0.1 Groups

Before we give the definition of a group, the reader might appreciate some motivation behind what a group is trying to capture. The axioms of a group are in the sense, all that you need for the equation $ax = b$ to have a unique solution. Of course, the reader may also be motivated by other examples, such as the rotations and reflections of a square, or other sorts of symmetries.

Definition 0.1 (Group). A group is a set G with a binary operation $\cdot : G \times G \to G$ such that

1. **(Associativity)** For all $x, y, z \in G$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
2. **(Identity)** There exists $e \in G$ such that for all $g \in G$, $e \cdot g = g \cdot e = g$.
3. **(Inverses)** For all $g \in G$, there exists $h \in G$ such that $g \cdot h = h \cdot g = e$.

Note that the order of properties 2 and 3 do matter. We cannot write property 3 before property 2. A remark about how the identity and inverse is written is order. We do need the fact that $e \cdot g = g \cdot e = g$, since if only $e \cdot g = g$ and $h \cdot g = e$ are given, this may not determine a group. [Jac09]

To make notation clearer, we shall write gh for $g \cdot h$. We may sometimes use addition to denote the group operation as well, writing $g + h$. Additionally, because of associativity, we can drop any brackets. This means that there is no ambiguity about what xyz is. Recall that when adding numbers, $(2 + 3 + 4) + 5 = (2 + 3) + (4 + 5)$. Of course, it follows that you can drop the brackets for finitely many elements.

Exercise 0.2. Let G be a group. Prove that associativity holds for finitely many elements $x_1, \ldots, x_n \in G$. For example, $(xy)(zw) = x((yz)w)$. (c.f. [DF04, Prop 1, p. 19])

Additionally, if we can commute elements under the group operation, the group is called Abelian. This is named in honor of the Norwegian mathematician Niels Abel, who contributed greatly to the development of group theory.

Definition 0.3 (Abelian group). Let G be a group. Then G is Abelian if for every $g, h \in G$, we have $gh = hg$.

Exercise 0.4. Show that the condition that $eg = ge = g$ (and similarly for inverses) can be replaced with simply $eg = g$ if we say that G is abelian.

At this point, the reader might be wondering whether the existence of identities and inverses necessarily guarantees that they are unique. This is indeed true.

Theorem 0.5 (Uniqueness of identity and inverses). Let G be a group. Then, the following are true.

1. The identity of G is unique.
2. If $g \in G$ has an inverse h, then it is unique.

Proof. (1) Let $e, e' \in G$ and suppose both e, e' are identities. Keeping in mind that they satisfy the property of being an identity, we have,

$$e = ee' = e'e = e'.$$

(2) Suppose h, h' are both inverses of g. Again keeping in mind that h, h' both satisfy the properties of being an inverse for g.

$$h = h(h'g) = h(gh') = (hg)h' = h'.$$

□

Henceforth we shall talk about "the" identity of a group, and "the" inverse of an element. If not explicitly mentioned, the identity of a group G will be denoted e. Additionally, if $g \in G$, then we shall denote the inverse of g by g^{-1}.

Let us now see some examples of groups.

Example 0.6 (Integers). The integers form a group under usual addition. Clearly the identity under addition is 0. Inverses are obvious. //

We trust that the reader is mathematically mature enough to not be confused by the usage of + for the group operation.

Example 0.7. The set of integers under usual multiplication is *not* a group. There is no multiplicative inverse for 2. //

Example 0.8 (Vector spaces)**.** Let V be a vector space over $\mathbb{R}$. Then V is a group under vector addition. //

Example 0.9 (General linear group)**.** Let $\mathbb{GL}_n(\mathbb{R})$ denote the set of $n \times n$ invertible matrices with real entries. Then this set is a group under the operation of matrix multiplication. //

Example 0.10 (Special linear group)**.** Let $\mathbb{SL}_n(\mathbb{R})$ denote the set of $n \times n$ matrices with real entries and determinant 1. This set forms a group under the operation of matrix multiplication. //

Example 0.11 (Dihedral group D_4)**.** Consider a square. We shall label the square's vertices in a counterclockwise direction. Let r denote a clockwise rotation and let s denote reflection on the vertical axis. The operation in this group shall be defined by applying successive transformations. So for instance, r^2 would be rotating clockwise, then rotating clockwise again. If we do instead rs, we would first flip the square on the vertical axis, then rotate the square clockwise. (The reader is highly encouraged to grab a piece of paper and do these operations for themselves.) The set of all these transformations forms a group under the operation of "doing a transformation after another". Of course, we need to add in the rotation by 0 degrees, which is the identity.

