

MATH 580–AUTUMN 2009
GROUP THEORY NOTES

1. BASIC GROUP THEORY

In this section, we aim to define the concept of an abstract group and prove some of the basic properties of groups. In this set of notes, S and T denote non-empty sets. First, let us recall the following definition from basic set theory.

Definition 1.1. *The Cartesian product of S and T (denoted $S \times T$) is the set of ordered pairs with first component in S and second component in T . In set notation,*

$$S \times T = \{(a, b) \mid a \in S, b \in T\}.$$

For a non-empty set S , we get the following definition that will be necessary to define a group.

Definition 1.2. *A binary operation on S is any function $\tau : S \times S \rightarrow S$.*

Many algebra text avoid using τ and ordered pairs when denoting binary operations. Instead they will often use the following conventions. Either they will use a dot so that $\tau(a, b) = a \cdot b$ or they will simply write the group elements adjacent to each other as $\tau(a, b) = ab$ so that the notation resembles the notation for a product in \mathbb{C} .

Example 1.1. *Here are some examples of binary operations.*

- a. *Let $S = \mathbb{Z}$ (the integers) with binary operation $a \cdot b = a + b$.*
- b. *Let $S = \mathbb{Z}$ with binary operation $a \cdot b = a - b$.*
- c. *Let $S = \mathbb{Z}$ with binary operation $a \cdot b = a \times b$.*
- d. *Let $S = \mathbb{Z}$ with binary operation $a \cdot b = a^3 + b^{|a|} - 2$.*
- e. *Let $S = \mathbb{Z}/n$ (the set of equivalence classes of \mathbb{Z} modulo n) with binary operation $[a] \cdot [b] = [a + b]$.*
- f. *Let $S = \mathbb{Z}/n$ (the set of equivalence classes of \mathbb{Z} modulo n) with binary operation $[a] \cdot [b] = [a \times b]$.*
- g. *Let $S = C(\mathbb{R})$ (the set of continuous functions $f : \mathbb{R} \rightarrow \mathbb{R}$) with binary operation $f \cdot g = f + g$.*
- h. *Let $S = C(\mathbb{R})$ with binary operation $f \cdot g = f \circ g$ (note, we need to verify that $f \circ g \in C(\mathbb{R})$ or equivalently that $f \circ g : \mathbb{R} \rightarrow \mathbb{R}$ is continuous).*
- i. *Let X be a finite set and $S = \text{Sym}(X)$ be the set of bijections $f : X \rightarrow X$ with binary operation $f \cdot g = f \circ g$ (note, in Math 345 we verified that $f \circ g \in \text{Sym}(X)$ or equivalently that $f \circ G : X \rightarrow X$ is a bijection).*
- j. *Let S be any non-empty set with binary operation $a \cdot b = a$.*

Not all binary operations are equally interesting from the perspective of algebra. In particular, we are interested in sets combined with binary operations that satisfy three properties.

Definition 1.3. A **group** (denoted G) is a set S with a binary operation \cdot that satisfies the following three properties.

- (G1) For any $a, b, c \in S$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- (G2) There exists an element $e \in S$ such that for all $a \in S$, $e \cdot a = a \cdot e = a$.
- (G3) For any $a \in S$, there exists an element $b \in S$ such that $a \cdot b = b \cdot a = e$.

Condition (G1) is referred to as **associativity**. The element e in condition (G2) is called an **identity element**. For any $a \in S$, the b in condition (G3) is called an **inverse** of a .

Remark 1.1. Many sources conflate the set S with the group G . These sources will write $a \in G$ to mean a in the set S having a particular binary operation \cdot .

If G is a group whose underlying set S is finite, we call G a **finite group**.

Here are some basic results about uniqueness of inverses and the identity element.

Proposition 1.1. Let G be a group. Then G has a unique identity element and every element has a unique inverse.

Proof. Let e_1 and e_2 be identity elements in G and consider the product $e_1 \cdot e_2$. Since e_1 is an identity element, $e_1 \cdot e_2 = e_2$. Similarly, since e_2 is an identity element, $e_1 \cdot e_2 = e_1$. Thus,

$$e_2 = e_1 \cdot e_2 = e_1.$$

Let $a \in G$ and let both b_1 and b_2 be inverses of a . Now consider the product

$$\begin{aligned} b_1 &= b_1 \cdot e && \text{(definition of identity)} \\ &= b_1 \cdot (a \cdot b_2) && \text{(definition of inverse)} \\ &= (b_1 \cdot a) \cdot b_2 && \text{(associativity)} \\ &= e \cdot b_2 && \text{(definition of inverse)} \\ &= b_2 && \text{(definition of identity)} \end{aligned}$$

□

Because inverses are unique, we often denote the inverse of $a \in G$ as a^{-1} . This uniqueness also affords us the following corollary.

Corollary 1.1. Let G be a group. For any elements $a, b \in G$, we have

- (i) $(a^{-1})^{-1} = a$.
- (ii) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Proof. To prove (i), we consider the products $a^{-1} \cdot a$ and $a \cdot a^{-1}$. By definition of a^{-1} , we have $a^{-1} \cdot a = a \cdot a^{-1} = e$. Since $(a^{-1})^{-1}$ is the unique such element of G such that

$$a^{-1} \cdot (a^{-1})^{-1} = (a^{-1})^{-1} \cdot a^{-1} = e$$

we have $a = (a^{-1})^{-1}$.

