Group Theory

Karan Elangovan

April 28, 2021

Contents

1 Groups

1.1 Group Axioms

Definition 1 (Group)**.** A group is an ordered pair $(G, \circ)$, where $\circ : G^2 \to G$ satisfying

1. (Associativity) The $\circ$ operation is associative.
2. (Identity) There exists an element $1 \in G$ such that $1 \circ x = x \circ 1 = x$ for all $x \in G$.
3. (Inverses) For every element x there exists an element x^{-1} such that $x \circ x^{-1} = x^{-1} \circ x = 1$.

From here on we will omit the $\circ$ symbol and just denote it by adjacency, and when the group operation is clear from context, we will refer to a group by its set.

Definition 2 (Subgroup)**.** Given a subset $H \subset G$, we say it forms a subgroup if H is a group under the induced group operation from G.

1.2 Cosets

Given subsets $A, B \subset G$, we may define their product as

$$AB = \{ab : a \in A, b \in B\}.$$

That is, the set of all possible products of elements from A and B. We see that from the associativity of element multiplication that multiplication of subsets is also associative.

In the case that A or B is a singleton, we just write xB and Ax for $\{x\}B$ and $A\{x\}$ respectively. The case that one of A, B is a subgroup and the other a singleton is of particular interest, leading us to the following definition:

Definition 3 (Cosets)**.** Let H be a subgroup of G. Then the left cosets of H in G, G/H are the subsets of the form xH for all $x \in G$. We define the right cosets, $H\backslash G$ similarly.

We have the following results about left and right cosets.

Theorem 1. Let H be a subgroup of G, and $x, y \in G$. Then all of the following hold

1. $Hx = Hy$ precisely when $xy^{-1} \in H$.
2. $|Hx| = |Hy|$.
3. $|Hx| = |xH|$.
4. $Hx = Hy$ or $Hx \cap Hy = \varnothing$.
5. $|G/H| = |HG|$

Proof. First assume $Hx = Hy$, then right multiplying by $\{y^{-1}\}$ yields $H(xy^{-1}) = H$. As H is a subgroup, $1 \in H$, so $1(xy^{-1}) = xy^{-1} \in H$. Now assume $xy^{-1} \in H$, then as subgroups are closed under multiplication, we have $Hxy^{-1} = H$, so multiplying by $\{y\}$ yields $Hx = Hy$. Hence we have (1).

Define $f : Hx \to Hy$ by $f(g) = gx^{-1}y$. This has inverse $f^{-1}(g) = gy^{-1}x$, so f is bijection, so $|Hx| = |Hy|$. A similar bijection may be defined for (3).

Say that $Hx \cap Hy \neq \varnothing$, so we may choose $g \in Hx \cap Hy$, so we have $h_1, h_2 \in H$ such that $g = h_1 x = h_2 y$, yielding $xy^{-1} = h_1^{-1} h_2 \in H$, meaning $Hx = Hy$. □

Of course by symmetry similar results hold for right cosets.

We now show that there are the same number of left and right cosets.

Theorem 2. Let H be a subgroup of G. Then $|G/H| = |H \backslash G|$.

Proof. We define the map $f : G/H \to H \backslash G$ by

$$f(gH) = Hg.$$

We first need to show that f is well-defined. Say $g_1 H = g_2 H$, then $g_1 g_2^{-1} \in H$, so $Hg_1 = Hg_2$. Similar logic shows that f is an injection. We also have f is trivially a surjection. So f is a bijection between the left and right cosets. Hence we have $|G/H| = |H \backslash G|$. □

In light of the previous result, we make the following definition:

Definition 4 (Index of a Subgroup)**.** Let H be a subgroup of G. We define the index of H in G, $[G : H]$ as the common cardinality of the left cosets and the right cosets of H in G, $|G/H| = |H \backslash G|$.

In light of our work, the next theorem now follows trivially.

