Math 103 Notes

Modern Algebra

Summer Session 1 2021
Taught by Professor Kyle Meyer

Table of Contents

1 Review: Equivalence Relations

We will go over topics covered in other courses that will be used in this course. We begin with the topic of equivalence relations.

1.1 Equivalence Relations

Let X be a non-empty set. Then, a **relation** over X is a subset R of $X \times X$. If $(x, y) \in R$, we say that x is R-related to y and write xRy.

So, for these relations, we should think about inequalities equalities, or congruences between integers.

Suppose R is a relation over X. Then:

- R is called **reflexive** if $\forall x \in X$, xRx. That is, every $x \in X$ is related to itself.
- R is called **symmetric** if $\forall x, y \in X$, $xRy \implies yRx$. In other words, if x is related to y, is y related to x?
- R is called **transitive** if $\forall x, y, z \in X$, xRy and yRz implies that xRz.

Definition 1.1: Equivalence Relation

R is called an **equivalence relation** if R is reflexive, symmetric, and transitive.

Remark: An equivalence relation is essentially an equality with respect to a certain measurement. In life, we often measure things or people with respect to properties (for example, scores or ratings). So, when we want to compare things, we pick a certain property and then, *from that point of view*, determine whether these things are equal. In this regard, equivalence relations are exactly equalities.

1.1.1 Example: Relations

Suppose X and Y are two non-empty sets and $f : X \to Y$ is a function. Let $\sim$ be the following relation over X:

$$\forall x_1, x_2 \in X \quad x_1 \sim x_2 \iff f(x_1) = f(x_2)$$

Then, $\sim$ is an equivalence relation[1].

Proof. We determine if an relation is an equivalence relation if it satisfies the three properties mentioned above.

- Reflexivity:
$$\forall x \in X, f(x) = f(x) \implies x \sim x$$
- Symmetric:
$$x_1 \sim x_2 \implies f(x_1) = f(x_2) \implies f(x_2) = f(x_1) \implies x_2 \sim x_1$$
- Transitive: We know that:
$$\forall x_1, x_2 \in X \qquad x_1 \sim x_2 \implies f(x_1) = f(x_2)$$
We also know that:
$$\forall x_2, x_3 \in X \qquad x_2 \sim x_3 \implies f(x_2) = f(x_3)$$
It follows that if $f(x_1) = f(x_2)$ and $f(x_2) = f(x_3)$, then $f(x_1) = f(x_3)$ and thus, $x_1 = x_3$. Namely, $x_1 \sim x_2$ and $x_2 \sim x_3$, then $x_1 \sim x_3$.

[1] Another way of interpreting this statement is as follows: x_1 is in relation to x_2 precisely when $f(x_1) = f(x_2)$. The claim here, then, is that this is an equivalence relation.

It follows that this is an equivalence relation. □

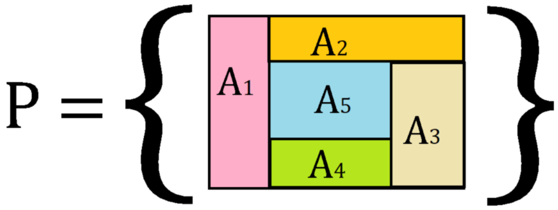
1.2 Equivalence Relation Partitions

Recall that P is called a **partition** of a non-empty set X if:

- Subsets: P consists of non-empty subsets of X.
- Disjointness: $A, B \in P$ and $A \neq B \implies A \cap B = \emptyset$. In other words, the subsets are disjoint.
- Covering: $\forall x \in X$, $\exists A \in P$ such that $x \in A$. In other words, every element in X will be in one of the subsets. Alternatively, $\bigcup_{A \in P} A = X$.

Remark:

- As mentioned, P is a set of sets. For instance, if we have $X = \{1, 2, 3\}$, one possible P is $P = \{\{1\}, \{2, 3\}\}$.
- Below is a visual diagram of what a partition may look like.



$$P = \{A_1, A_2, A_3, A_4, A_5\}$$
$$X = A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5$$

Suppose P is a partition of X. Then, we can get a classification function from X to P:

$$X \to P$$

$$x \mapsto [x]_P$$

Here, $[x]_P$ is the unique element of P which contains x. In other words, if we refer to the above diagram, we can think of $[x]_P$, a set, as one of the sets A_1, A_2, A_3, A_4, or A_5 which contains x. So, we can think of this function as saying that every $x \in X$ belongs to one of the sets $[x]_P$.

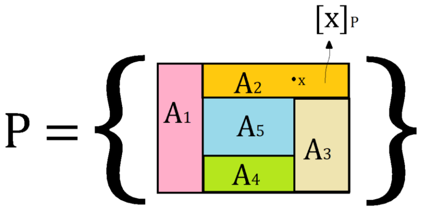
Notice that, because of the **covering** condition, x is contained in some element of P; additionally, because of the **disjointness** condition, x is in an unique element of P (i.e. it is in one of the sets which is in P). So, it follows that the function is well-defined.

By the previous example, $x \sim_P y \iff [x]_P = [y]_P$ is an equivalence relation. So, we obtain the following lemma.

Lemma 1.1

Suppose P is a partition of a non-empty set X. For $x, y \in X$, $x \sim y$ if x and y are in the same element of P. Then, $\sim$ is an equivalence relation.

Remark: Essentially, what this lemma is saying is that if $x \sim y$, then both x and y are in the same set which is in P. In other words, if we refer to the above diagram again, we can think of this situation as saying that both x and y are in one of A_1, A_2, A_3, A_4, or A_5. The diagram below complements the proof.



Proof. For $x \in X$, let $[x]_P$ to be the unique element of P which contains x. So, $x \mapsto [x]_P$ is a function from $X \to P$. By the previous example, $x \sim y \iff [x]_p = [y]_p$ is an equivalence relation over X. Notice that this means $x \sim y$ exactly when x and y are in the same element of P. □

1.3 Equivalence Relation Classes

Now, suppose that $\sim$ is the equivalence relation over a non-empty set X, we can partition X with respect to $\sim$.