To prove (ii), consider the product $(a \cdot b) \cdot (b^{-1} \cdot a^{-1})$

$$\begin{aligned} (a \cdot b) \cdot (b^{-1} \cdot a^{-1}) &= (a \cdot (b \cdot b^{-1})) \cdot a^{-1} && \text{(associativity)} \\ &= (a \cdot e) \cdot a^{-1} && \text{(definition of inverse)} \\ &= a \cdot a^{-1} && \text{(definition of identity)} \\ &= e && \text{(definition of inverse)} \end{aligned}$$

Similarly, we have $(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = e$. So $b^{-1} \cdot a^{-1}$ is the unique inverse of $a \cdot b$. \square

We should also make the following note regarding notation. For a group G , an element $a \in G$, and an integer $n \in \mathbb{Z}$, we define a^n in the following way

$$a^n = \begin{cases} \overbrace{a \cdot a \cdots a}^{n \text{ times}} & \text{if } n \geq 1 \\ e & \text{if } n = 0 \\ \overbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}^{|n| \text{ times}} & \text{if } n \leq -1 \end{cases} .$$

Notice that none of our axioms for groups demonstrate that $a \cdot b = b \cdot a$. This property (called **commutativity**) need not hold for arbitrary groups. So we get the following definition.

Definition 1.4. Let G be a group so that for any $a, b \in G$, $a \cdot b = b \cdot a$. Such a group is called an **abelian group**.

Since we now see that groups need not be commutative, one should verify the following proposition.

Proposition 1.2. Let S be a set with an associative binary operation \cdot . Suppose that the following conditions hold.

- (i) There exists elements e_R and e_L in S so that for any $a \in S$, $e_L \cdot a = a$ and $a \cdot e_R = a$.
- (ii) For any $a \in S$, there exists elements b_L and b_R in S , such that $b_L \cdot a = e_L$ and $a \cdot b_R = e_R$. Then S and \cdot define a group.

Proof. The proof mirrors that of Proposition 1.1. First, consider the product $e_L \cdot e_R$. By condition (i), $e_L \cdot e_R = e_R$ and $e_L \cdot e_R = e_L$ so

$$e_L = e_L \cdot e_R = e_R.$$

Thus $e_L = e_R$ is an identity element.

Now let $a \in S$ and consider

$$\begin{aligned}
 b_L &= b_L \cdot e_R && \text{(by condition (i))} \\
 &= b_L \cdot (a \cdot b_R) && \text{(by condition (ii))} \\
 &= (b_L \cdot a) \cdot b_R && \text{(by associativity)} \\
 &= e_L \cdot b_R && \text{(by condition (ii))} \\
 &= b_R && \text{(by condition (i))}
 \end{aligned}$$

So $b_L = b_R$ is an inverse for a .

Finally, since \cdot is associative, we see that conditions (G1), (G2), and (G3) of Definition 1.3 are satisfied. \square

2. SUBGROUPS AND COSETS

In this section, we to define the concept of a subgroup of a group and to derive an equivalence relation using the subgroup. As mentioned in the basic group theory notes, a group G is both a set S with a binary operation; however, we will often conflate notation and treat G like a set.

Definition 2.1. *Let G be a group (with group operation \cdot). Let H be a subset of G that is also a group with respect to the operation \cdot . We call H a subgroup of G .*

In this definition, notice that we have two sets G and H but only one group operation. So a subgroup is a subset of a group that is a group with respect to the same group operation. We now develop a set of criteria to determine when a subset of a group G is indeed a subgroup.

With this definition, we now prove the following proposition that gives criteria for when a subset of a group is a subgroup.

Proposition 2.1. *Let G be a group (with operation \cdot) and $H \subset G$ a subset. Suppose that the following conditions hold*

- (i) *For any $a, b \in H$, $a \cdot b \in H$.*
- (ii) *For any $a \in H$, $a^{-1} \in H$.*

Then $H \subset G$ is a subgroup.

Proof. Statement (i) shows that when we restrict the binary operation on G to the subset H , we get a binary operation on H . So since \cdot defines a binary operation on H , we now only need to verify the group axioms. When this occurs, we say that H is closed under the operation \cdot .

First, since the operation \cdot defined a group on G , we have that \cdot is associative. However, \cdot is also the operation on H , so associativity holds.

Second, let $a \in H$. By (ii), we have $a^{-1} \in H$. Moreover, by (i), $a \cdot a^{-1} \in H$. But $a \cdot a^{-1} = e \in H$. Furthermore, for any $b \in H$, we have $b \in G$ since $H \subset G$. So $e \cdot b = b \cdot e = b$ for all $b \in H$.

Third, for any $a \in H$, $a^{-1} \in H$ by (ii) and $a \cdot a^{-1} = a^{-1} \cdot a = e$ by definition of a^{-1} .

So H satisfies the group axioms for the operation \cdot . □

Let us consider some examples.

Example 2.1. Let G be the group of integers \mathbb{Z} under the addition operation.

