Abstract Algebra

Jim Coykendall

September 10, 2012

Chapter 1

Warm Up

The notation $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ refer to the natural numbers, the integers, the rational numbers, the real numbers and the complex numbers respectively.

Let $f : A \longrightarrow B$ and $g : B \longrightarrow C$ be functions. We define $\mathrm{im}(f) = f(A) = \{b \in B | b = f(a), a \in A\}$. If $D \subseteq B$ then $f^{-1}(D) = \{a \in A | f(a) \in D\}$. This is called the preimage of D (under f). If $b \in B$ then $f^{-1}(b)$ is called the fiber of f over b. The composite function $g \circ f$ is defined by $(g \circ f)(a) = g(f(a))$. Recall the following:

1. f is one to one or injective if $f(a_1) = f(a_2) \Longrightarrow a_1 = a_2$.
2. f is onto or surjective if $\mathrm{im}(f) = B$.
3. f is bijective if both f is both injective and surjective.
4. f has a left (resp. right) inverse if there is an $h : B \longrightarrow A$ such that such that $h \circ f = 1_A$ (resp. $f \circ h = 1_B$).

Proposition 1.0.1. *Let $F : A \longrightarrow B$.*

1. *f is one to one if and only if f has a left inverse.*
2. *f is onto if and only if f has a right inverse.*
3. *f is bijective if and only if there is a $g : B \longrightarrow A$ such that $f \circ g = 1_B$ and $g \circ f = 1_A$.*
4. *If $|A| = |B| < \infty$ then $f : A \longrightarrow B$ is bijective if and only if f is surjective if and only if f is injective.*

Definition 1.0.2. *Let A be a nonempty set.*

a) A binary realtion on A is a subset $R \subseteq A \times A$ and we write $a \sim b$ if and only if $(a, b) \in R$.

b) $\sim$ is said to be

1. *Reflexive if $a \sim a$ for all $a \in A$.*
2. *Symmetric if $a \sim b$ implies $b \sim a$ for all $a, b \in A$.*
3. *Transitive if $a \sim b$ and $b \sim c$ then $a \sim c$ for all $a, b, c \in A$.*

c) *If $\sim$ is symmetric, reflexive and transistive, then we say that $\sim$ is an equivalence relation.*

d) *If $\sim$ is an equivalence relation then the equivalence class of $a \in A$ is $\{x \in A | x \sim a\}$.*

e) *A partition of the set A is a collection $\{A_i\}$ of subsets of A such that $A = \bigcup_i A_i$ and $A_i \bigcap A_j = \emptyset$ is $i \neq j$.*

Example 1.0.3. *Consider the partitions of the ordinary integers $\mathbb{Z}$ (or even $\mathbb{Z}_n$).*

Proposition 1.0.4. *Let A be a nonempty set.*

- *If $\sim$ is an equivalence relation then the set of equivalence classes form a partition of A.*
- *If the subsets A_i of A form a partition, then there is a an equivalence relation on A such that the sets A_i form the equivalence classes.*

Here are some familiar and useful properties of the integers $\mathbb{Z}$.

Proposition 1.0.5. *Let $\mathbb{Z}$ denote the integers.*

a) *If $\emptyset \neq A \subset \mathbb{Z}^+$ then A has a least element.*

b) *If $a, b \in \mathbb{Z}, a \neq 0$ then we say that $a|b$ if there is a $c \in \mathbb{Z}$ such that $b = ac$.*

c) *Given any nonzero $a, b \in \mathbb{Z}$, there is a $d \in \mathbb{Z}$ (greatest common divisor or gcd) such that $d|a$ and $d|b$ and if d' is another common divisor of a and b then $d'|d$.*

d) *Given any nonzero $a, b \in \mathbb{Z}$, there is an $m \in \mathbb{Z}$ (least common multiple of lcm) such that $a|m$ and $b|m$ and if m' is another common multiple of a and b then $m|m'$.*

e) *Let $d = gcd(a, b)$ and $m = lcm(a, b)$, then $ab = dm$.*

f) *Given nonzero $a, b \in \mathbb{Z}$, then there exist $q, r \in \mathbb{Z}$ with $0 \leq r < |b|$ and $a = qb + r$.*

g) *Let $d = gcd(a, b)$, then there exists $x, y \in \mathbb{Z}$ such that $d = ax + by$.*

h) *(Fundmental Theorem of Arithmetic) If $n \geq 2$ is a natural number, then n can be expressed uniquely as a product of positive integers.*

Consider the following examples with an eye toward the previous result.