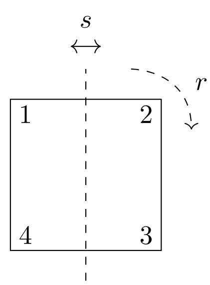

Figure 1: A square with some labels to help you visualize the dihedral group D_4

For better visuals, see [Gal20, Fig. 1.1, p. 28].

We can easily generalize this example. Given an n sided regular polygon, we can again let r denote rotation by $360/n$ degrees, and we let s denote reflection about some axis. The general construction of this is called the **dihedral group of an n-sided polygon** D_n. We also sometimes call this the dihedral group of order $2n$.

//

Example 0.12. The real numbers form a group under usual addition. The real numbers without 0 form another group under usual multiplication. //

Note that the previous example illustrates an important point. *The same (similar) set can be a different group when the operation is replaced.* This tells us that to specify a group, we need both the set, as well as the group operation. However, if the operation does not matter, or it is clear from context, we shall simply say that G is a group.

Exercise 0.13. Verify that all of the above examples which are claimed to be groups are indeed groups.

Exercise 0.14. Groups can be finite or infinite in size. Identify which of the above groups are finite and which are not.

Exercise 0.15. Not every group is Abelian. Identify which of the groups above are abelian and which are not.

We state a few more properties of groups. Many of the proofs below invoke the uniqueness of inverses, and the reader should keep this in mind as they read the proof.

Theorem 0.16. Let G be a group. Then, the following are true.

1. **(Generalized associativity)** For any $x_1, \dots, x_n \in G$, the value of $x_1 \cdots x_n$ is independent of how it is bracketed.
2. If $g \in G$, then $\left(g^{-1}\right)^{-1} = g$.
3. **(Socks-shoes property)** If $g, h \in G$, then $(gh)^{-1} = h^{-1}g^{-1}$.
4. **(Cancellation)** Let $g, h, h' \in G$. If $gh = gh'$ then $h = h'$. This is called left cancellation. Additionally, if $hg = h'g$, then $h = h'$. This is called right cancellation.

Proof. (1) is Exercise 0.2.

(2) Write

$$\left(g^{-1}\right)\left(g^{-1}\right)^{-1} = e = g^{-1}g.$$

Then the result follows by uniqueness of inverses.

(3)

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

(4) Exercise for reader. □

To ensure that the reader is adequately familiar with the techniques of the proof above, we include the following simple exercises.

Exercise 0.17. Prove part (4) of Theorem 0.16.

Exercise 0.18. Prove part 1-2 Theorem 0.16 again using Theorem 0.16 part (4).

Exercise 0.19. We called part 3 of Theorem 0.16 the socks-shoes property. Explain why we gave it that name.

At this point, it seems fitting to introduce an infinite family of examples of groups. We will be studying them closely in **??**.

Example 0.20 (Integers mod n)**.** Let $\mathbb{Z}_n = \{0, \dots, n-1\}$ be equipped with the operation of addition modulo n. That is, we define $+$ on $\mathbb{Z}_n$ to be given by $a + b = (a + b) \mod n$. This is called the *group of integers modulo* n, or alternatively *the cyclic group of order* n. We will soon see what this means. //

Throughout the section on group theory, whenever we write $\mathbb{Z}_n$, we are referring to the group of integers under addition modulo n.

Exercise 0.21. Verify that $\mathbb{Z}_n$ with the operation as defined above is indeed a group.