- a. Let $H = \{k \in \mathbb{Z} \mid 1 \leq k \leq 10\}$. Notice that H is **not** a subgroup. In fact, $6 \in H$ and $8 \in H$, but $6 + 8 = 14 \notin H$ so H is **not** closed under addition.
- b. Let $H = \mathbb{N}$. For any $a, b \in \mathbb{N}$, $a \cdot b = a + b \in \mathbb{N}$. So H satisfies (i) and is closed under addition. However for any $a \in \mathbb{N}$, $a^{-1} = -a$ for the addition operation and $-a \notin \mathbb{N}$. So H is **not** a subgroup.
- c. Let $H = 3\mathbb{Z} = \{3k \mid k \in \mathbb{Z}\}$. For any $a, b \in H$, there exists $j, k \in \mathbb{Z}$ so that $a = 3j$ and $b = 3k$. Thus $a \cdot b = a + b = 3j + 3k = 3(j + k)$ and, since $j + k \in \mathbb{Z}$, we find $a + b \in H$. Thus H is closed under addition. Now let us consider inverses. For any $a \in H$, there exists $k \in \mathbb{Z}$ with $a = 3k$. Thus $a^{-1} = -a = 3(-k)$ and, since $-k \in \mathbb{Z}$, we see that $a^{-1} \in H$.

Let us consider another wider example.

Example 2.2. Let G be any group and $H = \{e\}$. Then H is a subgroup of G . Notice that for any $a, b \in H$, $a = b = e$ and $a \cdot b = e \cdot e = e \in H$. So H is closed under the group operation. Furthermore, for any $a \in H$, $a = e$ and $a^{-1} = e^{-1} = e = a \in H$, so H satisfies the subgroup hypothesis.

With Example 2.2, we get the following definition.

Definition 2.2. Let G be a group. Then the subsets $\{e\}$ and G are subgroups of G . We call these the trivial subgroups of G .

We conclude our examples with the following lemma.

Lemma 2.1. Let G be a finite group and let $a \in G$. Then the subset $H = \{a^n \mid n \in \mathbb{N}\}$ is a subgroup of G .

Proof. For any $h_1, h_2 \in H$, we can find $j, k \in \mathbb{N}$ so that $h_1 = a^j$ and $h_2 = a^k$. Then $h_1 \cdot h_2 = a^j \cdot a^k = a^{j+k}$. Since $j + k \in \mathbb{N}$, we find $h_1 \cdot h_2 \in H$. So H is closed under the group operation.

Suppose that for any $j, k \in \mathbb{N}$ with $j \neq k$ that $a^k \neq a^j$, then the function $f : \mathbb{N} \rightarrow H$ given by $f(n) = a^n$ is a bijection from \mathbb{N} to H . So H is infinite. But $H \subset G$ and G is finite, a contradiction. Thus we have that for some $j, k \in \mathbb{N}$ with $j \neq k$, $a^j = a^k$ (without loss

of generality, suppose that $j > k$). Thus, $a^j \cdot a^{-k} = a^k \cdot a^{-k} = e$. But $a^j \cdot a^{-k} = a^{j-k}$, so $a^{j-k} = e$.

If $j - k = 1$, we see that $a = a^1 = e$. Furthermore, $a^n = e^n = e$ for all $n \in \mathbb{N}$. Thus $H = \{e\}$, a trivial subgroup.

If $j - k \geq 2$, we see that $a^{j-k} = a \cdot a^{j-k-1} = a^{j-k-1} \cdot a$. So $a^{j-k-1} = a^{-1}$ and we have that $j - k - 1 \in \mathbb{N}$.

For any $h \in H$, there is an $n \in \mathbb{N}$ so that $h = a^n$. Furthermore, $h^{-1} = a^{-n} = a^{n(j-k-1)}$, but $n(j-k-1) \in \mathbb{N}$, so $h^{-1} \in H$. Therefore H satisfies the criteria for a subgroup of G . \square

We call the subgroup $H \subset G$ in Lemma 2.1 the cyclic subgroup of G generated by a , since it is formed by all the powers of the element a . We can also form cyclic subgroups of infinite groups. For G infinite and $a \in G$, let $H = \{a^n \mid n \in \mathbb{Z}\}$. Notice here we must actually specify that $a^{-1} \in H$ since a^{-1} need not be equal to a^n for any $n \in \mathbb{N}$. We typically use the notation $\langle a \rangle$ to denote the cyclic subgroup generated by a .

It could also be the case that the cyclic subgroup $H = G$. In this case, we call G a cyclic group. Here are some examples.

Example 2.3. *We have the following example of cyclic groups.*

- a. *Let G be the group of equivalence classes of the integers mod n (\mathbb{Z}/n) under the addition operation $[a] + [b] = [a + b]$ (which we previously showed is well defined). Then G is a finite cyclic group generated by the element $a = [1]$ where $a^n = [n]$.*
- b. *Let G be the group of integers (\mathbb{Z}) under addition. Then G is an infinite cyclic group generated by the element $a = 1$. In this case $a^n = n$, $a^0 = 0$, and $a^{-n} = -n$.*

The definition of cyclic subgroups also gives the following definition.

Definition 2.3. *Let G be a group, $a \in G$. Suppose that there exists an $n \in \mathbb{N}$ for which $a^n = e$, we then let $\text{ord}(a) = \min\{n \in \mathbb{N} \mid a^n = 1\}$ be the smallest since positive integer. We say that a is an element of finite order and we call that order n . If no such n exists, we say that a has infinite order.*

The relationship between the order is given by the following lemma.

Lemma 2.2. *Let G be a group, $a \in G$ have finite order, and $H = \langle a \rangle$ be the cyclic group generated by a . Then $|H| = \text{ord}(a)$.*

Proof. Let $n = \text{ord}(a)$. For any $m \in \mathbb{Z}$, we can find integers q and r with $0 \leq r \leq n - 1$ so that $m = qn + r$ (this is the Division Algorithm). So

$$a^m = a^{nq+r} = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$$

and we see that $H = \{a^0 = e, a, a^2, \dots, a^{n-1}\}$ and $|H| \leq n$.