Example 1.0.6. *Consider the structure on the sets $\mathbb{Z}/n\mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z})^*$ with "ordinary" addition and multiplication modulo n.*

Chapter 2

Groups

2.1 The Basics

First some basic notions.

Definition 2.1.1. *A binary operation $\circ$ on the nonempty set G is a function $G \times G \longrightarrow G$.*

a) We say that $\circ$ is associative if $g \circ (h \circ k) = (g \circ h) \circ k$ for all $g, h, k \in G$.

b) WE say that $\circ$ is commutative if $g \circ h = h \circ g$ for all $g, h \in G$.

Example 2.1.2. *Ordinary multiplication on the reals, addition on the reals, matrix multiplication.*

Definition 2.1.3. *A group G is a nonempty set equipped with a binary operation $\circ$ such that*

a) $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in G$.

b) There exists $e \in G$ such that $e \circ g = g \circ e = g$ for all $g \in G$.

c) For all $g \in G$, there is an $h \in G$ such that $g \circ h = h \circ g = e$.

From now on, we will suppress that $\circ$ notation and use juxtapostion to denote the operation. If $gh = hg$ for all $g, h \in G$, we say that G is abelian. If $|G|$ we say that G is finite.

Example 2.1.4. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Q}^*$*, the group of rearrangements on the Rubik's cube,* C_6, S_3.

Theorem 2.1.5. *Let G be a group.*

a) $e \in G$ is unique.

b) for all $a \in G$, a^{-1} is unique.

c) $(a^{-1})^{-1} = a$ *for all* $a \in G$.

d) $(ab)^{-1} = b^{-1}a^{-1}$ *for all* $a, b \in G$.

Definition 2.1.6. *Let* G *be a group, we define the order of* G *(*$|G|$*) to be the order of the underlying set* G.

Example 2.1.7. $|\mathbb{Z}_n| = n$.

Definition 2.1.8. *Let* G *be a group.*

a) If $a \in G$ *then* $\circ(a) = |a| = min\{n \in \mathbb{Z}^+ | a^n = e\}$ *(and is said to be* ∞ *if no such* n *exists).*

b) The exponent of G *(*$exp(G)$*) is the smallest positive integers* n *such that* $a^n = e$ *for all* $a \in G$.

2.2 Standard Examples

Here we present some classes of examples of groups.

Dihedral Groups

The dihedral group may be thought of as the group of symmetries on the $n-$gon ($n > 2$). All possible symmetries are generated by superpositions of a rotation of $\frac{2\pi}{n}$ and a flip over the $y-$axis. If we denote the rotation by r and the flip by s, one can see geometrically that $r^n = e = s^2$ and that $srs = r^{-1}$. This is often written as the presentation

$$D_n = \langle r, s | r^n = s^2 = e, srs = r^{-1} \rangle.$$

Symmetric Groups

Symmetric groups may be considered the most important example here. We will study these more carefully later and we will also show that any group may be realized as a subgroup of a symmetric group. Fro now, we will outline what the symmetric groups are.

Let A be a set, we let $S_A = \{f : A \longrightarrow A | f \text{ is bijective.}\}$. Note that the bijectivity is important to ensure that ever element has an inverse. For convenience of notation we denote by the cycle

$$(a_1\ a_2\ \cdots\ a_n)$$

the function that takes a_i to a_{i+1} and a_n to a_1. It can be shown that every element fo S_n can be written as a product of disjoint cycles.

The operation here is function composition. For instance, we have

$$(1\ 2\ 5\ 6\ 4)(2\ 1\ 4\ 5)(1\ 3)(4\ 3)(3\ 6\ 2) = (1\ 3\ 4)(2\ 6)(5)$$

It is fairly easy to show that if $n \geq 3$ then S_n is nonabelian, and that disjoint cycles commute. We will look more deeply at S_n later.