For $x \in X$, we let $[x] = \{y \in X \mid y \sim x\}$ (all the elements that are $\sim$-related to x).[2] We call $[x]$ the **equivalence class of x with respect to $\sim$**. When $x \sim y$, we can say that x is equivalent to y with respect to $\sim$.

Proposition. *Suppose $\sim$ is an equivalence relation over a non-empty set X. Then, $\{[x] \mid x \in X\}$ is a partition of X.*

This proposition is essentially asking us to show the following properties:

- Covering: Every element of this set belongs to one of these equivalence classes.
- Disjointness: If we pick two equivalence classes, they do not intersect.

The following lemma follows from this proposition.

Lemma 1.2

$$x \sim y \iff [x] = [y]$$

Proof. We want to show that $[x] = [y] \implies x \sim y$. Recall that the equivalence class of x ($[x]$) and the equivalence class of y ($[y]$) are *sets* and, in particular, we know that $[x]$ consists of all elements that are related to x, including x. Since $\sim$ is reflexive, we know that:

$$x \sim x \implies x \in [x]$$

But, since $[x] = [y]$, then it follows that $x \in [y] \implies x \sim y$. Thus, $[x] = [y] \implies x \sim y$.

To show that $x \sim y \implies [x] = [y]$, we need to show equality of sets $[x] = [y]$. This means that it is necessary and sufficient to prove $[x] \subseteq [y]$ and $[y] \subseteq [x]$.

- To prove $[x] \subseteq [y]$, we let $z \in [x]$. This means that $z \sim x$. However, since $x \sim y$, by transitivity, it follows that $y \sim z$, which implies that $z \in [y]$. Hence, $[x] \subseteq [y]$.
- We note that $x \sim y \implies y \sim x$ by symmetry. Therefore, by the first bullet point, $[y] \subseteq [x]$.

So, it follows that $x \sim y \implies [x] = [y]$. □

Now that we proved the lemma, we can now prove the proposition.

[2] So, it's obvious that $[x] \subseteq X$.

Proof. As mentioned, we need to show that the covering and disjointness properties exist in this partition.

- Covering: $\forall x \in X$, we know that $x \sim x$ by the reflexive property (since $\sim$ is an equivalence relation). Thus, it follows that $x \in [x]$. This means that x is related to x and x is an equivalence class of x, so every element in X belongs to one of the equivalence classes. This implies that the $[x]$ sets are non-empty subsets and cover X.

- Disjointness: Suppose $z \in [x] \cap [y]$ (both equivalence classes are not disjoint). We need to show that they are equal. We know that:

$$z \in [x] \cap [y] \implies z \in [x] \implies z \sim x \implies [z] = [x]$$

$$z \in [x] \cap [y] \implies z \in [y] \implies z \sim y \implies [z] = [y]$$

Where the last two steps came from the lemma. Then, putting these two together, we have:

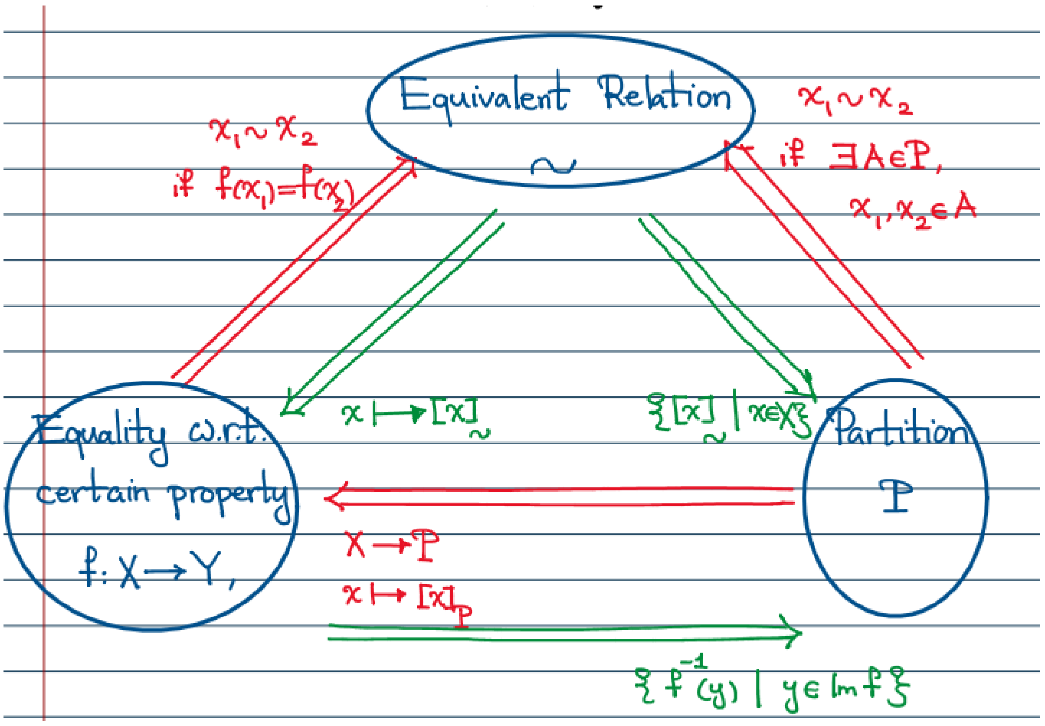
$$[z] = [x] \text{ and } [z] = [y] \implies [x] = [y]$$

We showed that $[x] \cap [y] \neq \emptyset \implies [x] = [y]$, the contrapositive of the disjointness property.

Thus, the proof is complete. □

1.4 Summary

The following diagram provides a brief summary of what we've learned[3]



[3] This diagram was taken from Professor Alireza Salehi Golsefidy's notes.

2 Review: Congruences, Long Division, Modulo

In this section, we discuss congruences, long division, and modulo.

2.1 Congruence

The set of integers is denoted by $\mathbb{Z}$. For $a, b \in \mathbb{Z}$, we say that a divides b and write $a|b$ if $b = ak$ for some $k \in \mathbb{Z}$. Suppose n is a non-zero integer. Then, we say that a is **congruent** to b modulo n and write one of the following if $n|(a-b)$:

$$a \equiv b \pmod{n}$$

$$a \overset{n}{\equiv} b$$

One way to think of this is through a clock. A clock has n numbers (usually 12 numbers). Then, a and b will be on the same spot. For instance, suppose we have 9PM (denoted by the 21st hour). Then, we know that:

$$21 \equiv \boxed{9} \pmod{12}$$

In other words, the hour hand for 9PM will be in the same position as 9AM.