Now suppose there exists $s, t \in \{0, 1, 2, \dots, n-1\}$ with $a^s = a^t$. Without loss of generality suppose that $s \leq t$, then $0 \leq t - s \leq n - 1$. So

$$e = a^s \cdot a^{-s} = a^t \cdot a^{-s} = a^{t-s}$$

but $n = \text{ord}(a)$ is the smallest positive integer with $a^n = e$, so $t - s = 0$ and $s = t$. Thus the elements in $H = \{e, a, a^2, \dots, a^{n-1}\}$ are distinct. So $|H| = n$. \square

With the definition of subgroups, we can also define an equivalence relation on G as follows.

Definition 2.4. Let G be a group and H a subgroup. We say that for $a, b \in G$ that $a \equiv_H b$ if $a \cdot b^{-1} \in H$. We refer to this relation as congruence modulo H .

Next we aim to show that this is an equivalence relation.

Proposition 2.2. Let G be a group and H a subgroup. Then equivalence modulo H defines an equivalence relation on G .

Proof. Since H is a subgroup, we have that $e \in H$. So for any $a \in G$, $a \cdot a^{-1} = e \in H$. So $a \equiv_H a$ for all $a \in G$.

Suppose that $a \equiv_H b$. Then $a \cdot b^{-1} \in H$. But H is a subgroup so $(a \cdot b^{-1})^{-1} \in H$. By Corollary 1.1, we have that $(a \cdot b^{-1})^{-1} = (b^{-1})^{-1} \cdot a^{-1} = b \cdot a^{-1}$. So $b \cdot a^{-1} \in H$ and $b \equiv_H a$.

Next suppose that $a \equiv_H b$ and $b \equiv_H c$. Then $a \cdot b^{-1} \in H$ and $b \cdot c^{-1} \in H$. Since H is a subgroup $(a \cdot b^{-1}) \cdot (b \cdot c^{-1}) \in H$. But we see that

$$\begin{aligned} (a \cdot b^{-1}) \cdot (b \cdot c^{-1}) &= (a \cdot (b^{-1} \cdot b)) \cdot c^{-1} && \text{(associativity)} \\ &= (a \cdot e) \cdot c^{-1} && \text{(definition of inverse)} \\ &= a \cdot c^{-1} && \text{(definition of identity)} \end{aligned}$$

So $a \cdot c^{-1} \in H$ and $a \equiv_H c$. \square

Now let us consider what the equivalence classes for this equivalence relation.

Definition 2.5. Let G be a group and H be a subgroup of G . For any $g \in G$, we call the set $H \cdot g = \{h \cdot g \mid h \in H\}$ the right coset of H containing g .

Because H is a subgroup, $e \in H$. Thus $g = e \cdot g \in H \cdot g$ so $H \cdot g$ actually contains g so calling it the right coset containing g is not a misnomer. Now consider the following proposition.

Proposition 2.3. Let G be a group and H be a subgroup. Consider the equivalence relation in Proposition 2.2. Then the right cosets $H \cdot g$ is the equivalence class of g with respect to this equivalence relation.

Proof. Let $g \in G$ and $[g]$ be the equivalence class of g under \equiv_H . We want to show that $[g] = H \cdot g$ as sets.

Let $a \in [g]$. The $a \equiv_H g$ so $a \cdot g^{-1} \in H$. Thus, there exists an element $h \in H$ so that $a \cdot g^{-1} = h$. Therefore $(a \cdot g^{-1}) \cdot g = h \cdot g$. Moreover,

$$(a \cdot g^{-1}) \cdot g = a \cdot (g^{-1} \cdot g) = a \cdot e = a$$

so $a = h \cdot g$. Thus $[g] \subset H \cdot g$.

Let $a \in H \cdot g$. Then there exists an element $h \in H$ so that $a = h \cdot g$. Thus $a \cdot g^{-1} = (h \cdot g) \cdot g^{-1}$. So

$$(h \cdot g) \cdot g^{-1} = h \cdot (g \cdot g^{-1}) = h \cdot e = h,$$

thus $a \cdot g^{-1} \in H$. So we see that $a \equiv_H g$ and $H \cdot g \subset [g]$. \square

One could reasonably ask whether it makes sense to define left cosets as $g \cdot H = \{g \cdot h \mid h \in H\}$. We call the set $g \cdot H$, the left coset containing g . These left cosets are equivalence classes for a related, but different, equivalence relation on G . In this case, we let G be a group and H be a subgroup. We define the relation on G by saying that $a, b \in G$ are related if $a^{-1} \cdot b \in H$ (notice the difference from above with respect to which element is inverted). It is also worth noting that the coset $H \cdot g$ need not be the same as $g \cdot H$ as sets. We can, however, form a bijection between them.

Lemma 2.3. *Let G be a group and H a subgroup, then for any $g \in G$, there exists a bijection $\varphi_g : H \cdot g \rightarrow g \cdot H$ given by $\varphi_g(a) = g \cdot a \cdot g^{-1}$.*

Proof. First, let $b \in g \cdot H$, then there exists an $h \in H$ with $b = g \cdot h$. Now let $a = h \cdot g$ (same h that we found for b). Thus $a \in H \cdot g$ and

$$\varphi_g(a) = g \cdot a \cdot g^{-1} = g \cdot h \cdot g \cdot g^{-1} = g \cdot h \cdot e = g \cdot h = b$$

so our φ_g is surjective.