Matrix Groups

First we recall that a field ($\mathbb{F}$) is a set with two binary operations $(+, \cdot)$ such that $(\mathbb{F}, +)$ and $(\mathbb{F} \setminus \{0\}, \cdot)$ are abelian groups and the operations come together through the distributive property

$$a(b+c) = ab + ac, \text{ for all } a, b, c \in \mathbb{F}.$$

A fact that we will show later is that if $\mathbb{F}$ is a finite field, then $|\mathbb{F}| = p^n$ where p is a positive prime number. We introduce the following notation

1. $\mathrm{M}_n(\mathbb{F})$ is the collection of $n \times n$ matrices over $\mathbb{F}$
2. $\mathrm{GL}_n(\mathbb{F})$ is the collection of $n \times n$ matrices over $\mathbb{F}$ with nonzero determinant.
3. $\mathrm{SL}_n(\mathbb{F})$ is the collection of $n \times n$ matrices over $\mathbb{F}$ with determinant 1

Note that the first is a group under matrix addition and the next two are groups under matrix multiplication.

Theorem 2.2.1. *If $\mathbb{F}$ is a finite field with $q = p^m$ elements, then*

$$|GL_n(\mathbb{F})| = (q^n - 1)(q_n - q) \cdots (q^n - q^{n-1})$$

Proof. Let $M \in \mathrm{GL}_n(\mathbb{F})$. Think of building M constructively, row-by-row. This first row can be any $n-$ vector over $\mathbb{F}$ except the zero vector. The second row can be any vector not in the span of the first vector (so there are $q^n - q$ choices). The third row can be any vector that is not in the span of the first two rows (leaving $q^n - q^2$ choices). Continuing this gives the desired result. □

The Group of Quaternions

The group of quaternions has some interesting connections with physics. The group is given by

$$\mathrm{Q}_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with the relations $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki - j$.

2.3 Morphisms

Morphisms are fuctions with algebraic structure. Morphisms are the key tools for comparing algebraic strutures. For example, $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ are sets of the same size, but group-theoretically, they are different.

Definition 2.3.1. *Let $(G, \circ)$ and $(H, *)$ be groups. A function $\phi : G \longrightarrow H$ such that $\phi(x \circ y) = \phi(x) * \phi(y)$ for all $x, y \in G$ is called a homomorphism of groups.*

If $\phi : G \longrightarrow H$ is a homomorphism of groups, we say that ϕ is injective or a monomorphism if ϕ is one to one, we say that ϕ is an epimorphism or surjective if *phi* is onto. A homomorphism that is bijective is called an ispmorphism.

Given any group, G, the identity map from G to itself is an isomorphism. The map $\phi : G \longrightarrow e$ is surjective. The exponential and natural logarithm map are isomorphisms between the additive group of the reals and the multiplicative group of positive reals.

Example 2.3.2. *Consider the isomorphism between D_3 and S_3 that takes the rotation r to $(1\ 2\ 3)$ and the flip s to $(2\ 3)$.*

Theorem 2.3.3. *Let $\phi : G \longrightarrow H$ be a homomorphism.*

a) $\phi(1_G) = 1_H$.

b) $\phi(x^n) = (\phi(x))^n$ *and* $\phi(x^{-1}) = (\phi(x))^{-1}$.

c) If $|x| = n < \infty$ then $|\phi(x)|$ divides $|x|$ (and we have equality if ϕ is an isomorphism).

d) If ϕ is an isomorphism then $|G| = |H|$.

e) If ϕ is an isomorphism then G is abelian if and only if H is abelian.

Proof. Exercise. □

Chapter 3

Subgroups

3.1 Preliminaries

Subgroups are smaller groups within an existing group. Much about the parent group can be gleaned from understanding its subgroups. At the same time, knowing the subgroups of a given groups is often quite important. For example, understanding the subgroups of the Rubik's group is important in finding optimal solutions. Additionally, algebraic objects can often be associated to geometric structures (and vice versa) and subgroups may correspond to important geometric subobjects.

Definition 3.1.1. *Let G be a group. $H \subseteq G$ is called a subgroup if H is a group in its own right (with operation inherited from G).*

Proposition 3.1.2. *$H \subseteq G$ is a subgroup if and only if for all $x, y \in H, xy^{-1} \in H$.*

Proof. One direction (if H is a subgroup) is pretty clear. So suppose that for all $x, y \in H$ we have that $xy^{-1} \in H$. Since $x, x \in H$, $xx^{-1} = e \in H$. Now since $e \in H$, we have that $ex^{-1} = x^{-1} \in H$. Finally note that if $x, y \in H$, we have shown that $y^{-1} \in H$. So we have that $x(y^{-1})^{-1} = xy \in H$. □

Example 3.1.3. $\mathbb{Z} \subseteq \mathbb{Q}$. *Also note that D_n can be realized as a subgroup of S_n.*

We now introduce some concepts that we will study more extensively later. Its utility at this juncture is to give interesting examples of subgroups. First we define a normal subgroup.