Example 0.22 (Group of units)**.** Let $U(n)$ denote the set of all nonnegative integers $k \leq n$ such that $\gcd(k, n) = 1$. Then $U(n)$ is a group under the operation of multiplication modulo n. That is, if $a, b \in U(n)$, $ab = a \cdot b \mod n$. //

We now give as an example, an infinite family of non abelian groups. This family of groups is important because in a sense, they contain every other finite group.

Example 0.23 (Symmetric groups)**.** Let $S = \{1, \dots, n\}$. Then consider the set of all permutations of S (bijective functions from S to S). We shall call this set S_n, which stands for *symmetric group on* n *things*. This set is a group under function composition. //

Exercise 0.24. Prove that S_n is a group under function composition.

We will not have the reader prove that this is non abelian yet, until we develop more tools in **??**.

It is common to perform repeated multiplication in groups with a single element. Nobody wants to write $gggggggg$. How shall we clean this up? Notation. Recall from elementary school that a^n is the act of multiplying a by itself n times. To better leverage our intuitions from these times, we can define similar notation for repeated multiplication in groups. Let G be a group and $g \in G$. We shall write

$$g^n = \underbrace{gg\cdots g}_{n \text{ times}}$$

to mean g multiplied by itself n times. If the group operation is denoted by addition, we write

$$n \cdot g = \underbrace{g + g + \cdots + g}_{n \text{ times}}$$

to mean g added to itself n times. In either way, these are the same concept. This does leave the small problem of leaving multiplying g by itself 0 times undefined. What should g multiplied by itself no times be? Drawing back from the intuition of exponentiation from elementary school, we may recall that raising a real number to the 0th power yields 1. But what is 1? Well, it is the multiplicative identity of the real numbers. This suggests a similar definition for groups. Thus, g^0 (or $0 \cdot g$) is *defined* to be e, the group identity.

Good notation should leverage existing intuitions and feel natural, and easy to work with. At this point, the reader is probably wondering whether this notation really does satisfy the usual properties of exponentiation. It turns out that these usual properties of exponentiation really only depend on associativity. Thus, we have the fact that $a^{n+m} = a^n \cdot a^m$. In Exercise 0.30, we shall see that $a^i a^j = a^{i+j}$ as well, thus the familiar intutition of repeated multiplication or addition of numbers carries over.

Example 0.25. Let G be the set of real numbers under multiplication, and consider the real number π. Notice that $\pi^0 = 1$, under usual exponentiation and our definition, and $\pi^n = \pi \cdots \pi$ n times, which again, agrees with the usual definition. //

> **Definition 0.26** (Order of an element)**.** If $g \in G$, then we denote $|g|$ to be the *least positive integer* n such that $g^n = e$.

Example 0.27. In the group $\{1, -1, i, -i\}$ under the operation of complex multiplication, the element i has order 4 as $i^4 = -1$ and 4 is the least positive integer for which this holds true for. //

Example 0.28. Let $G = \mathbb{Z}_6$. We leave the reader to calculate the order of every element. Note that the only possible orders of elements in this group are 1,2,3 and 6. We will see why this is true in **??**. //

We shall also define the order of a group.

> **Definition 0.29** (Order of a group)**.** Let G be a group. Then $|G|$ is the number of elements in G if G is finite, or if G is infinite, it is ∞.

At this point, the reader may be wondering why the abuse of notation. Is this abuse of notation even justified? Or will it lead to confusion down the road? Unfortunately, at this stage, we aren't able to provide a good answer to why this notational abuse is justified. However, we promise the reader that in later chapters, such as **??**, we will justify this.

We close off this section with some exercises and problems.

0.1.1 Problems

Exercise 0.30 (Power notation)**.**

1. Prove that $a^{i+j} = a^i a^j$ for all nonnegative integers i, j.
2. Prove that $a^{ij} = (a^i)^j$ for all nonnegative integers i, j.
3. Prove that $a^{-i} = (a^i)^{-1}$.
4. Prove that $a^{i+j} = a^i a^j$ and $a^{ij} = (a^i)^j$ for all integers i, j.