Let $a, b \in H \cdot g$ so that $\varphi_g(a) = \varphi_g(b)$. Thus $g \cdot a \cdot g^{-1} = g \cdot b \cdot g^{-1}$. So

$$(g^{-1} \cdot g) \cdot a \cdot (g^{-1} \cdot g) = (g^{-1} \cdot g) \cdot b \cdot (g^{-1} \cdot g)$$

which implies $a = e \cdot a \cdot e = e \cdot b \cdot e = b$ and we see that φ_g is injective. \square

We can also use a similar proof to show that we have a bijection between any two right cosets (or equivalently any two left cosets).

Proposition 2.4. *Let G be a group and H a subgroup. Then, for any $a, b \in G$, there exists a bijection $\phi_{ab} : H \cdot a \rightarrow H \cdot b$ given by $\rho_{a^{-1}b}(g) = g \cdot (a^{-1} \cdot b)$.*

Proof. Let $g \in H \cdot b$, then there exists an $h \in H$ such that $g = h \cdot b$. Let $g_0 = h \cdot a$ (same h we found for g). Thus $g_0 \in H \cdot a$ with

$$\rho_{a^{-1}b}(g_0) = g_0 \cdot (a^{-1} \cdot b) = (h \cdot a) \cdot (a^{-1} \cdot b) = h \cdot (a \cdot a^{-1}) \cdot b = h \cdot b = g$$

so $\rho_{a^{-1}b}$ is surjective.

Let $g_1, g_2 \in H \cdot a$ so that $\rho_{a^{-1}b}(g_1) = \rho_{a^{-1}b}(g_2)$. Thus $g_1 \cdot (a^{-1} \cdot b) = g_2 \cdot (a^{-1} \cdot b)$. Then

$$g_1 \cdot (a^{-1} \cdot b) \cdot (b^{-1} \cdot a) = g_2 \cdot (a^{-1} \cdot b) \cdot (b^{-1} \cdot a)$$

and $g_1 = g_1 \cdot e = g_2 \cdot e = g_2$ so $\rho_{a^{-1}b}$ is surjective. \square

With this proposition let's us prove the following theorem for finite groups called Lagrange's Theorem.

Theorem 2.1 (Lagrange's Theorem). *Let G be a finite group and H a subgroup. The number of elements in H (denoted $|H|$) divides the number of elements in G (denoted $|G|$).*

Proof. Consider the equivalence relation congruence modulo H . Since the right cosets form a set of equivalence classes for this equivalence relation, they form a partition of G . As such, we can find a finite list of elements $\{g_1, g_2, \dots, g_m\}$ so that $G = \bigcup_{i=1}^m H \cdot g_i$ and $H \cdot g_i \cap H \cdot g_j = \emptyset$ when $i \neq j$. So

$$|G| = \sum_{i=1}^m |H \cdot g_i|.$$

However, Proposition 2.4 shows that $|H \cdot g_i| = |H \cdot e|$ for all i and $H \cdot e = H$. Thus $|G| = m|H|$ and we see $|H|$ divides $|G|$. \square

Finally, let us introduce the notion of index for a subgroup.

Definition 2.6. *Let G be a group, $H \subset G$ a subgroup, and G/H the set of left cosets for G modulo H . If $|G/H|$ is a finite set, we call H a finite index subset of G and define a quantity $[G : H] = |G/H|$ called the index of H in G . If G/H is an infinite set, we say that H has infinite index in G .*

Example 2.4. *Consider the following example of groups with subgroups of both finite and infinite index.*

- a. *Let G be the group of integers with the operation addition $(\mathbb{Z}, +)$. Let $H = \{3x \mid x \in \mathbb{Z}\}$ be the subgroup of multiples of 3. Then H is a finite index subset of G with $[G : H] = 3$.*
- b. *Let G be the group of real numbers with the operation addition $(\mathbb{R}, +)$ and let $H = \mathbb{Z}$ be the group of the integers. Then H is an infinite index subgroup of G .*

3. HOMOMORPHISMS AND QUOTIENT GROUPS

In this section, we aim to define the concept of group homomorphism and quotient groups. Because we will be considering groups with possibly different operations, we will now suppress the \cdot notation. So for a group G and elements $a, b \in G$, we will simply write ab in lieu of $a \cdot b$. Similarly, for a subgroup H of G and an element $g \in G$, we let Hg rather than $H \cdot g$ denote the right coset of H containing g . We will use an identical convention for right cosets.

The main idea behind a homomorphism of groups is that it is a function between groups that respects the structure of both the groups. One can remember this by noting that "homo" means "same" and "morph" means "shape".

Definition 3.1. Let G and H be groups and let $f : G \rightarrow H$ be a function. We call f a homomorphism from G to H if for any $a, b \in G$, we have $f(ab) = f(a)f(b)$.

For readers familiar with linear algebra, one can think of this as the group theory analogue to linear transformations. A vector space V over the real numbers \mathbb{R} is a set where we have an addition operation and a scaling operation with the following two conditions.

- (i) For any $v, v' \in V$, we have $v + v' \in V$.
- (ii) For any $v \in V$ and $a \in \mathbb{R}$, we have $a \cdot v \in V$.

A linear transformation $T : V \rightarrow W$ between real vector spaces V and W is a function having the following related properties.

- (i) For any $v, v' \in V$, we have $T(v + v') = T(v) + T(v')$.
- (ii) For any $v \in V$ and $a \in \mathbb{R}$, we have $T(a \cdot v) = a \cdot T(v)$.