Definition 3.1.4. *Let N be a subgroup of G. We say that N is normal in G if $g^{-1}Ng = N$ for all $g \in G$.*

Example 3.1.5. *For example, the subgroup of order 3 is normal in S_3 but no subgroup of order 2 is.*

And now the concept of group actions.

Definition 3.1.6. *A group action of the group G on the set A is a map $G \times A \longrightarrow A$ (written $g \cdot a$) such that*

a) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, $g_1, g_2 \in G$, $a \in A$.

b) $e \cdot a = a$ *for all* $a \in A$.

Perhaps the easiest example of a group acting on a set is for a group G to act on itself by left multiplication. Invertible matrices acting on $\mathbb{R}^n$ is an example that you may have encountered in a linear algebra course.

Definition 3.1.7. *Let $A \subseteq G$ be a nonempty subset.*

a) $C_G(A) = \{g \in G | g^{-1}ag = a, \forall a \in A\}$, *the centralizer of A in G.*

b) $Z(G) = \{g \in G | gx = xg, \forall x \in G\}$, *the center of G.*

c) $N_G(A) = \{g \in G | g^{-1}Ag = A\} = \{g \in G | g^{-1}ag \in A, \forall a \in A\}$, *the normalizer of A in G.*

Note that it is immediate that both $\mathrm{C}_G(A)$ and $\mathrm{N}_G(A)$ are groups and $\mathrm{C}_G(A) \subseteq \mathrm{N}_G(A)$. WE record the following.

Theorem 3.1.8. *$C_G(A) \subseteq N_G(A)$ are subgroups of G as us $Z(G) = C_G(G)$.*

Proof. Exercise. □

Theorem 3.1.9. *Let G act on the set S. The following are subgroups of G.*

a) $G_s = \{g \in G | gs = s\}$ *(the stabilizer of s).*

b) $K = \{g \in G | gs = s, \forall s \in S\}$ *(the kernal of the action).*

Theorem 3.1.10. *Let $\phi : G \longrightarrow H$ be a homomorphism. The follwoing are subgroups.*

a) $ker(\phi) = \{g \in G | \phi(g) = e_H\}$.

b) $im(\phi) = \{\phi(g) | g \in G\}$.

As an exercise, show that $\mathrm{N}_G(\ker(\phi)) = G$ (and note that $\ker(\phi)$ is actually a normal subgroup of G).

The next theorem is extremely useful from a practical point of view.

Theorem 3.1.11. *If $\phi : G \longrightarrow H$ be a homomorphism of groups, then ϕ is one to one if and only if $ker(\phi) = e_H$.*

Proof. It is clear that if ϕ is one to one, then $\ker(\phi) = e_H$. For the other direction, suppose that $\ker(\phi) = e_H$ and suppose that $\phi(x) = \phi(y)$, $x, y \in G$. We now obtain

$$e_H = (\phi(x))^{-1}\phi(y) = \phi(x^{-1})\phi(y) = \phi(x^{-1}y)$$

and so $x^{-1}y \in \ker(\phi) = e_H$. Hence $y = x$ and we are done. □

3.2 The Classification of Cyclic Groups

Cyclic groups are the groups that are generated by a single element. More precisely, we give the following definition.

Definition 3.2.1. *We say that G is cyclic if there is an $x \in G$ such that*

$$G = \{x^n | n \in \mathbb{Z}\}.$$

We say, in this case, that $G = \langle x \rangle$.

Note that G is not necessarily infinite, the above listed set may have an enormous amount of repetition.