2.2 Congruence and Equivalence Relations

Lemma 2.1

$\overset{n}{\equiv}$ is an equivalence relation over $\mathbb{Z}$.

Proof. Recall that something is an equivalence relation if it satisfies the three properties mentioned in definition 1.1. So, we need to show that $\overset{n}{\equiv}$ satisfies these.

- Reflexive: For every $a \in \mathbb{Z}$, we know that $a - a = 0$ is a multiple of n as $n \times 0 = 0$. Hence, $a \overset{n}{\equiv} a$.
- Symmetric: We have that:

$$\begin{aligned} a \overset{n}{\equiv} b &\implies n|(a-b) \\ &\implies \exists k \in \mathbb{Z}, a - b = nk \\ &\implies b - a = n\underbrace{(-k)}_{\text{In } \mathbb{Z}} \\ &\implies b \overset{n}{\equiv} a \end{aligned}$$

- Transitive: We know that:

$$a \overset{n}{\equiv} b \implies n|(a-b) \implies \exists k \in Z, a - b = nk$$

  We also know that:

$$b \overset{n}{\equiv} c \implies n|(b-c) \implies \exists l \in \mathbb{Z}, b - c = nl$$

  Combining the statements, we now have:

$$(a-b) + (b-c) = nk + nl \implies a - c = n\underbrace{(k+l)}_{\text{In } \mathbb{Z}} \implies a \overset{n}{\equiv} c$$

Thus, $\overset{n}{\equiv}$ is an equivalence class. □

2.3 Congruence and Partitions

As we have seen earlier, every equivalence relation gives us a **partition** and an **equality function**. For $a \in \mathbb{Z}$, the equivalence class of a with respect to $\overset{n}{\equiv}$ is called the **mod-n residue class of** a and is denoted by $[a]_n$. By the results that we proved for equivalence relations, we have that:

- $\{[a]_n \mid a \in \mathbb{Z}\}$ is a partition of $\mathbb{Z}$; and
- $a \overset{n}{\equiv} b \iff [a]_n = [b]_n$

The partition $\{[a]_n \mid a \in \mathbb{Z}\}$ is denoted by $\mathbb{Z}_n$ and it is called **the set of integers modulo** n. Notice that:

$$\begin{aligned} b \in [a]_n &\iff b \overset{n}{\equiv} a \\ &\iff n|(b-a) \\ &\iff \exists k \in \mathbb{Z}, b - a = nk \\ &\iff \exists k \in \mathbb{Z}, b = a + nk \\ &\iff b \in \{a + nk \mid k \in \mathbb{Z}\} \quad \text{Arithmetic Progression} \end{aligned}$$

To understand the set $\mathbb{Z}_n$ better, we recall the well-ordering principle and the long division property of integers. One of the important properties of positive integers is the **well-ordering principle**. This principle can be viewed as an axiom that we assume $\mathbb{Z}$ has.

2.3.1 Well-Ordering Principle

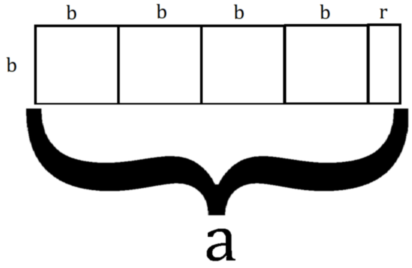
Every non-empty subset of the set $\mathbb{Z}_{\geq 0}$ of non-negative integers has a minimum. Using the well-ordering principle, we can prove the division algorithm.

2.3.2 The Division Algorithm

For every $a \in \mathbb{Z}$, $b \in \mathbb{Z} - \{0\}$, there is a unique pair (q, r) of integers such that:

$$a = bq + r \qquad 0 \leq r \leq |b|$$

To show that this is the case, consider the following diagram:



For positive integers a and b, we can keep "cutting off" the $b \times b$ squares until we are left with either a rectangle smaller than $b \times b$ (i.e. if $r > 0$), or nothing at all (i.e. $r = 0$). In this sense, the number of $b \times b$ squares that we cut off is denoted by q (or k soon). Then, it follows that r is the smallest non-negative integer in the arithmetic progression $a - bk$.

Now, we want to formalize this argument. We begin by defining:

$$\Sigma := [a]_b \cap \mathbb{Z}_{\geq 0} = \{a + bk \mid k \in \mathbb{Z}, a + bk \geq 0\}$$

Here, we denote Σ as a variable, not a summation. We want to use the well-ordering principle on the set Σ to show that it has a minimium (more specifically, that Σ is not empty). Our first claim is:

$$\Sigma \text{ is not empty.}$$

Proof. Since $b \neq 0$, we know that $|b| \geq 1$. Hence, $|b||a| \geq |a|$. Therefore:

$$\underbrace{|b|(|a|+1)+a}_{a \pm b(|a|+1)} \geq |a| + |b| + a \geq |b| > 0$$

It follows that $[a]_b$ has a positive integer. □

By the above claim and the well-ordering principle, Σ has a minimum. Now, suppose r is the minimum of Σ. Then, $r = a - bq$ for some $q \in \mathbb{Z}$. Our second claim is that $r < |b|$.

Proof. Suppose to the contrary that $r \geq |b|$. Then, $r - |b| \geq 0$ and:

$$r - |b| = a - bq - |b| = a - b(q \pm 1)$$

In the above statement, we know that $r = a - bq$, which is in the arithmetic progression. When we subtract $|b|$, we are still in this arithmetic progression since all we're doing is adding or subtracting b; in either case, we're not leaving the arithmetic progression. So, it follows that $r - |b|$ is still in this arithmetic progression.

Hence, $r - |b| \in \Sigma$ (recall that Σ consists of non-negative integers). This is a contradiction as $r - |b|$ is smaller than the minimum r of Σ. □

By this claim, we obtain the existence of the pair (q, r) with:

- $a = bq + r$
- $0 \leq r < |b|$

Now, we want to prove the uniqueness.