So linear transformations respect the structure of both vector spaces. As such, linear transformations of vector spaces can be thought of as homomorphisms of vector spaces.

Let us prove some results about homomorphisms of groups.

Lemma 3.1. Let G and H be groups and $f : G \rightarrow H$ be a homomorphism. Further, let e_G be the identity element of G and e_H the identity element of H . Then we get the following equalities.

- (i) $f(e_G) = e_H$.
- (ii) For any $g \in G$, $f(g^{-1}) = f(g)^{-1}$.

Proof. To prove (i) consider that $e_G e_G = e_G$ since it is the identity for G . Thus

$$f(e_G) = f(e_G e_G) = f(e_G)f(e_G).$$

But $f(e_G) \in H$ as group, so there exists an inverse element $f(e_G)^{-1} \in H$. Thus

$$e_H = f(e_G)^{-1} f(e_G) = f(e_G)^{-1} f(e_G) f(e_G) = e_H f(e_G) = f(e_G).$$

To prove (ii), let $g \in G$. Since G is a group, g has an inverse g^{-1} so that $g g^{-1} = g^{-1} g = e_G$. Thus

$$e_H = f(e_G) = \begin{cases} f(g^{-1}g) = f(g^{-1})f(g) \\ f(gg^{-1}) = f(g)f(g^{-1}) \end{cases},$$

so $f(g^{-1})$ is an inverse of $f(g)$ in H . However, group inverses are unique so $f(g^{-1}) = f(g)^{-1}$. \square

Now let us recall a definition from linear algebra that we can adapt to group homomorphisms. For a linear transformation $T : V \rightarrow W$, we defined a set $\ker(T) = \{v \in V \mid T(v) = 0\}$, called the kernel of T , that gave us a subspace of V . With this in mind, let us define an analogue for group homomorphisms.

Definition 3.2. Let G and H be groups and let e_G and e_H be their respective identity elements. For any homomorphism $f : G \rightarrow H$, we define a set

$$\ker(f) = \{g \in G \mid f(g) = e_H\}$$

called the kernel of f .

Now we prove the following proposition.

Proposition 3.1. Let G and H be groups with e_G and e_H their respective identity elements. For any group homomorphism $f : G \rightarrow H$, $\ker(f)$ is a subgroup of G .

Proof. Notice that Lemma 3.1 shows that $f(e_G) = e_H$ so that $e_G \in \ker(f)$ so $\ker(f) \neq \emptyset$.

Next, let us show that $\ker(f)$ is closed under the group operation on G . Let $a, b \in \ker(f)$, then

$$f(ab) = f(a)f(b) = e_H e_H = e_H$$

so $ab \in \ker(f)$. So $\ker(f)$ is closed under the group operation for G .

Finally, let $a \in \ker(f)$ and consider $f(a^{-1})$. By Lemma 3.1, we see that $f(a^{-1}) = f(a)^{-1}$. However $f(a) = e_H$ so $f(a)^{-1} = e_H^{-1} = e_H$. So $f(a^{-1}) = e_H$ and $a^{-1} \in \ker(f)$.

So $\ker(f)$ is a non-empty set satisfying the subgroup axioms. □

We would also like to consider homomorphisms that satisfy certain general properties of functions. In particular, we have the following definition.

Definition 3.3. Let G and H be groups and $f : G \rightarrow H$ be a group homomorphism. We have the following definitions for homomorphisms that are injective, surjective, and bijective.

- If f is injective, we call f a monomorphism.
- If f is surjective, we call f an epimorphism.
- If f is bijective, we call f an isomorphism.

As with linear transformations of vector spaces, we can determine whether a group homomorphism is injective by studying the kernel.

Lemma 3.2. Let G and H be groups and $f : G \rightarrow H$ be a group homomorphism. Then f is injective (i.e., f is a monomorphism) if and only if $\ker(f) = \{e_G\}$.

Proof. Suppose f is injective. First, by Lemma 3.1, $f(e_G) = e_H$. Therefore, $\{e_G\} \subset \ker(f)$. Let $a \in \ker(f)$, then $f(a) = e_H$. By Proposition 3.1, we have that $e_G \in \ker(f)$. Thus $f(a) = e_H = f(e_G)$. However, f is injective so $a = e_G$ and $\ker(f) \subset \{e_G\}$. Therefore $\ker(f) = \{e_G\}$.

Now suppose that $\ker(f) = \{e_G\}$ and let $a, b \in G$ such that $f(a) = f(b)$. Then $f(a)f(b)^{-1} = e_H$. But by Lemma 3.1, $f(b)^{-1} = f(b^{-1})$ and since f is a homomorphism

$f(a)f(b^{-1}) = f(ab^{-1})$. So we see that

$$e_H = f(a)f(b)^{-1} = f(ab^{-1})$$

and $ab^{-1} \in \ker(f)$. However $\ker(f) = \{e_G\}$, so $ab^{-1} = e_G$ which shows that $a = b$. So f is injective. \square

Now, let us consider the right and left cosets of the kernel of a homomorphism. Let G and H be groups and $f : G \rightarrow H$ be a homomorphism. Further, let $K = \ker(f)$. For any $a \in G$, consider the right coset $Ka = \{ka \mid k \in K\}$. We would like to show that $Ka = \{g \in G \mid f(g) = f(a)\}$

Suppose that $b \in Ka$, then there exists a $k \in K$ such that $b = ka$. Then

$$f(b) = f(ka) = f(k)f(a) = e_H f(a) = f(a)$$

so $b \in \{g \in G \mid f(g) = f(a)\}$.

