a) = a = \varphi(a,e)$, {identity},

d.) $\forall a \in G, \exists!\, a^{-1} \in G$ such that $\varphi(a,a^{-1}) = e = \varphi(a^{-1},a)$, {inverse}.

1a. A group is said to be *Abelian* when the product is commutative.

1b. The group mapping is usually indicated simply by the use of juxtaposition of the two elements in question, occasionally by the use of $\circ$, or with $+$ when it is an Abelian group.

2. A *homomorphism* of two groups is a mapping $f : G_1 \to G_2$, which preserves the product, i.e., $f(g)f(h) = f(g \circ h)$, where we have indicated the product in G_1 with $\circ$ and the product in G_2 with simple juxtaposition, to underscore the fact that the two products are different.

2a. An *isomorphism* of two groups is a homomorphism that is one-to-one.

3. A nonempty subset $H \subset G$ is a subgroup of the group G provided H is closed under multiplication, i.e., under the product inherited from G.

3a. We use the notation Hr to denote the set $\{h \circ r \mid h \in H\}$.

3b. It is reasonable to write the requirement for a subset in the form $H^2 \subset H$, where the notation H^2 is meant to imply $\{h \circ m \mid h, m \in H\}$.

3c. If H is a subgroup of G and $r, s \in G$, then either $Hr = Hs$ or Hr and Hs are disjoint. The former happens when $rs^{-1} \in H$.

3d. If H is a subgroup of G and $p \in G$, then H and $pHp^{-1} \equiv \{p \circ h \circ p^{-1} \mid h \in H\}$ are isomorphic subgroups, although not necessarily distinct.

4. If H is a subgroup of G, then, from among all the sets $\{Hg \mid g \in G\}$ one picks all those that are distinct; the resulting set is called the set of *right cosets* of G relative to H. Similarly one can have a set of *left cosets*.

5. Two elements, $a, b \in G$ are called *conjugate* if and only if $\exists p \in G$ such that $a = pbp^{-1}$.

We use the notation $a \sim b$.

5a. Conjugacy is an equivalence relation,

i.e., it is	*reflexive,*	*symmetrical,*	*transitive*
	$a \sim a$,	$a \sim b \Leftrightarrow b \sim a$,	$a \sim b$ and $b \sim c \ \Rightarrow \ a \sim c$,

6. The order of $a \in G$ is the smallest integer such that $a^n = e$. For a finite group it is obvious that n exists; for infinite groups not every element need have finite order.

When a group is finite, with p elements, then the following are some useful theorems:

6a.) p/n is an integer for every $a \in G$,

6b.) a and pap^{-1} have the same order, for all $p \in G$.

6c.) the only element of order 1 is the identity, e,

6d.) a and a^{-1} have the same order,

6e.) the order of a^m, for any integer m, cannot exceed the order of a.

7. The *class* of $a \in G$ is $\{pap^{-1} \mid p \in G\}$, i.e., the set of all elements conjugate to a.

8. The *normalizer* of $a \in G$ is $\{p \mid pa = ap\}$; it is a subgroup of G.

8a. The normalizer of a subgroup is the set of all the (distinct) normalizers of its elements.

9. An *invariant*, or *normal*, or *self-conjugate* subgroup, H, of G, is one such that the sets of its left- and right-cosets are equal, i.e., $\forall p \in G$, $Hp = pH$, or $pHp^{-1} = H$, $\forall p \in G$. In this case, the set of cosets forms a group, denoted by G/H; it is called the *quotient group*.

10. A *simple group* is one which possesses no proper invariant subgroup.

10a. A semisimple group is one which possesses no proper, invariant, Abelian subgroup.

11. Let a group G be acting as transformations on a space S, with the action (or transformation) denoted by $g(s) \in S$, for any $g \in G$.

11a. For $s \in S$, the *orbit* of s under G is the subspace of S defined by $\{t = g(s) \mid g \in G\}$.

11b. For $s \in S$, the subset of G defined as $\{g \mid g(s) = s\}$ is a subgroup, called the *isotropy subgroup* of $s \in S$, or, ofttimes in physics, the *"little" group* of G for $s \in S$

11c. If S consists of a single orbit, i.e., if all points in S can be obtained by the action of some element of G on some fixed initial point, then we say that G *acts transitively on* S.

11d. If S is a vector space, and the action preserves the group multiplication as well as the linearity of the vector space, then we say that S is a *G-module*.