Proof. Suppose the pairs (q, r) and (q', r') satisfy the desired properties; that means:

(a) $a = bq + r = bq' + r'$

(b) $0 \leq r, r' \leq |b|$

Then, $b(q - q') = (r' - r)$. Notice that:

$$0 \leq r \implies r' - r \leq r' < |b|$$

$$0 \leq r' \implies r' - r \geq -r > -|b|$$

Then, we have that:

$$|r' - r| < |b|$$

And we obtain that:

$$|r' - r| = |b|(q - q') = |b||q - q'|$$

And, thus:

$$|b||q - q'| < |b|$$

This implies that $|q - q'| < 1$. Since $|q - q'|$ is a non-negative integer less than 1, it is 0. Thus, $q = q'$. It follows that:

$$r' - r = b(q - q') = 0$$

This implies that $r = r'$. Thus, this shows the uniqueness. □

Suppose the pair (q, r) is given in the long division algorithm. Then, q is called the **quotient** of a divided by b and r is called the remainder of a divided by b. Using the long division algorithm, we obtain that $\mathbb{Z}_n$ has n elements.

Proposition. *Suppose n is an integer more than 1. Then:*

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\} \quad |\mathbb{Z}_n| = n$$

Proof. For every $a \in \mathbb{Z}$, by the long division algorithm, there are integers q and r such that $a = nq + r$ and $0 \leq r < n$. □

3 Introduction to Binary Operations and Group Theory

We want to explore the idea behind *algebraic structures.* In particular, we want to explore these structures in more detail compared to earlier courses (either in past college or high school algebra classes).

To do this, we need to think about *what* algebra really is. We might think about solving equations like $x^2 + 3x + 5 = 0$ for x. In particular, what is really happening here?

Well, there are a couple of operations going on. Specifically, we have *addition* and *multiplication.*

$$x \times x + 3 \times x + 5 = 0$$

We now want to examine these operations. Both of these operations $(+, \times)$ take in two numbers and output one number. The question we might have, then, is: how can we can generalize these operations?

3.1 Binary Operations

A **binary operation** is a way of taking in two values and outputting one value. Of course, we might now ask: what can these values be? These values can come from any specific set.

For example, we can consider addition over the integers ($\mathbb{Z}$). The sum of two integers is an integer. Similarly, we could consider multiplication over the integers. Again, the product of two integers is an integer. We could also consider multiplication or addition over the real, rational, or complex numbers.

The idea is that whatever "type" we give our binary operation, we will get that same "type" for our output. To formalize this, we have the following definition:

Definition 3.1: Binary Operation

A binary operation $*$ over a set S is a function mapping $f : S \times S \to S$. For each $(a, b) \in S \times S$, we will denote the element $*((a, b))$ of S by $a * b$.[a]

[a] As a side note, in this class, $a * b$ is equivalent to $f(a, b)$ and $b * a$ is equivalent to $f(b, a)$.

We also introduce the notion of closure, which will be used later.

Definition 3.2: Closure

Let $*$ be a binary operation on S and let H be a subset of S. The subset H is **closed under** $*$ if for all $a, b \in H$ we also have $a * b \in H$. In this case, the binary operation on H given by restricting $*$ to H is the **induced operation** of $*$ on H.

Anything that is "like" addition or multiplication is probably a binary operation. For example, let's consider **matrices**.

- Addition of matrices of a fixed dimension. More specifically, the set of $n \times m$ matrices (here, n and m are fixed positive integers) over the integers, rationals, reals, or complex numbers under matrix addition is a binary operation.

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} + \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{bmatrix} = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} & a_{13} + b_{13} \\ a_{21} + b_{21} & a_{22} + b_{22} & a_{23} + b_{23} \end{bmatrix}$$

- Multiplication of matrices of a fixed dimension. More specifically, the set of $n \times n$ matrices (square matrices). We could also just multiply a $(n \times m)$ matrix by a $(k \times l)$ matrix assuming $m = k$ (otherwise, multiplying these two matrices will result in undefined behavior).

So far, we considered binary operations on infinite sets in which we need some sort of formula to describe (e.g. $f_\cup(A, B) = A \cup B$). Now, if we have a finite set, we could define a binary operation exhaustively by just saying what the binary operation does on every pair of entries.

For example, given the set $S = \{a, b, c, d, e\}$. We can define a binary operation on S with the below (random) table (first entry on left side, second entry on top side).

	a	b	c	d	e
a	a	c	d	d	e
b	b	c	c	b	a
c	d	e	e	b	b
d	a	a	a	c	a
e	b	b	c	c	d

Denote the binary operation to be #.

- What is $c\#d$? The answer is b.
- What is $e\#((a\#b)\#c)$? The answer is d.
- Suppose we have $X\#a = a$. What is X? The answer is $X = a, d$.

3.2 Properties of Binary Operations

What properties could binary operations have?[4]

- **Commutativity:** A binary operation is commutative if the order of the two inputs does not matter. For example, if f is a function corresponding to a binary operation, then:

  $$f(a, b) = f(b, a) \quad \forall a, b \in S$$

  More commonly:

  $$a * b = b * a \quad \forall a, b \in S$$

  For example, addition or multiplication of numbers is commutative. Unions and intersections of sets is also commutative. *However*, matrix multiplication is *not* commutative. Our example above is also not commutative.

- **Associativity:** A binary operation is associative if the order of applying the operation (in a string) does not matter. Specifically:

  $$(a * b) * c = a * (b * c) \quad \forall a, b, c \in S$$

  Which means that we can write $a * b * c$ without ambiguity.

  For example, addition or multiplication of numbers is associative. Addition or multiplication of matrices is also associative. Our example above is not associative.

- **Identity:** A binary operation has a two-sided identity element and a two-sided inverse for every element.

  More specifically, we say that ϵ is a left identity if $f(\epsilon, s) = s$ for all $s \in S$. ϵ is a right identity if $f(s, \epsilon) = s$ for all $s \in S$. Then, ϵ is a two-sided identity if it is both a left identity and right identity.