Now suppose that $b \in \{g \in G \mid f(g) = f(a)\}$ and consider

$$f(ba^{-1}) = f(b)f(a^{-1}) = f(b)f(a)^{-1} = f(a)f(a)^{-1} = e_H$$

so $ba^{-1} \in K$ or, equivalently, $b \in Ka$.

However, a nearly identical argument shows that the left coset $aK = \{g \in G \mid f(g) = f(a)\}$. So we find that for any $a \in G$, the sets $aK = Ka$ as sets. Note that we are not claiming that for every $k \in K$, $ak = ka$. Rather for these sets to be equal, we are saying that for any $k \in K$, there exists $k' \in K$ so that $ak = k'a$. Subgroups such as these are of particular importance.

Definition 3.4. Let G be a group and K a subgroup of G such that for every $g \in G$, we have $gK = Kg$. We call K a normal subgroup of G .

We notice the condition that $gk = k'g$ is equivalent to $gkg^{-1} = k'$ or $gkg^{-1} \in K$. So consider the following lemma.

Lemma 3.3. Let G be a group and H be a subgroup of G . Let us define a set $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$. Then gHg^{-1} is a subgroup of G .

Proof. Let us first verify that gHg^{-1} is closed under the group operation on G . Let $a, b \in gHg^{-1}$. Then there exists $h, h' \in H$ so that $a = ghg^{-1}$ and $b = gh'g^{-1}$. So

$$ab = (ghg^{-1})(gh'g^{-1}) = gh(g^{-1}g)hg^{-1} = gheh'g^{-1} = gh'h'g^{-1}.$$

Since H is a subgroup, $hh' \in H$ and $ab \in gHg^{-1}$. So gHg^{-1} is closed under the group operation on G .

Now we only need to show that for any $a \in gHg^{-1}$, $a^{-1} \in gHg^{-1}$. Consider $a \in gHg^{-1}$, then there exists $h \in H$ so that $a = ghg^{-1}$. Thus

$$a^{-1} = (ghg^{-1})^{-1} = (g^{-1})^{-1}h^{-1}g^{-1} = gh^{-1}g^{-1}.$$

Since H is a subgroup, $h^{-1} \in H$ and $a^{-1} \in gHg^{-1}$. \square

For a group G , a subgroup $H \subset G$, and an element $g \in G$, we call the subgroup gHg^{-1} the conjugate subgroup of H by g . So we see that H is a normal subgroup if $gHg^{-1} = H$ for all $g \in G$. Equivalently, H is normal in G if H has no conjugate subgroups in G other than itself.

One can ask why normal subgroups are important. The answer is that they allow us to define a new group as a quotient of a group and a normal subgroup.

Definition 3.5. *Let G be a group, K a normal subgroup, and G/K the set of left cosets for K in G . We can define a binary operation on G/K as $(aK) \cdot (bK) = (ab)K$.*

We should verify that this operation is well-defined. Suppose that $aK = a'K$ and $bK = b'K$. Then $a^{-1}a' \in K$ and $b^{-1}b' \in K$. Consider the product $(b^{-1}a^{-1})(a'b') = b^{-1}(a^{-1}a')b'$. Since K is normal $b^{-1}K = Kb^{-1}$. So for any $k \in K$, there exists $k' \in K$ so that $b^{-1}k = k'b^{-1}$. In particular $a^{-1}a' \in K$, so there exists k' so that $b^{-1}(a^{-1}a') = k'b^{-1}$. Thus,

$$(b^{-1}a^{-1})(a'b') = b^{-1}(a^{-1}a')b' = k'(b^{-1}b').$$

But $(b^{-1}b') \in K$ and since K is a subgroup $k'(b^{-1}b') \in K$. Therefore, $(b^{-1}a^{-1})(a'b') \in K$ and $(ab)K = (a'b')K$. So our multiplication is well defined.

We now consider the following proposition that shows that G/K is a group under coset multiplication.

Proposition 3.2. *Let G be a group, K a normal subgroup, G/K the set of left cosets of K in G , and \cdot the binary operation on G/K that is given by coset multiplication. Then G/K is a group under the operation \cdot .*

Proof. We need only verify the group axioms. First, since the group operation on G is associative, we have that for any $a, b, c \in G$ $a(bc) = (ab)c$. Thus

$$aK \cdot (bK \cdot cK) = aK \cdot (bc)K = (a(bc))K = ((ab)c)K = (ab)K \cdot cK = (aK \cdot bK) \cdot cK$$

for any $a, b, c \in G$. Thus \cdot is an associate product on G/K .

Next let $a \in G$ and consider the coset $eK = K$. Then $aK \cdot eK = (ae)K = aK$ and $eK \cdot aK = (ea)K = aK$. So the coset $K = eK$ is the identity element.

Finally, for any $a \in G$ consider $aK \cdot a^{-1}K = (aa^{-1})K = eK = K$ and $a^{-1}K \cdot aK = (a^{-1}a)K = eK = K$. For every coset aK , we have a coset $a^{-1}K$ that is the inverse of aK .

Thus we have verified all of the group axioms. □

One should note that since K is normal $aK = Ka$ for all $a \in G$. So we could have done the exact same construction for right cosets and gotten the same group. We call G/K the quotient group of G by K . Now we connect quotient groups to group homomorphisms with the following proposition.