Theorem 3 (Lagrange's Theorem)**.** Let G be a subgroup of H, then we have

$$|G| = [G : H]|H|.$$

Proof. The left cosets of H in G form a partition of G, with each equivalency class of cardinality $|H|$. Hence we have $|G| = |H|[G : H]$. $\square$

Theorem 4. Let $K \leq L \leq G$, then we have

$$[G : L][L : K] = [G : K]$$

Proof. Let A and B be left transversals of G/L and L/K, respectively.

First we note that if $a, a' \in A$ and $b, b' \in B$ are such that $abK = a'b'K$, then we have

$$\begin{aligned} abKL &= a'b'KL \\ abL &= a'b'L \\ aL &= a'L \\ a &= a' \\ b &= b'. \end{aligned}$$

Hence $abK = a'b'K$ precisely when $a = a'$ and $b = b'$.

Define the mapping $f : A \times B \to AB$ by

$$f(a, b) = ab.$$

This is trivially surjective and is injective by our initial observation. Hence we have

$$\begin{aligned}|AB| &= |A||B| \\ &= [G:L][L:K].\end{aligned}$$

Define the mapping $g : AB \to G/K$ by

$$g(x) = xK.$$

By the initial observation this is injective. We see that

$$\begin{aligned}\cup g(AB) &= ABK \\ &= AL \\ &= G.\end{aligned}$$

So we have that g is surjective. Hence we have

$$\begin{aligned}[G:K] &= |AB| \\ &= [G:L][L:K].\end{aligned}$$

□

The above result is a generalisation of Lagrange's Theorem, which follows by letting K be the trivial subgroup.

We now derive an upper bound for the index of finite intersections of subgroups.

Theorem 5. Let $H_1, H_2, \ldots, H_m \leq G$. Then we have

$$[G : \cap_{i=1}^{n} H_i] \leq \prod_{i=1}^{n} [G : H_i].$$

Proof. Consider $H, K \leq G$. Define the mapping $f : K/(H \cap K) \to G/H$ by

$$f(k(H \cap K)) = kH.$$

This is well-defined as $H \cap K \leq H$. Now we show that f is injective:

$$\begin{aligned} f(k_1(H \cap K)) &= f(k_2(H \cap K)) \\ k_1 H &= k_2 H \\ k_1 k_2^{-1} &\in H \cap K \\ k_1(H \cap K) &= k_2(H \cap K). \end{aligned}$$

So we have that

$$\begin{aligned} [K : H \cap K] &\leq [G : H] \\ [G : K][K : H \cap K] &\leq [G : K][G : H] \\ [G : H \cap K] &\leq [G : K][G : H]. \end{aligned}$$

Hence the result for an arbitrary finite intersection follows from a trivial induction. □

In particular this means that a finite intersection of subgroups of finite index has a finite index itself.

Another natural product to consider is that between two subgroups, H and K. Of course in general this is not a subgroup itself, however we may derive a formula for the cardinality of this product when H and K are finite.

Theorem 6. Let H and K be finite subgroups of G. Then we have

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof. We note that

$$HK = \cup\{Hk\}_{k \in K}$$

Now say that $Hk_1 = Hk_2$ for $k_1, k_2 \in K$, then we have that $k_1 k_2^{-1} \in H \cap K$, or equivalently $(H \cap K)k_1 = (H \cap K)k_2$. The converse follows trivially. So we have a bijective correspondence between $\{Hk\}_{k \in K}$ and the right cosets of $H \cap K$ in K.

Hence we have

$$\begin{aligned} |HK| &= |H|[K : H \cap K] \\ &= \frac{|H||K|}{|H \cap K|}. \end{aligned}$$

□

1.3 Subgroup Generation

An arbitrary subset $X \subset G$ is not necessarily a subgroup under the induced operation. So we aim to define the notion of the "smallest" subgroup that contains X.

Definition 5 (Generated Subgroup)**.**