Exercise 0.31 (Order of an element is the same as the order of its inverse)**.** Show that $|a| = \left|a^{-1}\right|$

Exercise 0.32 (Divisors and orders)**.** Let G be a group, $a \in G$ and let $|a| = n$. Let d be a divisor of n. Prove that $\left|a^d\right| = n/d$.

Problem 0.1. Let G be a group and $a, b \in G$. Prove that $\left|aba^{-1}\right| = |b|$. Now show that $|ab| = |ba|$.

Problem 0.2. Let G be a group. Prove that if for every $g \in G$, we have $g^2 = e$, then G is Abelian.

Problem 0.3. Let S be a set with an associative and commutative binary operation $\cdot$ on it, with the additional property that given any $a, b \in S$, there exists $c \in S$ such that, $a \cdot c = b$. Prove that for all $x, y, z \in S$, if $x \cdot z = y \cdot z$, then $x = y$.

Problem 0.4. Suppose that G is a group such that $(ab)^i = a^i b^i$ for 3 consecutive integers i, for all $a, b \in G$. Prove that G is abelian.

Problem 0.5. Let G be a nonempty finite set that is closed under an associative binary operation such that for every $x, y, z \in G$,

1. **(Left cancellation)** if $xy = xz$ then $y = z$, and;
2. **(Right cancellation)** if $yx = zx$ then $y = z$.

Prove that G is a group. Find an example that if one of the cancellation laws were not assumed, that G is not a group. (Find an example without left cancellation and without right cancellation)

Problem 0.6 (Fundamental Group)**.** This exercise is best done with knowledge of topology.

Let X be a nonempty path-connected space, and $x_0 \in X$ be a point. Recall that a *loop* in X is a continuous map $p : [0, 1] \to X$ such that $p(0) = p(1)$.

0.2 Subgroups

In the previous section, the reader may have observed that some groups are seemingly contained in other groups. For example, the special linear group is a subset of the general linear group. The notion of a substructure is a very common theme throughout the study of abstract algebra. Before we give the definition of a subgroup, the reader should keep the idea of a subgroup being a smaller group contained in a bigger group in mind.

Definition 0.33 (Subgroup)**.** Let G be a group. A subset $H \subseteq G$ is a **subgroup** of G if the following properties hold under the operation of G.

1. The identity of G is in H.
2. For all $x, y \in H$, $xy \in H$.
3. For all $x \in H$, $x^{-1} \in H$.

This tells us that if we restrict the operation of G to H, then H is still a group. We shall notate the situation of H being a subgroup of G by $H \leq G$. If H is a *proper* subgroup of G, it means that H is a proper subset of G, and we denote this by $H < G$.

Before we continue, we shall give some examples of subgroups.
Example 0.34. Any group is a subgroup of itself. //
Example 0.35 (Trivial example)**.** Let $G = \mathbb{Z}$ under usual addition and $H = \{ 0 \}$. Then H is a subgroup of G. In general, if G is any group and $H = \{ e \}$ then H is a subgroup of G, and it is called the *trivial subgroup of* G. //

A quick remark is that if G is a group with a single element, then G is called the *trivial group*.
Example 0.36 (Roots of unity)**.** Let $G = \mathbb{C} \setminus \{ 0 \}$ with the operation of multiplication and let $H = \{ 1, -1, i, -i \}$. Then H is a proper subgroup of G. //
Example 0.37. Let $G = \mathbb{Z}_5$. Then the *only* subgroups of G are $\{ 0 \}$ and G itself. //

We emphasize that $\mathbb{Z}_5$ really does only have 2 subgroups. The reason for this will be seen in the next section.

Note that some authors will define a subgroup of G to be a subset $H \subseteq G$ such that H is a group under the operation of G. This definition is equivalent to the one above. Note that restricting an associative binary operator on G to a subset of it still leaves it associative. The reader should verify this for themselves.

We now give some equivalent formulation of the definition of a subgroup in the form of a theorem. These are often called the subgroup tests (c.f. [Gal20]).

Theorem 0.38 (Subgroup tests)**.** Let G be a group and $H \subseteq G$. Then, the following are equivalent.