Proposition 3.3. *Let G be a group, $K \subset G$ a normal subgroup, G/K the quotient group of G by K , and $\pi : G \rightarrow G/K$ the function $\pi(g) = gK$. Then π is a homomorphism with $\ker(\pi) = K$.*

Proof. Let $g_1, g_2 \in G$ and consider $\pi(g_1g_2) = (g_1g_2)K$. By the definition of the product on G/K , we see $(g_1g_2)K = (g_1K) \cdot (g_2K) = \pi(g_1)\pi(g_2)$. So $\pi(g_1g_2) = \pi(g_1)\pi(g_2)$ for all $g_1, g_2 \in G$. Thus, π is a group homomorphism.

Now let $g \in K$, so $gK = K$. By definition of π , $\pi(g) = gK$, so $\pi(g) = K$. However K is the identity element of G/K , so $g \in \ker(\pi)$. So we see $K \subset \ker(\pi)$.

Now let $g \in \ker(\pi)$. Then $\pi(g) = K$ (since K is the identity element of G/K). By definition of π , $\pi(g) = gK$, so $gK = K$. Thus $g \in K$ and $\ker(\pi) \subset K$.

Thus we have shown that π is a homomorphism and $K = \ker(\pi)$. □

So we see that any normal subgroup is the kernel of a homomorphism to a quotient group. We have also shown that all kernels are normal subgroups.

3.1. Exercises. . Here are some exercises pertaining to material above.

1. Which of the examples of sets with operations in Example 1.1 are groups?
2. Let G be a finite group. Prove the the following statements
 - a. For any $a \in G$, there exists an $n \in \mathbb{N}$ so that $a^n = e$. (Here n may depend on $a \in G$).
 - b. There exists an $N \in \mathbb{N}$ such that for any $a \in G$, $a^N = e$. (Here N is independent of $a \in G$).
3. Let G be a group containing an even number of elements. Show that there exists an element $a \in G$ such that $a \neq e$ and $a^2 = e$.
4. Let G be a group such that for any $a \in G$, we have $a^2 = e$. Show that G is abelian (i.e., G is a commutative group).
5. Let G be a finite group with binary operation \cdot and H a non-empty finite subset of G that is closed under the operation \cdot . Show that H is a subgroup.
6. Let G be the set of bijections of the set $\{1, 2, 3\}$ with the group operation that is composition. Let σ_0 be the identity bijection in G (i.e., $\sigma_0(k) = k$ for all $k \in \{1, 2, 3\}$) and let $\sigma_{(12)}, \sigma_{(123)} \in G$ be the following elements

$$\sigma_{(12)}(k) = \begin{cases} 2 & \text{if } k = 1 \\ 1 & \text{if } k = 2 \\ 3 & \text{if } k = 3 \end{cases} \quad \text{and} \quad \sigma_{(123)}(k) = \begin{cases} 2 & \text{if } k = 1 \\ 3 & \text{if } k = 2 \\ 1 & \text{if } k = 3 \end{cases} .$$

- a. Show that the set $H = \{\sigma_0, \sigma_{(12)}\}$ is a subgroup of G .
- b. Show that $H \cdot \sigma_{(123)} \neq \sigma_{(123)} \cdot H$.
7. Let G be a group with subgroups H and K . Show that $H \cap K$ is a subgroup of G .
8. Let G be a finite group and $a \in G$. Show that $\text{ord}(a)$ divides $|G|$.

9. Let G be a finite group, K a normal subgroup, and G/K the quotient group of G by K . Show that G/K is finite and $|G| = |K||G/K|$.
10. Let G be a group and H a finite index subgroup with $[G : H] = 2$. Show that H is a normal subgroup of G .
11. Let G be a group, H an abelian group, and $f : G \rightarrow H$ a group homomorphism.
 - a. Show that for any two elements $g_1, g_2 \in G$ that the element $g_1g_2g_1^{-1}g_2^{-1} \in \ker(f)$.
 - b. Show that G is abelian if and only if $g_1g_2g_1^{-1}g_2^{-1} = e_G$ for any two elements $g_1, g_2 \in G$.
 - c. Show that if G is not abelian, then f must not be injective.
12. Let G be a group and consider the following exercises regarding various subsets of G .
 - a. Let $a \in G$ and $C_G(a) = \{g \in G \mid ga = ag\}$ (this set is called the centralizer of a in G). Show that $C_G(a)$ is a subgroup of G .
 - b. Let $H \subset G$ be a subgroup of G and $N_G(H) = \{g \in G \mid \{ghg^{-1} \mid h \in H\} = H\}$ (this set is called the normalizer of H in G). Show that $N_G(H)$ is a subgroup of G .
 - c. Let $Z = \{z \in G \mid zg = gz \text{ for all } g \in G\}$ (this set is called the center of G). Show that Z is a normal subgroup of G .
13. Let G be a group, $H \subset G$ a subgroup, and $N \subset G$ a normal subgroup. Let $HN = \{hn \mid h \in H, n \in N\}$, show that HN is a subgroup of G . If H is also normal, show HN is a normal subgroup. Is HN a subgroup if neither H or N is normal?
14. Let n, d , and k be positive integers with $n = dk$. Further let \mathbb{Z}/n and \mathbb{Z}/d be the group of equivalence classes of the integers mod n and d respectively under coset addition. Consider the function $f : \mathbb{Z}/d \rightarrow \mathbb{Z}/n$ given by $f([a]) = [ka]$. Show that f is an injective homomorphism.