GROUP THEORY

JOSEPH BALSELLS

These notes derive from Jansen and Boon's *Theory of Finite Groups: Applications in Physics*, 1967.

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 an 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.

The normalizer of S in a group G is defined as

$$N_G(S) = \{g \in G | gS = Sg\}$$

Note that this is a weaker requirement than for g to be in the centralizer. Both are subgroups of G

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. The coset aH is independent of the representative a (proof). 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. Moreover all of the cosets have the same number of elements as H. The number of distinct cosets, including H itself, is called the **index of H in G** and is denoted $|G\!:\!H|$. [1]

Stated in this language, Lagrange's theorem states

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

Lagrange's theorem is useful for finding proper subgroups of a group. The division of G into cosets of H, including H itself, is called the *coset decomposition of G with respect to H.*

3. Mappings of Groups

A mapping between two groups which preserves the group structure is called a **group homomorphism** or, simply, a **homomorphism**. An isomorphic mapping between a group and itself is called **automorphic**, or an **automorphism**.

Theorem 4 *If $f : G \to G'$ is a group homomorphism, then the image $f(G)$ of G is always a subgroup of G' with unit element $f(e)$, where e is the unit element of G.*

Let $f : G \to G'$ be a homomorphism, and let e' be the unit element of the group G'. Then the collection of all elements of G which have e' as their image is called the **kernel** of the homomorphic mapping $f : G \to G'$. In other words: the kernel is the fiber $f^{-1}(e')$, of the unit element e' of G'.

Theorem 5 *The kernel of a homomorphic mapping $f : G \to G'$ is a subgroup of G.*

Theorem 6 *All fibers of the homomorphic mapping $f : G \to G'$ contain the same (finite or infinite) number of elements of G.*

A subgroup $H < G$ is **normal (invariant)** iff $gH = Hg$ i.e., the left and right cosets coincide. The kernel of a homomorphism is a normal subgroup.

[1] Intuitively, the index gives the number of "copies" (cosets) of H that fill up G.

4. Decomposition of a Group into Classes

An equivalence relation is an extension of equality. We say two elements are **equivalent** if $x \sim y$. The equivalence property obeys

$$\begin{aligned} (i) &\quad x \sim x \\ (ii) &\quad \text{if } x \sim y, \text{ then } y \sim x \\ (iii) &\quad \text{if } x \sim y, \text{ and } y \sim z, \text{ then } x \sim z \end{aligned}$$

Elements belonging to the same coset are equivalent.

Conjugate elements of a group G are equivalent. Two elements, g, g', are conjugate if

$$g' = s^{-1} g s \quad \text{for some} \quad s \in G$$

Any group G can be partitioned into conjugation classes of group elements.

$$G = \sum \text{ classes with no elements in common}$$

The unit element, e, of G is always in a class by itself. Hence none of the other classes can be subgroups of G. Likewise every element of the center of G, $C(G)$, is in a class by itself.

Theorem 7 *All the elements of one class are of the same order*

In the symmetric groups, elements with the same **disjoint cycle structure** belong to the same class.

Theorem 8 *The number of elements in any class of a group G is a divisor of the order of G*

5. Conjugate Subgroups and Factor Groups

Any subgroup of index 2 is normal (we have H with index 2 and the only other coset is either aH or Ha so these have to be equal). If a group does not contain any proper normal subgroups then it is called **simple**. Otherwise it is **composite**.

Theorem 9 *A subgroup H of a group is normal if, and only if, with every element $h \in H$ also the complete class $C_h \subset H$.*

All elements of an abelian group are in their own class so any subgroup of an abelian group is normal.

The center of a group is thus normal.

The kernel of a homomorphism is a normal subgroup. (Prove converse, that any normal subgroup can be the kernel of a homomorphism).

The cosets of a normal subgroup define another group called the **factor group**. Let N be a normal subgroup of G and aN and bN distinct left cosets. Then $(aN)(bN) = abN$ is the natural multiplication. we call the cosets elements of the **quotient group** or **factor group** $Q = G/N$.

The order of a factor group is the same as the index of the normal subgroup.

The **Natural mapping** $f : G \to G/N$ is a homomorphism. N is the kernel of this homomorphism.

Theorem 10 (Isomorphism theorem) *The factor group G/N is isomorphic to the homomorphic image $f(G)$ of G where N serves as the kernel of this homomorphism.*

6. Product Groups

A group G is called the **product** of two of its subgroups, and written $G = HK$, if each element $g \in G$ can be written as $g = hk$, with $h \in H$ and $k \in K$. If the set HK is identical to the set KH, then we say that H and K commute.

Example: The Klein four-group, V_4

Note: in general the product of two subgroups, HK, is *not* a group. For abelian groups it is always true that HK is a subgroup, in which case it is called the **sum** of H and K.

For an arbitrary group G, the following condition is necessary and sufficient:

Theorem 11 *If H and K are two subgroups of G, then the product HK is again a subgroup of G if, and only if, H and K commute: $HK = KH$.*

If either H or K is normal, then $HK = KH$ is a subgroup. If both are normal, then HK is normal.

A group G is called a **direct product** of its subgroups H and K and written $G = H \times K$, if the following conditions are fulfilled:

Abstract (external) direct product. Product of different groups. The previous direct product was representing a group as a direct product of its subgroups. Whereas this inherited the composition law of the group, abstract direct products do not inherit any composition law.

Semi-direct product

Alternating group

Appendix A. Classification of groups by order

A.1. **Order 1.**

- The unit element: $\{e\}$

A.2. **Order 2.**

- Z_2

A.3. **Order 3.**

- Z_3
- S_3

A.4. **Order 4.**

- Z_4
- V_4