  For example, 0 is a two-sided identity for addition and 1 is a two-sided identity for multiplication. For matrix addition, the zero-matrix is a two-sided identity. For matrix multiplication, the matrix with

[4] In this course, we will consider binary operations with all the properties excluding commutativity.

ones on the diagonal and zeros everywhere else is the identity element. In our example above, # does not have a left or right identity.

Given a two-sided identity, we can also consider the idea of an inverse. In addition, this is the negative/negation. In multiplication, this is the reciprocal. The additive inverse of x is $-x$. The multiplicative inverse of x is $\frac{1}{x}$ (for all $x \neq 0$).

For a general binary operation $f : S \times S \to S$ with a two-sided identity ϵ, an element $s \in S$ has a two-sided inverse if there exists an element $t \in S$ such that:

$$\underbrace{f(s,t)}_{\text{Right Inverse}} = \overbrace{f(t,s)}^{\text{Left Inverse}} = \epsilon$$

So, a property for binary operations would be for every element to have a two-sided inverse, which requires a two-sided identity element.

Remark: Commutativity does not imply associativity.

3.3 Groups

Of course, the properties of binary operations that were discussed just now are very much applicable in something called **groups**. Simply put, we can say that a group is a set combined with an operation. However, it's a little more complicated than that. The following definition will make that clearer:

Definition 3.3: Group

A group is a set G, closed under a binary operation $*$, satisfying the three properties:

1. Associativity: For all $a, b, c \in G$, we have:

$$(a * b) * c = a * (b * c)$$

2. Identity/Neutral Element: There is an element $\epsilon \in G$ such that for all $x \in G$:

$$\epsilon * x = x * e = x$$

3. Inverse: Corresponding to each $a \in G$, there is an element $a' \in G$ such that:

$$a * a' = a' * a = \epsilon$$

   It is also common to denote the inverse of a as a^{-1} instead of a'.

Remark:

- Notationally, this can be represented by $(G, *)$ or $\langle G, * \rangle$. This is saying that we are pairing a set with a binary operation.
- With regards to how we write the inverse, unless otherwise mentioned, I will use a' and a^{-1} interchangeably.

Important Note

The two most common groups are additive and multiplicative groups. Thus, for some $h \in G$, where $(G, *)$ is a group, it is important to mention what their inverses and identity elements are. As mentioned in the previous section:

Group	Inverse	Identity
Multiplicative $(G, \times)$	$h^{-1} = h' = \frac{1}{h}$	$\epsilon = 1$
Addition $(G, +)$	$h^{-1} = h' = -h$	$\epsilon = 0$

We will discuss these more in the examples.

For any other group, the inverse and identity element depends on how the group and its binary operation is defined. Refer to the definition of a group.

3.4 Basic Properties of Groups

Suppose $(G, *)$ is a group. Then, we note the following properties of groups.

3.4.1 Uniqueness of the Identity.

Could we have two unique two-sided identities in G? The answer is no. The proof is as follows.

Proof. Assume by contradiction that we had ϵ_1 and ϵ_2, both of which are unique two-sided identity elements. Then, we know that $\epsilon_1 * \epsilon_2 = \epsilon_2$ since ϵ_1 is an identity. But, since ϵ_2 is also an identity, then $\epsilon_1 * \epsilon_2 = \epsilon 1$. So, it follows that ϵ_1 and ϵ_2 are not unique; in other words, $\epsilon_1 = \epsilon_2$. □

3.4.2 Uniqueness of Inverses.

If g_1, g_2 are both inverses of some element h, then[5]:

$$g_1 * h = h * g_2 = \epsilon$$

Additionally, we know that:

$$g_1 * (h * g_2) = g_1 * \epsilon = g_1$$

$$(g_1 * h) * g_2 = \epsilon * g_2 = g_2$$

And so it follows that $g_1 = g_2$, thus h will have a unique inverse. To be more concrete, we have the proof.

Proof. We note that $g_1 * h = \epsilon$ and $h * g_2 = \epsilon$. Then:

$$\begin{aligned} g_1 &= g_1 * \epsilon && \epsilon \text{ is the identity element.} \\ &= g_1 * (h * g_2) \\ &= (g_1 * h) * g_2 && \text{Associativity} \\ &= \epsilon * g_2 \\ &= g_2 && \epsilon \text{ is the identity element.} \end{aligned}$$

So, it follows that $g_1 = g_2$. Thus, an element h will have a unique inverse. □

3.4.3 Cancellation.

Suppose we have the expression $g * a = g * b$. This implies that $a = b$. Similarly, the expression $a * g = b * g$ can be simplified to $a = b$.

[5] Here, we denote g_1 as the left-inverse and g_2 is the right-inverse.

Proof. From the definition of a group, we know that an inverse exists for every element in G. Let g^{-1} be the inverse of g. Then:

$$\begin{aligned} g * a = g * b &\implies g^{-1} * (g * a) = g^{-1} * (g * b) \\ &\implies (g^{-1} * g) * a = (g^{-1} * g) * b && \text{Associativity (Prop. 1)} \\ &\implies \epsilon * a = \epsilon * b && \text{Definition of Inverse (Prop. 3)} \\ &\implies a = b && \text{Definition of Identity (Prop. 2)} \end{aligned}$$

The other way is similar. □

Remark: Although $g * a = g * b$, $g * a \neq b * g$ ($g * a$ is not necessarily equal to $b * g$).

3.4.4 Inverse of Operation of Two Elements.

Lemma 3.1

Suppose $(G, *)$ is a group. Then, for every $g, h \in G$, we have:

$$(g * h)^{-1} = h^{-1} * g^{-1}$$

Proof. Since the inverse of an element is unique, it is enough to check that:

$$(g * h) * (h^{-1} * g^{-1}) = (h^{-1} * g^{-1}) * (g * h) = \epsilon$$

So:

$$\begin{aligned} (g * h) * (h^{-1} * g^{-1}) &= g * (h * h^{-1}) * g^{-1} && \text{Associativity (Prop. 1)} \\ &= g * \epsilon * g^{-1} && \text{Definition of Inverse (Prop. 3)} \\ &= (g * \epsilon) * g^{-1} && \text{Associativity (Prop. 1)} \\ &= g * g^{-1} && \text{Definition of Identity (Prop. 2)} \\ &= \epsilon && \text{Identity Element} \end{aligned}$$

Similarly:

$$\begin{aligned} (h^{-1} * g^{-1}) * (g * h) &= h^{-1} * (g^{-1} * g) * h && \text{Associativity (Prop. 1)} \\ &= h^{-1} * \epsilon * h && \text{Definition of Inverse (Prop. 3)} \\ &= (h^{-1} * \epsilon) * h && \text{Associativity (Prop. 1)} \\ &= h^{-1} * h && \text{Definition of Identity (Prop. 2)} \\ &= \epsilon && \text{Identity Element} \end{aligned}$$

So, the proof is complete. □

3.4.5 Inverse of an Inverse.

We should note that, despite using the -1 superscript to denote a multiplicative inverse, this applies to any valid binary operation under a group.