1. H is a subgroup of G.
2. H is nonempty, for all $x, y \in H$ we have $xy \in H$. For all $x \in H$ we have $x^{-1} \in H$.
3. H is nonempty, and for all $x, y \in H$, we have $xy^{-1} \in H$.

Proof. We will not insult the reader's intelligence by providing a proof. □

Exercise 0.39. Prove Theorem 0.38.

Readers who have had linear algebra will recall that to test whether U is a subspace of a vector space V, we would check that U is nonempty, if $x + y \in U$ and $\lambda x \in U$ for some scalar λ. This will actually suffice to show that U is a subgroup of V has well.

In general, to test whether something is a subgroup, we can apply the following framework. Suppose G is a group and $H \subseteq G$ with some property P. We first check that H is nonempty. This usually involves verifying that $e \in G$ satisifies the property P. Next, we show that if x, y satisfy the property P, then xy^{-1} also satisfies the property P. We can then apply the subgroup test to conclude that H is a subgroup of G.

The reader is probably wondering why checking for existence of inverses is needed. After all, in linear algebra, when checking that U is a subspace, we didn't need to check that the additive inverse of $u \in U$, $-u$ is in U. This is because this step was completed when we checked that U is closed under scalar multiplication. However, with groups, this is not sufficient.

Example 0.40 (Why are inverses needed)**.** Consider the set of natural numbers $\mathbb{N} \subseteq \mathbb{Z}$ where $\mathbb{Z}$ is the group of integers under addition. Then $\mathbb{N}$ is nonempty, contains the identity of $\mathbb{Z}$ and is closed under the operation of $\mathbb{Z}$, but does not contain inverses for any $n > 0$. //

However, if H is a *finite* subset of G, it is sufficient to check that H is closed under the operation of G.

Theorem 0.41. Let G be a group and $H \subseteq G$ be a *finite subset* of G. Then, H is a subgroup if and only if for all $x, y \in H$, $xy \in H$.

Proof. A good exercise. □

Exercise 0.42. Prove Theorem 0.41

We now introduce 2 more definitions, the centralizer of an element and the center of a group. These are both subgroups (exercise) and will be used in the future to prove the Sylow Theorems, and some other counting theorems.

Definition 0.43 (Centralizer)**.** Let G be a group and $a \in G$. Then define

$$C(a) = \{ g \in G : ga = ag \} .$$

We call this the **centralizer of** a in G. This is the subgroup of all the elements that commute with a.

Exercise 0.44. Prove that $C(a)$ is a subgroup of G.

Definition 0.45 (Center of a group)**.** Let G be a group. Then define

$$Z(G) = \{ g \in G : \forall x \in G, gx = xg \} .$$

We call this the **center of** G. This is the subgroup of the elements in G that commute with all other elements.

If the group is clear, we will sometimes simply write just C to indicate the center of the group.

Exercise 0.46. Prove that $Z(G)$ is a subgroup of G.

0.2.1 Problems

Exercise 0.47. Let G be a group and H, K be subgroups. Prove that $H \cap K$ is a subgroup of G. Now suppose H_α, $\alpha \in \Lambda$ is an arbitrary family of subgroups. Show that $\bigcap_{\alpha \in \Lambda} H_\alpha$ is a subgroup.

Exercise 0.48. Let G be a group and H, K be subgroups of G. Is $H \cup K$ always a subgroup of G? If so, prove it. If not, find a counterexample.

Exercise 0.49. Let G be an Abelian group and let $g \in G$. Let $n \in \mathbb{Z}$ be a fixed integer. Show that the set $H = \{ x \in G : x^n = e \}$ is a subgroup of G. Is this true if G is not Abelian?

Exercise 0.50. Let G be a group and suppose that for all $x, y, z \in G$, if $xy = yz$ then $x = z$. Prove that G is Abelian.