Example 3.2.2. *$\mathbb{Z}_n$ and $\mathbb{Z}$ are cyclic groups. And, in a certain sense, this list is exhaustive.*

Proposition 3.2.3. *If $G = \langle x \rangle$ then $|G| = |x|$.*

Proof. (Note that in any event, $|G| \geq |x|$ and $\langle x \rangle \subseteq G$.) Suppose first that $G = \langle x \rangle$ and G is finite. It suffices to show that $|G| \leq |x|$. Since every element of G is a power of x (say $g_k = x^k$), the map $f : I \longrightarrow G$ (I is the collection of positive integers less than or equal to $|x|$) is a surjection. This establishes the proposition in the finite case. For the case where G is of infinite order, it is clear that the generator x cannot be of finite order. □

Proposition 3.2.4. *Suppose G is a group, $x \in G$ and $m, n \in \mathbb{Z}$. If $x^m = 1 = x^n$ then $x^{gcd(m,n)} = 1$.*

Proof. We know that if $d = \gcd(m, n)$ then there exist $a, b \in \mathbb{Z}$ such that $am + bn = d$. Hence $x^d = x^{am+bn} = (x^m)^a(x^n)^b = 1$. □

Theorem 3.2.5. *Any two cyclic groups of the same order are isomorphic.*

Proof. (Sketch) If $G = \langle x \rangle$ is of infinite order, then the map $n \longrightarrow x^n$ from $\mathbb{Z}$ to G is an isomorphism. USe the previous result to establish the finite case. □

Theorem 3.2.6. *Let G be a group and $x \in G$ of order $n \leq \infty$.*

a) If $n = \infty$ then $|x^a| = \infty$ for all $a \neq 0$.

b) If $n < \infty$ then $|x^a| = \frac{n}{gcd(a,n)}$.

Proof. If x^a has finite order, it is easy to see that x has finite order. Now let $d = \gcd(a, n)$. $(x^a)^{\frac{n}{d}} = 1$ since $d|a$. Now suppose that $(x^a)^k = 1$. Certainly $ak = mn$ and writing $a = da'$ and $n = dn'$ with $\gcd(a', n') = 1$. We now have $a'k = mn'$ and hence $a'|m$. We conclude that $k = \frac{m}{a'}\frac{n}{d}$ is an integer multiple of $\frac{n}{d}$. So this means that the order of x^a is a multiple of $\frac{n}{d}$ and we are done. □

Theorem 3.2.7. *Let $H = \langle x \rangle$.*

a) If $|x| = \infty$ then $H = \langle x^a \rangle$ if and only if $a = \pm 1$.

b) If $|x| = n < \infty$ then $H = \langle x^a \rangle$ if and only if gcd$(a, n) = 1$.

Proof. Exercise. □

Theorem 3.2.8. *Let G be a cyclic group.*

a) If $H \subseteq G$ is a subgroup, then H is cyclic.

b) If $\phi : G \longrightarrow H$ is onto, then H is cyclic.

c) If $|G| = n < \infty$ then for all $m|n$ there is a unique subgroup of G of order m.

Proof. a) Let $H \subseteq G = \langle x \rangle$ be a nontrivial subgroup. Consider $\{n \in \mathbb{N} | x^n \in H\}$. Since H is a subgroup of G, this set in nonempty and hence has a least element (sa d). We claim that H is generated by x^d. Since $\langle x^d \rangle$ is clearly contained in H, we merely need to show that other containment. To this end, suppose that $h \in H$. Since G is cyclic, $h = x^m$ and we will assume WLOG that $m > 0$. Writing $m = qd + r$ with $0 \leq r < m$. If $r \neq 0$, we have that $x^r = (x^m)((x^d)^m)^{-1} \in H$ which contradicts the minimality of d and we have established the claim.

For b), let x be the generator of G. Verify that $\phi(x)$ is the generator for H (the surjectivity of ϕ is important here.

For c), suppose that $n = mk$. Notice that the order of the subgroup generated by x^k is precisely m. It suffices to show that this is the only subgroup of order m. Suppose there is another group of order m (necessarily cyclic). We call this subgroup $H = \langle x^a \rangle$. By the above, the order of $|x^a| = |H|$ is given by $\frac{n}{\gcd(a,n)} = m$. Since $m = \frac{n}{\gcd(k,n)}$, we have that $d := \gcd(a, n) = \gcd(k, n)$. Since there are integers r, s such that $ra + sn = d$, we have that

$$x^d = (x^a)^r (x^n)^s = x^{ar} \in H$$

and since $d|k$ we have that $x^k \in H$. Hence $\langle x^k \rangle \subseteq H$ and since they both have order m, we must have equality. This establishes the theorem. □

We now make some last observations of this chapter.