Lemma 3.2

For every $g \in G$, $(g^{-1})^{-1} = g$.

Proof. We have that $g^{-1} * g = \epsilon$. Multiplying both sides by $(g^{-1})^{-1}$ from the left, we now have:

$$((g^{-1})^{-1} * g^{-1}) * g = (g^{-1})^{-1} * \epsilon = (g^{-1})^{-1}$$

Hence, $\epsilon * g = (g^{-1})^{-1}$ and so $g = (g^{-1})^{-1}$. □

3.5 Examples and Non-Examples

Here, we briefly talk about some examples and non-examples of groups.

3.5.1 Example: Addition

For example, the integers under addition are a group. Notationally, this is represented by $(\mathbb{Z}, +)$.

- It's obvious that addition is associative. That is:

$$(a + b) + c = a + (b + c) = a + b + c$$

- The identity element is 0 (we note that $0 \in \mathbb{Z}$). This is because:

$$0 + x = x + 0 = x$$

- The inverse is $-x$. This is because:

$$x + (-x) = (-x) + x = 0$$

We also know that the reals, rationals, or complex numbers under addition are also groups. Notationally, this is represented by $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, or $(\mathbb{C}, +)$, respectively.

3.5.2 Example: Multiplication

Let's now consider multiplication. In particular, multiplication does give a binary operation over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. It's obvious that this is associative and 1 is the two-sided identity element. However, what about the inverse?

- If we try to take the integers under multiplication as a group, then we'll run into problems. This is because the multiplicative inverse of every $\underline{\text{integer}}$ except ±1 is not an integer. For example, if we tried 2, then the multiplicative inverse of 2 is $\frac{1}{2}$. However, $\frac{1}{2} \notin \mathbb{Z}$.

- Rational numbers are closer. For instance, $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$. However, this is only defined if $a \neq 0$. The solution is to remove 0. Define $\mathbb{Q}^*$ to be the non-zero rational numbers (i.e. $\mathbb{Q}^* = \mathbb{Q} - \{0\}$). Then, $(\mathbb{Q}^*, \times)$ is a group. Similarly, we can make $\mathbb{R}$ and $\mathbb{C}$ groups under multiplication by removing 0.

  We note that this change does not affect the closure property because we can only achieve $a \times b = 0$ if and only if $a = 0$ or $b = 0$. Since $a \notin \mathbb{R} - \{0\}$ and $b \notin \mathbb{R} - \{0\}$ (or $\mathbb{Q}$ or $\mathbb{C}$), then we are still closed and our binary operation is still well-defined.

3.5.3 Non-Example: Addition and Multiplication

We mentioned that $(\mathbb{Q}-\{0\}, \times)$, $(\mathbb{R}-\{0\}, \times)$, and $(\mathbb{C}-\{0\}, \times)$ are groups. However, we note that $(\mathbb{Z}-\{0\}, \times)$ and $(\mathbb{Z}_{\geq 0}, +)$ are *not* groups.

- We already briefly explained why $\mathbb{Z}$ under multiplication is not a group. The same idea applies even if we do not include 0; that is, $\mathbb{Z} - \{0\}$ is not a group. We know that $\mathbb{Z} - \{0\}$ has a unique identity element under ×; this element is 1. This is the case because, if ϵ is the identity element of $\mathbb{Z} - \{0\}$ under ×, then by definition:

$$\epsilon \times x = x \times \epsilon = x$$

Which implies that $\epsilon = 1$. We also know that $2 \in \mathbb{Z} - \{0\}$. However, 2 does not have an inverse in $\mathbb{Z} - \{0\}$. To show this, we prove by contradition. If 2 has an inverse in $\mathbb{Z} - \{0\}$, then by definition it follows that for some $a' \in \mathbb{Z} - \{0\}$:

$$2 \times a' = a' \times 2 = \epsilon$$

But, since we know that $\epsilon = 1$, it follows that:

$$2 \times a' = 1$$

But, as the only solution to this is $\frac{1}{2}$, we know that $\frac{1}{2} \notin \mathbb{Z} - \{0\}$. Thus, this is a contradiction. Thus, $\mathbb{Z} - \{0\}$ under multiplication is not a group.

- We know that $\mathbb{Z}_{\geq 0}$ has a unique identity element under addition and that is 0. This is because if ϵ is a unique element of $(\mathbb{Z}_{\geq 0}, +)$, then by definition, we know that:

$$\epsilon + x = x + \epsilon = x$$

It is obvious that $\epsilon = 0$. Now, we want to show that 1 does not have an inverse with respect to addition in $\mathbb{Z}_{\geq 0}$. We'll prove this by contradiction. Suppose 1 does have an inverse. Recall that if 1 does have an inverse, then there is an $x \in \mathbb{Z}_{\geq 0}$ such that for some $a' \in \mathbb{Z}_{\geq 0}$:

$$a' + 1 = 1 + a' = \epsilon$$

But, as $\epsilon = 0$, it follows that:

$$a' + 1 = 0 \iff a' = -1$$

However, we note that $-1 \notin \mathbb{Z}_{\geq 0}$ so this is a contradiction. Thus, $\mathbb{Z}_{\geq 0}$ under addition is not a group.

