GROUP THEORY

JOSEPH BALSELLS

1. Axioms

A group is a set with a special algebraic structure satisfying the group axioms:

Axiom 1 A multiplication law exists.

$$a, b \in G \implies a \cdot b = c \in G$$

i.e. the group is *closed* under composition.

Axiom 2 The associative law holds.

$$(ab)c = a(bc)$$

Axiom 3 The group contains and identity element (usually denoted e)

$$ae = a$$

Axiom 4 The inverse of any element is also contained within the group.

$$\exists a^{-1} \in G \text{ s.t. } aa^{-1} = e$$

You may find yourself wondering,"Why are *these* the axioms, why not more, why not less, why not different ones?" The most satisfying answer is that these are the axioms which lead to the most interesting theory. Any of these axioms could be done without, just that we would not have group theory, we would have something different. For example, by revoking the requirement for each element to have an inverse we are left with what are called *monoids*. Note that the commutative law need not hold in general. Groups which do obey commutativity among all its elements are called *abelian*.

From these axioms a number of theorems are immediate. From Axiom 2 we can prove that parenthesis are not required for any number of products so long as the order is unchanged. From Axiom 3 we can prove that the identity element is unique.

The **Multiplication / Cayley Table** contains all possible products and fully describes the group. Note: the entries are pq where p is the row and q is the column (so the column entry acts first, then the row entry).

A **Cyclic Group** is a group generated by a single element. For example,

$$< i >= \{1, i, -1, -i\}$$

This group is abelian and isomorphic to the integers mod 4 under addition.

2. Subgroups

Let G be a group and H a subset of G. Then H is called a *subgroup* of G if H is a group. Note that this is satisfied if for each $h \in H$ also $h^{-1} \in H$. The following theorem gives and equivalent test.

Theorem 1 *A non-empty subset H of a group G is a subgroup of G if, and only if, with each pair of elements $h, h' \in H$, also $h^{-1}h' \in H$.*

Proof. □

Alternatively, H is a subgroup of G if $h(h')^{-1} \in H$, i.e., A subset of G which is closed under "division" is a subgroup of G.

Theorem 2 *Let S be an arbitrary subset of a group G. Let $C(S)$ be the set of all elements of G which commute with all the elements of S. Then $C(S)$ is a subgroup of G.*

$C(S)$ is called the **centralizer of** S. If $S = G$ then $C(G)$ is called the **center of the group** G. For abelian groups $C(S), C(s)$, and $C(G)$ are always G itself.

Theorem 3 (Lagrange) *The order of any subgroup of G divides the order of G.*

The proof follows after Euler using cosets. Let H be a proper subgroup of G. Then there exists $a \notin H$ and we form the **left coset**

$$aH = \{ah_t \mid h_t \in H \text{ and } a \notin H\}$$

Note that the coset aH is *never* a group since it never contains the identity. In a similar way we can define the **right coset** of H as

$$Ha = \{h_t a \mid h_t \in H \text{ and } a \notin H\}$$

We first prove that the coset aH is independent of the representative a. That is, if aH and bH are two cosets that have one element in common, then they are *identical*. Thus if follows that the division of a group into cosets is a division of the group into disjoint sets of group elements. The number of distinct cosets, including H itself, is called the **index of** H **in** G and is denoted $|G : H|$. Intuitively the index gives the number of "copies" (cosets) of H that fill up G.

Stated in this language, Lagrange's theorem states

$$|G : H| = \frac{|G|}{|H|}$$