Proposition 3.2.9. *If $\{H_i\}_{i \in \Lambda}$ is a collection of subgroups of G, then $\bigcap_{i \in \Lambda} H_i \subseteq G$ is a subgroup of G*

Proof. Exercise. □

Proposition 3.2.10. *If A is a subset of G, then we define*

$$\langle A \rangle = \bigcap H$$

where H ranges over the subgroups of G containing A.

Another way to think of $\langle A \rangle$ is as the collection of all "words" that can be formed from the "letters" a and a^{-1} where $a \in A$.

Example 3.2.11. *Draw a lattice representing the subgroups of D_4, $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, and S_3*

Chapter 4

Quotient Groups and Homomorphisms

4.1 Normality and Quotients

We begin with the definition of normal subgroup.

Definition 4.1.1. *Let $N \leq G$, we say that N is a normal subgroup of G ($N \trianglelefteq G$) if $g^{-1}Ng = N$ for all $g \in G$ (equivalently $N_G(N) = G$).*

Note $N \trianglelefteq G$ if and only if $g^{-1}ng \in N$ for all $g \in G$.

Example 4.1.2. *Find all the subgroups of S_3 and determine which are normal.*

Proposition 4.1.3. *If G is abelian and $H \subseteq G$ then $H \trianglelefteq G$.*

Proof. Exercise. □

Proposition 4.1.4. *Let $\phi : G \longrightarrow H$ be a homomorphism, then ker(ϕ) $\trianglelefteq G$.*

Proof. Let $k \in \ker(\phi)$ and $x \in G$. $\phi(x^{-1}kx) = (\phi(x))^{-1}\phi(k)\phi(x) = e_H$. Hence $x^{-1}kx \in \ker(\phi)$ and we are done. □

Definition 4.1.5. *Let $H \subseteq G$ be a subgroup. We define a left (resp. right) coset of H is G via*

$$gH = \{gh|h \in H\} \text{ (resp. } Hg = \{hg|h \in H\}.$$

Any element of a left (resp. right) coset is called a representative of the coset.

Example 4.1.6. *Consider $2\mathbb{Z} \subseteq \mathbb{Z}$. There are precisely two left (right) cosets. Also this subgroup is normal. If we consider the subgroup of order 3 in S_3, it is normal and its left and right cosets coincide (as sets). Contrast this with a subgroup of order 2. In this second case, the left (right) cosets again partition S_3 but they do not coincide.*

Theorem 4.1.7. *Let $H \subseteq G$. The collection of left (right) cosets of H in G forms a partition of G. More precisely,*

$$G = \bigcup_{g \in G} gH$$

and if $g_i H \bigcap g_j H \neq \emptyset$ then $g_i H = g_j H$.

Proof. Since $g \in G$ and $H \subseteq G$, each $gH \subseteq G$ and hence $G \supseteq \bigcup_{g \in G} gH$. For the other containment, note that for all $g \in G$, $g \in gH$. So $G \subseteq \bigcup_{g \in G} gH$.

To see the other statement, suppose that $xH \bigcap yH \neq \emptyset$, that is let $z \in xH \bigcap yH$. We write $z = xh_1 = yh_2$ and hence $y = xh_1 h_2^{-1}$. Now let $yh \in yH$ be arbitrary. Since $yh = xh_1 h_2^{-1} h$, we have that $yH \subseteq xH$. By a symmetric argument we obtain the other containment and hence $xH = yH$. □

Proposition 4.1.8. *Let $H \subseteq G$ be a subgroup and $x, y \in G$, then $xH = yH$ if and only if $y^{-1}x \in H$ (so $xH = yH$ if and only if x and y represent the same coset).*

Proof. ($\Longrightarrow$) Suppose first that $xH = yH$. Hence there exist $h_1, h_2 \in H$ such that $xh_1 = yh_2$. Hence $y^{-1}x = h_2 h_1^{-1} \in H$.

($\Longleftarrow$) Since $y^{-1}x = h \in H$, we have that $x = yh$. If $xh_1 \in xH$, then observe that $xh_1 = yhh_1 \in yH$. Additionally, if $yh_1 \in yH$, we see that $yh_1 = yhh^{-1}h_1 = xh^{-1}h_1 \in xH$. This establishes the result. □

Proposition 4.1.9. *Let G be a group and N a subgroup of G. $N \trianglelefteq G$ if and only if $gN = Ng$ for all $g \in G$ (that is, left cosets are right cosets).*

Proof. ($\Longrightarrow$) Recall that $N = g^{-1}Ng$. Let $ng \in Ng$. Since $g^{-1}ng = n_1 \in N$, $ng = gn_1 \in gN$. The other containment is similar.

