Group Theory, Part I: Definitions and Basics

Jay Havaldar

A **group** is a set together with a binary operation (multiplication) so that:

- Multiplication is associative.
- There is an identity e so that $eg = ge = g$.
- For each g there is an inverse g^{-1} so that $gg^{-1} = g^{-1}g = e$.
- The group is closed under multiplication.

The **order** of an element a is the minimum integer n so that $a^n = e$. The subgroup consisting of all elements of the group of finite order is called the **torsion subgroup**.

Example An important example of a group is the dihedral group D_n. It is generated by two kinds of elements: rotations, and reflections. It describes the symmetries of an n-gon with composition. The two kinds of elements are respectively described as:

$$r^n = es^2 = esrs = r^{-1}$$

D_1 is for example defined as
$1, r$ so it is simply $\mathbb{Z}/2\mathbb{Z}$. On the other hand, $D_2 =$
$1, r, s, rs$ is not cyclic; it is called the **Klein** group or the 4-group, which is distinct from $\mathbb{Z}/4\mathbb{Z}$.

0.1 The General Linear Group

An important group is the general group $GL(V)$. For an n-dimensional vector space V over a field, we can think of $GL(V)$ as the set of $n \times n$ matrices over a field with nonzero determinant -- with multiplication defined in the usual way (once we fix a basis).

A **bilinear form** $\phi : V \times V \to F$ that is linear in each variable. An **automorphism** of ϕ is is an isomorphism $\alpha : V \to V$ so that:

$$\phi(\alpha v, \alpha w) = \phi(v, w)$$

With a choice of a basis, we can restate this condition in terms of the matrix for α and the matrix P for ϕ:

$$(Av)^T \cdot PAw = v^T Pw$$
$$v^T A^T PAw = v^T Pw$$

So:

$$A^T PA = P$$

In particular, if ϕ is **symmetric**, i.e.:

$$\phi(v, w) = \phi(w, v)$$

Then we have the following definition.

Definition: For a symmetric non-degenerate bilinear form ϕ, define its automorphism group $Aut(\phi)$ to be the isomorphisms α so that $\phi(\alpha v, \alpha w) = \phi(v, w)$. This is called the **orthogonal group** of ϕ.

Definition: For a skew-symmetric non-degenerate bilinear form ϕ, define its automorphism group $Aut(\phi)$ to be the isomorphisms α so that $\phi(\alpha v, \alpha w) = \phi(v, w)$. This is called the **symplectic group** of ϕ.

In this case, we can write ϕ in some basis as the matrix:

$$J_{2m} = \begin{bmatrix} 0 & I_m \\ -I_m & 0 \end{bmatrix}$$

Where $2m = n$. Therefore, the symplectic group condition simply means a matrix has the property:

$$A^T J_{2m} A = J_{2m}$$

0.2 Subgroups

A subgroup is a subset of a group which is closed under multiplication and inverses, and which contains the identity. A particularly important is called the center of a group.

Definition: The **center** of a group G, denoted $Z(G)$ consists of all the elements which commute with all of G, i.e.:

$$Z(G) = \{z \in G \ : \ zx = xz \ \forall x \in G\}$$

Proposition

An intersection of subgroups is a subgroup.

The proof here is fairly straightforward.

We can talk about the **cosets** of a subgroup H as elements of the form aH for some $a \in G$, where:

$$aH = \{ah \ : \ h \in H\}$$

Cosets are well-defined, and are either disjoint or equal. Suppose that $a\ inbH$, then we can say for some $h \in H$:

$$a = bhaH = bhH = bH$$

So that means we can write a coset as aH for any choice of representative a. By the above argument, if two cosets share a single element, they are the same set. Finally, we can map aH

to bH via multiplication by ba^{-1} (and conversely, map from bH to aH via multiplication by ab^{-1}). Thus, all the cosets are the same size.

Definition: The **index** of a subgroup H of G is the number of left cosets of H in G, and is denoted $(G : H)$.

Proposition (Lagrange's Theorem)

The order of a subgroup divides the order of the group.

We have:

$$|G| = (G : H)|H|$$

Therefore, $|H|$ divides $|G|$.

As a corollary, we consider the group generated by a certain element a. It has size n, where n is the order of a, and forms a subgroup. Thus, the order of any element in a group divides the order of the group.

We also have the following ``cancellation'' theorem. If H is a subgroup of G and K is a subgroup of H, we have:

$$(G : K) = (G : H)(H : K)$$

0.3 Homomorphisms

Definition: A **homomorphism** between groups G, G' is a map $\varphi : G \to G'$ so that $\varphi(ab) = \varphi(a)\varphi(b)$. In a sense, a homomorphism preserves the structure of the group. If a homomorphism is bijective, we say that it is an **isomorphism**.