3.5.4 Example: Addition and Modular Arithmetic

More examples of groups come from modular arithmetic. For instance, consider addition modulo n for some integer n. The set that we're going to be working with is *equivalence classes* modulo n. Recall that[6]:

$$[0]_n = \overline{0} = \{\dots, -3n, -2n, -n, 0, n, 2n, 3n, \dots\}$$
$$[1]_n = \overline{1} = \{\dots, 1-3n, 1-2n, 1-n, 1, 1+n, 1+2n, 1+3n, \dots\}$$
$$[2]_n = \overline{2} = \{\dots, 2-3n, 2-2n, 2-n, 2, 2+n, 2+2n, 2+3n, \dots\}$$
$$\vdots$$
$$[n-1]_n = \overline{n-1} = \{\dots, -n-1, -1, n-1, 2n-1, \dots\}$$

We define our binary operation on the set of equivalence classes $\{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$. What properties does this have? We know that modulo n addition on these equivalence classes is:

- Associative (and commutative).
- It has identity $\overline{0}$. If you have equivalence class $\overline{k}$ (for $k \geq 1$), then the inverse if $\overline{n-k}$ for $1 \leq k \leq n-1$ so that $1 \leq n-k \leq n-1$. We note that:

$$\overline{k} + \overline{n-k} = \overline{0} \pmod{n}$$
$$k + (n-k) = n \in \overline{0}$$

- $\overline{0}$ is the inverse of $\overline{0}$.

We denote this group as $(\mathbb{Z}_n, + \pmod{n})$, where $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$. When it is clear, we can drop the lines.

[6] In general, $[a]_n = \overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \mod n\}$

3.5.5 Example: Multiplication and Modular Arithmetic

Could we do multiplication modulo n as a group? Well, multiplication modulo n on the set $\mathbb{Z}_n$ is an associative, commutative, binary operation with identity $\overline{1}$. However, inverses are potentially an issue ($\overline{0}$ specifically will be an issue). Can we fix this by removing all uninvertible elements?

- Yes, but can we characterize uninvertible elements? Well, the greatest common divisor of two integers is a linear combination. This is useful because we can think about $\gcd(k, n)$ where $k \in \{1, \ldots, n-1\}$. Specifically, if $\gcd(k, n) = 1$, then $ak + bn = 1$ implies that $\overline{a} \times \overline{k} = \overline{1} \pmod{n}$. In other words, k is invertible if $\gcd(n, k) = 1$.
- What if $\gcd(k, n) > 1$? If k was invertible under multiplication modulo n, then $\overline{a}\overline{k} = \overline{1} \pmod{n}$. But, that would mean that there is a linear combinations of a and k that is equal to 1. Thus, k is invertible under multiplication modulo n if and only if $\gcd(k, n) = 1$.

Let's now consider only taking equivalence classes $\overline{k}$ where $\overline{k}$ is relatively prime for n. We will now make the claim that $(U(n), \times \pmod{n})$ is a group. We know that this is associative and commutative, we justified that it has an inverse and an identity element. However, is this still closed?

More formally, why do we have closure of the binary operations? We could think about this in several ways. We could give a proof that the product two integers that are relatively prime to n is still relatively prime to n, or we can think about this more algebraically: namely, we can justify that the product of two invertible equivalence classes is also invertible.

If k_1, k_2 are both invertible, then $k_1 k_2$ is also invertible. Why is this the case? Well, k_1 and k_2 being invertible means that there is some value k_1^{-1} and k_2^{-1}. So, let's consider $k_2^{-1}k_1^{-1}$. We know that:

$$\begin{aligned}(k_1 k_2)\left[k_2^{-1}k_1^{-1}\right] &= k_1\left[k_2 k_2^{-1}\right]k_1^{-1}\\ &= k_1 \epsilon k_1^{-1}\\ &= k_1 k_1^{-1}\\ &= \epsilon\end{aligned}$$

3.6 Exponents of Elements

Suppose $(G, *)$ is a group and $g \in G$. For a positive integer n, we let:

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

For a negative integer n, we let:

$$g^n = \underbrace{(g^{-1}) * \cdots * (g^{-1})}_{-n \text{ times}}$$

Lemma 3.3

For $n, m \in \mathbb{Z}$, $(g^n)^m = g^{nm}$.

Proof. We will consider various cases depending on the signs of m and n.

- Case 1: Suppose m and n are positive. Then:

$$(g^n)^m = \underbrace{g^n * \cdots * g^n}_{m \text{ times}} = \underbrace{\overbrace{(g * \cdots * g)}^{n \text{ times}} * \cdots * \overbrace{(g * \cdots * g)}^{n \text{ times}}}_{m \text{ times}} = \underbrace{g * \cdots * g}_{mn \text{ times}} = g^{mn}$$

  Here, g^n means we need to multiply g n times. But, since we need to multiply g^n m times, it follows that this is simply g^{nm}.

- Case 2: Suppose m is positive and n is negative. Then:

$$(g^n)^m = \underbrace{g^n * \cdots * g^n}_{m \text{ times}} = \underbrace{(\overbrace{g^{-1} * \cdots * g^{-1}}^{-n \text{ times}}) * \cdots * (\overbrace{g^{-1} * \cdots * g^{-1}}^{-n \text{ times}})}_{m \text{ times}} = \underbrace{g^{-1} * \cdots * g^{-1}}_{-mn \text{ times}} = g^{mn}$$

  Here, we note that $mn < 0$.

- Case 3: Suppose m is negative and n is positive. Then:

$$(g^n)^m = \underbrace{(g^n)^{-1} * \cdots * (g^n)^{-1}}_{-m \text{ times}} = \underbrace{(\overbrace{g * \cdots * g}^{n \text{ times}})^{-1} * \cdots * (\overbrace{g * \cdots * g}^{n \text{ times}})^{-1}}_{-m \text{ times}}$$

  We note that, by the previous lemma, $(\underbrace{g * \cdots * g}_{n \text{ times}})^{-1} = \underbrace{g^{-1} * \cdots * g^{-1}}_{n \text{ times}}$. Hence:

$$(g^n)^m = \underbrace{(\overbrace{g^{-1} * \cdots * g^{-1}}^{n \text{ times}}) * \cdots * (\overbrace{g^{-1} * \cdots * g^{-1}}^{n \text{ times}})}_{-m \text{ times}} = \underbrace{g^{-1} * \cdots * g^{-1}}_{-mn \text{ times}} = g^{mn}$$

  Here, we note that $mn < 0$.