Exercise 0.51. Let G be a group. Prove that $(ab)^2 = a^2b^2$ if and only if $ab = ba$. Prove that $(ab)^{-2} = b^{-2}a^{-2}$ if and only if $ab = ba$. [Gal20, Ex. 36, Ch 1, p. 56]

Exercise 0.52 (Conjugates)**.** Let G be a group and let $x \in G$. Let H be a subgroup of G. Define $xHx^{-1} = \{ xhx^{-1} : h \in H \}$, which is called the *conjugate of* H *by* x. Show that

1. xHx^{-1} is a subgroup of G,
2. if H is cyclic then so is xHx^{-1},
3. if H is Abelian then so is xHx^{-1}.

We remark that conjugacy is an equivalence relation on G. Specifically, define $x \sim y$ if and only there exists $g \in G$ such that $x = gyg^{-1}$. This exercise is important because we will use this concept to prove the Sylow Theorems.

Exercise 0.53 (Centralizers and conjugates)**.** Let G be a group and let $x \in G$. Show that $g \in C(x)$ if and only if $gxg^{-1} = x$. Conclude that $C(x) = \{ g \in G : gxg^{-1} = x \}$.

Problem 0.7. Prove that no group is the union of 2 proper subgroups. (No cheating and looking this up)

Problem 0.8. Does there exist an infinite group where every element has finite order?

0.3 Direct Products

In the previous section, we have seen groups contained within other groups, in the form of subgroups. Now we turn to the other aspect: building bigger groups from smaller groups.

Definition 0.54 (Direct Product)**.** Let G, H be groups. The **direct product of G and H** is defined to be the set

$$G \times H = \{ (g, h) : g \in G, h \in H \},$$

endowed with the group operation $(g, h)(g', h') = (gg', hh')$.

Recall from linear algebra that given vector spaces V, W, one can form the product of these vector spaces $V \times W$. This is the same notion. Some authors may call this the *external direct product* of groups [Gal20, Ch 8], and denote it with $G \oplus H$. The reader show now attempt the following exercises to gain some familiarity with this definition.
Exercise 0.55. Prove that the direct product of $G \times H$ is a group.
Exercise 0.56. Prove that if G, H are abelian then so is $G \times H$.
Exercise 0.57. Let $g \in G$ and $h \in H$. We shall note that $(g, h) \in G \times H$. Show that (e, h) and (g, e) commute with each other.
Exercise 0.58 (Order of elements in direct products)**.** Let $g \in G$ and $h \in H$, and consider $G \times H$. Prove that $|(g, h)| = \operatorname{lcm}(|g|, |h|)$.

Let us now see some examples of direct products.
Example 0.59. We take $\mathbb{Z}_2 \times \mathbb{Z}_2$. What does this group look like? We can write out the set explicitly, as it is small:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{ (0,0), (0,1), (1,0), (1,1) \}.$$

Although this group is abelian, notice that it is not cyclic. If it were cyclic then it would have an element of order 4, but no such element exists in this group. //
Example 0.60. Take $\mathbb{Z}_2 \times \mathbb{Z}_3$. Again, let us look at what this group looks like.

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{ (0,0), (0,1), (0,2), (1,0), (1,1), (1,2) \}.$$

There are 6 elements in this group. In fact, this group is cyclic! We leave the reader to find which element has order 6. //

A natural question is how do we deal with the product of more than 2 groups. Let's say we have groups G, H, K. There are two ways to think about this direct product: $(G \times H) \times K$ and $G \times (H \times K)$. Are these the same group? It turns out that the answer to this question is yes, but the reader will have to await for the definition of a group isomorphism to be able to prove this fact.

What about the infinite case? Suppose we have for each $n \in \mathbb{N}$, a group G_n. We can define the direct product in the same way as in Definition 0.54. The group operation also follows similarly.
Exercise 0.61. Formulate the definition of a direct product of infinitely many groups. Prove that this definition does indeed define a group.
Exercise 0.62. Is there an infinite group where every element has finite order?

0.4 Homomorphisms and Isomorphisms

One may say that algebra is the study of relations. At a higher level, we can even ask how are 2 groups related to each other.