0.3.1 Cayley's Theorem

An important theorem is Cayley's Theorem, which says we can think of each group as a subgroup of a permutation group. For $a \in G$, define the map:

$$\phi_a : G \to G\phi_a(b) = ab$$

Thus, the map ϕ_a is just multiplication by A. We can also show that it is a bijection, since we have:

$$\phi_a \circ \phi_{a^{-1}}(b) = \phi_a(a^{-1}b) = aa^{-1}b = b$$

And in fact we can say that: - Each ϕ_a is a bijection from G to G, hence $\phi_a \in S_{\|G\|}$, the symmetric group or group of permutations of G. - The map $\Phi : a \mapsto \phi_a$ is an injective map from G to $S_{\|G\|}$.

So this brings us to Cayley's Theorem:

Any finite group is a subgroup of a symmetric group.

0.4 Normal Subgroups

Definition: A subgroup N of a group G is normal if $gNg^{-1} = N$ for all $g \in G$. A normal subgroup is denoted $N \trianglelefteq G$.

It is sufficient to check that $gNg^{-1} \subset N$ for each g, since multiplying gives us $Ng^{-1} = g^{-1}N \implies N \subseteq g^{-1}Ng$, and substituting $g = g^{-1}$ we get the reverse inclusion.

Note however, that we can find a subgroup N and an element g so that $gNg^{-1} \subset N$ with strict inequality; however, if this holds for all g, then we indeed have a normal subgroup.

Proposition

Every subgroup of index two is normal.

Suppose H is a subgroup of index two. Pick $g \in G$ which is not in H. then gH is the complement of H. Similarly, Hg is the complement of H. So we have $gH = Hg$. Then $gHg^{-1} = H$.

Definition: A group is **simple** if it has no normal subgroups other than itself and the trivial subgroup.

Proposition

Suppose H, N are subgroups of G and N is a normal subgroup. Then $HN = \{hn : h \in H, n \in N\}$ is a subgroup of G. If H is also a normal subgroup, then HN is a normal subgroup of G.

Note that $gNg^{-1} = N$, so that we can write $gN = Ng$. For any $n \in N$, we can write $gn = n'g$ where $n' \in N$.

Taking $h_1n_1, h_2n_2 \in HN$, we have:

$$(h_1n_1)(h_2n_2) = h_1h_2n_1'n_2 \in HN$$

So indeed HN is closed under multiplication. It contains the identity automatically, and we can check inverses:

$$(hn)^{-1} = n^{-1}h^{-1} = h^{-1}n'^{-1} \in HN$$

So indeed HN is a subgroup.

If H, N are both normal, we can write:

$$gHNg^{-1} = gHg^{-1}gNg^{-1} = HN$$

And we are done. We can also define the normal subgroup generated by any set in G.

Definition: For any set $X \subset G$, the smallest normal subgroup generated by X is exactly:

$$\bigcup_{g \in G} gXg^{-1}$$

Theorem

> A subgroup N of G is normal iff it is the kernel of some homomorphism.

Evidently, the kernel of a homomorphism is a normal subgroup since for any $x \in \ker \varphi$:

$$\varphi(gxg^{-1}) = \varphi(g)e\varphi(g)^{-1} = e$$

Conversely, we map $g \mapsto gN$, i.e. map to cosets. We just need to show that G/N has a group structure which is preserved by this map. Define $(aN)(bN) = (ab)N$. We need to show that this multiplication is well defined.

Suppose that $aN = a'N$ and $bN = b'N$. Then we can show:

$$abN = a(bN) = ab'N = aNb' = a'Nb' = a'b'N$$

Where we use freely here that $aN = Na$ by the fact that N is a normal subgroup. So indeed this map is well defined, and preserves the group structure, and its kernel is evidently N. We call G/N the **quotient** of G by N.

0.5 The Isomorphism Theorems

As per usual, we have the isomorphism theorems.

First Isomorphism Theorem

> Let $\varphi : G \to G'$ be a homomorphism of groups. Then:
>
> $$\frac{G}{\ker \varphi} \cong \varphi(G)$$

And since $\ker \varphi$ is a normal subgroup by the above discussion, we have that $\varphi(G)$ is a subgroup of G'.

Second Isomorphism Theorem

> Let S be a subgroup of G, and N a normal subgroup of G. Then: - SN is a subgroup of G. - $S \cap N$ is a normal subgroup of S. - $\frac{SN}{N} \cong \frac{S}{S\cap N}$.

Third Isomorphism Theorem

> Suppose K, N are normal subgroups of G with $N \subseteq K \subseteq G$. Then:
>
> $$\frac{G/N}{K/N} \cong \frac{G}{K}$$

Furthermore, we have the following correspondences from the third isomorphism theorem:

“Fourth” Isomorphism Theorem

Suppose N is a normal subgroup of G. Then there is a correspondence between subgroups K of G which contain N and subgroups of G/N, given by:

$$K \leftrightarrow kN$$

Where $k \in K$ is a representative. Similarly, the same bijection gives a correspondence between normal subgroups K of G which contain N and normal subgroups of G/N.