($\Longleftarrow$) Given that $gN = Ng$, we must show that $g^{-1}ng \in N$. By assumption, we have that $ng = g_1^n$ and hence, $g^{-1}ng = n_1 \in N$. □

The next result is fundamental in the study of groups.

Proposition 4.1.10. *Let $N \trianglelefteq G$ and let $G/N := \{gN | g \in G\}$ denote the set of left (right) cosets of N in G. The binary operation defined by*

$$(g_1 N)(g_2 N) = (g_1 g_2)N$$

makes G/N into a group (quotient or factor group).

Proof. We must first show that this binary operation is well defined. To this end, suppose that $x_1, x_2 \in xN$ and that $y_1, y_2 \in yN$. We need to show that $x_1 y_1 N = x_2 y_2 N$, and by an earlier result, we merely need to show that $(x_2 y_2)^{-1}(x_1 y_1) \in N$. By assumption, we have that $x_1 = xa$, $x_2 = xb$, $y_1 = yc$, $y_2 = yd$ with $a, b, c, d \in N$. Hence we have that

$$(x_2 y_2)^{-1}(x_1 y_1) = d^1 y^{-1} b^{-1} x^{-1} xayc = d^1 y^{-1} b^{-1} ayc \in N$$

since N is normal. So this operation is well-defined. With this in hand it is easy to show that G/N is a group (with identity eN, and the inverse of xN is $x^{-1}N$). □

The next result really ties the room together.

Theorem 4.1.11. *The following conditions are equivalent.*

a) $N \trianglelefteq G$.

b) $N_G(N) = G$.

c) $gN = Ng$ *for all* $g \in G$.

d) G/N *is a group.*

Proposition 4.1.12. N *is normal in* G *if and only if there is a homomorphism* ϕ *on* G *such that* $N = ker(\phi)$.

Proof. Exercise, consider the canonical homomorphism $\phi : G \longrightarrow G/N$. □

4.2 Counting Corollaries and Lagrange's Theorem

We first recall the fact that if $H \subseteq G$ is a subgroup, then G is partitioned by the (left) cosets of H in G. We introduce a famous theorem due to Lagrange.

Theorem 4.2.1. *If* G *is finite and* $H \subseteq G$*, then* $|H|$ *divides* $|G|$ *and the quotient is the number of (left) cosets of* H *in* G.

We first remark that parts of this theorem goes through in the infinite case.

Proof. We have already established that the collection of (left) cosets of H forms a partition of G. Noting that $|gH| = |H|$ for all $g \in G$, and $\bigcup_{g\in G} gH = G$, we see that if k denotes the number of left cosets of H in G, then $|G| = k|H|$. □

We denote the number of (left) cosets of H in G be $|G : H|$.

Example 4.2.2. $|\mathbb{Z} : n\mathbb{Z}| = n$ *if* $n > 0$. *What happens if* $n = 0$*?*

Corollary 4.2.3. *If* G *is a finite group and* $x \in G$ *then* $|x|$ *divides* $|G|$.

Corollary 4.2.4. *If* $|G| = p$*, where* p *is prime, then* $G \cong \mathbb{Z}/p\mathbb{Z}$.

Here is a very important and famous theorem due to Cauchy.

Theorem 4.2.5. *If* $|G| = n < \infty$ *and* $p|n$ *then there exists* $x \in G$ *such that* $|x| = p$.

Proof. We write G multiplicatively and let

$$S = \{(x_1, x_2, \cdots, x_p) | x_i \in G, x_1 x_2 \cdots x_p = 1\}.$$

Note that $|S| = |G|^{p-1} = n^{p-1}$ (since the first $p-1$ elements can be chosen at will and the last one is "forced"). Hence p divides $|S|$.

On the set S we say that $a \sim b$ if b is a cyclic permutation of a (e.g. $a = (x_1, x_2, \cdots, x_p)$ and $b = (x_i, x_{i+1}, \cdots, x_p, x_1, x_2, \cdots, x_{i-1})$). (Show that $\sim$ is an equivalence relation.

Notice that if

□