In mathematics, the theme of a structure preserving transformation is common. You may have seen continuous and differentiable functions in middle school. These functions preserve certain properties of the real numbers. If you've had linear algebra, you might have seen linear transformations. Linear transformations preserve certain properties of vector spaces. We shall now introduce the notion of a group homomorphism, which preserves certain properties of groups.

Definition 0.63 (Group Homomorphism)**.** Let G, H be groups. Then a **(group) homomorphism** is a function $\phi : G \to H$ such that for all $x, y \in G$,

$$\phi(xy) = \phi(x)\phi(y).$$

A **(group) isomorphism** is a group homomorphism that is bijective.

So a homomorphism is a function that preserves group operations. You can call this an operation-preserving map. Additionally, we shall say that G and H are isomorphic, or G is isomorphic to H if there is an isomorphism $\phi : G \to H$.

Definition 0.64 (Group Automorphism)**.** Let G be a group. A **(group) automorphism** is an isomorphism $f : G \to G$.

So a group automorphism is a group isomorphism where the domain and the codomain are the same.

Before we continue, the reader should really appreciate how simple this definition is. With just the simple equation $\phi(xy) = \phi(x)\phi(y)$, we can capture all the algebraic properties we care about. As algebraists, we often talk about two groups being the "same". While they may not be equal as sets, if they are isomorphic, then every algebraic property you could care about is preserved.

Example 0.65 (Linear maps)**.** Let V, W be vector spaces and $T : V \to W$ be linear. Then T is a group homomorphism, when considering V, W as groups (under vector addition). If T is an isomorphism of vector spaces, then it is also necessarily a isomorphism of groups. //

Example 0.66 (Exponential)**.** Let $G = \mathbb{R}$ under addition, and $H = \mathbb{R}^+$, the positive reals, under multiplication. Define $\phi : G \to H$ by $\phi(x) = e^x$, the exponential function. Then, $\phi(x + y) = \phi(x)\phi(y)$ by properties of exponentials. In fact, this is an isomorphism. //

Exercise 0.67. Prove that ϕ as defined above is an isomorphism.

We shall immediately prove some useful properties of homomorphisms.

Theorem 0.68 (Properties of homomorphisms)**.** Let G, H be groups and $\phi : G \to H$ be a group homomorphism. Then, the following are true.

1. $\phi(e) = \overline{e}$. That is, homomorphisms take the group identity to the identity.
2. $\phi(x^n) = \phi(x)^n$, for all $n \in \mathbb{Z}$.
3. If K is a subgroup of G, then $\phi[K]$ is a subgroup of H. Thus, the image of a subgroup is a subgroup.
4. If J is a subgroup of H, then $\phi^{-1}[J]$ is a subgroup of G. Thus, the preimage of a subgroup is a subgroup.
5. If K is a subgroup of G and K is Abelian, $\phi[K]$ is Abelian.

Proof. For property 1,

$$\overline{e}\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e).$$

The result follows by right-cancellation.

Properties 2-5 are exercises. □

Exercise 0.69. Prove property (2) of Theorem 0.68. *Hint: First show it for nonnegative n, then show that* $\phi(g^{-1}) = \phi(g)^{-1}$.

Exercise 0.70. Prove the rest of Theorem 0.68

Exercise 0.71. Let G be a group. The set of automorphisms on a group G is denoted $\mathrm{Aut}(G)$, and this is called the **group of automorphisms on** G.

For $g \in G$, define $\varphi_g : G \to G$ to be the function $\varphi_g(x) = gxg^{-1}$. Let $\mathrm{Inn}(G) = \{ \varphi_g : g \in G \}$. This is called the **inner automorphism group on** G.

1. Prove that $\mathrm{Aut}(G)$ is a group under function composition.
2. Prove that φ_g is an automorphism. Conclude that $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$.

0.4.1 Problems

Exercise 0.72 (Product of groups is commutative)**.** Let G, H be groups. Prove that $G \times H$ is isomorphic to $H \times G$.

Exercise 0.73 (Product of groups is associative)**.** Let G, H, K be groups. Prove that $(G \times H) \times K$ is isomorphic to $G \times (H \times K)$.