- Case 4: Suppose m and n are negative. Since it is easier to work with positive numbers, let $m = -r$ and $n = -s$ where $r, s > 0$. Then, we have to show that $(g^{-r})^{-s} = g^{rs}$. By definition, we know that $g^{-r} = \underbrace{g^{-1} * \cdots * g^{-1}}_{r \text{ times}}$. Hence, $(g^{-r})^{-s} = [(g^{-1})^r]^{-s}$. By the case where $n > 0$ and $m < 0$, we deduce that $(x^r)^{-s} = x^{-rs}$. Therefore:

$$(g^{-r})^{-s} = (g^{-1})^{-rs} = \underbrace{(g^{-1})^{-1} * \cdots * (g^{-1})^{-1}}_{rs \text{ times}} = \underbrace{g * \cdots * g}_{rs \text{ times}} = g^{rs}$$

- Case 5: Suppose $m = 0$. Since $m = mn = 0$, it follows that:

$$(g^n)^m = \epsilon$$

$$g^{nm} = \epsilon$$

- Case 6: Suppose $n = 0$. By the same reasoning as case 5, we have that $n = mn = 0$. So:

$$(g^n)^m = \epsilon^m = \epsilon$$

$$g^{mn} = \epsilon$$

Here, we notice that $\epsilon * \cdots * \epsilon = \epsilon$ and $\epsilon^{-1} = \epsilon$, and so $\epsilon^m = \epsilon$. So, we showed that $(g^n)^m = g^{mn}$ for every $m, n \in \mathbb{Z}$. □

Important Note

- When we are working with an multiplicative group $(G, \times)$, then g^n means:

$$g^n = \begin{cases} \underbrace{g \times \cdots \times g}_{n \text{ times}} & n > 0 \\ 1 & n = 0 \\ \underbrace{\frac{1}{g} \times \cdots \times \frac{1}{g}}_{-n \text{ times}} & n < 0 \end{cases}$$

- When we are working with an additive group $(G, +)$, instead of writing g^n, we write ng. So, in $(G, +)$:

$$ng = \begin{cases} \underbrace{g + \cdots + g}_{n \text{ times}} & n > 0 \\ 0 & n = 0 \\ \underbrace{(-g) + \cdots + (-g)}_{-n \text{ times}} & n < 0 \end{cases}$$

So, instead of writing $(g^n)^m = g^{mn}$, we write $m(ng) = (mn)g$.

- For other valid groups, it depends on how you define the operation for the group.

Lemma 3.4

For every $m, n \in \mathbb{Z}$:

$$g^m * g^n = g^{m+n}$$

Proof. Like the previous proof, we will consider various cases depending on the signs of m and n. Since it is easier to work with positive numbers, we will write $m = \text{sign}(m)r$ and $n = \text{sign}(n)s$ where $r = |m|$ and $s = |n|$, where:

$$\text{sign} : \mathbb{R} \to \{-1, 1\}$$

- Case 1: Suppose m and n are positive. Then:

$$g^m * g^n = (\underbrace{g * \cdots * g}_{m \text{ times}}) * (\underbrace{g * \cdots * g}_{n \text{ times}}) = \underbrace{g * \cdots * g}_{m+n \text{ times}} = g^{m+n}$$

- Case 2: Suppose $m = -r$ (m is negative), $n = s$ (n is positive), $r < s$ ($m + n$ is positive). Then, by the previous case:

$$g^r * g^{s-r} = g^s \implies g^{s-r} = (g^r)^{-1} * g^s = g^{-r} * g^s$$

- Case 3: Suppose $m = -r$, $n = s$, $r > s$ ($m + n$ is negative). Then, by the first case:

$$\begin{aligned} g^s * g^{r-s} = g^r &\implies g^{r-s} = (g^s)^{-1} * g^r \\ &\implies (g^{r-s})^{-1} = ((g^s)^{-1} * g^r)^{-1} \\ &\implies g^{-(r-s)} = (g^r)^{-1} * ((g^s)^{-1})^{-1} \\ &\implies g^{-r+s} = g^{-r} * g^s \end{aligned}$$

- Case 4: Suppose $m = 0$. Then:

$$g^m * g^n = \epsilon * g^n = g^n = g^{m+n}$$

- Case 5: Suppose $n = 0$. Then:

$$g^m * g^n = g^m * \epsilon = g^m = g^{m+n}$$

By the above cases, we obtain the claim when $n \geq 0$ and $m \in \mathbb{Z}$. So:

- Case 6: Suppose $n = -s$ (n is negative) and $s > 0$. Then:

$$g^{m-s} * g^s = g^m \implies g^{m-s} = g^m * (g^s)^{-1} \implies g^{m-s} = g^m * g^{-s}$$

This concludes the proof. □

4 More on Groups

Now, we will look into the structure of groups. Specifically, we will consider how groups can be *the same*. We'll also consider subgroups and generating groups and subgroups from elements and the order of elements.

4.1 Groups and Sizes

A question we might consider is, for a given finite size, what different types of groups can we have?

For instance, what can groups of size 2 look like? Well, we need to have a set of size 2. Denote this set $\{a, b\}$. We also need a binary operation for this set. We'll make use of a table to better demonstrate this.

	a	b
a		
b		

Because we want a group, one of a or b needs to be an identity. Let's choose a to be the identity. Then:

	a	b
a	a	b
b	b	a

At this point, b has to be its own inverse (a cannot be the inverse). Now, if b is the identity element, then our table would look like[7]:

	a	b
a	b	a
b	a	b

4.2 Group Isomorphism

Even if groups are not literally the same, they can be isomorphic (essentially the same as relabelling the elements of the set). Formally, the relabelling will be an invertible (or bijective) map between the sets of the groups that preserves the group structure.

Specifically, if we have a group G_1 with operation $*_1$ and a group G_2 with operation $*_2$, an isomorphism from G_1 to G_2 is a function $f : G_1 \to G_2$ such that f is a bijection and:

$$f(g *_1 h) = f(g) *_2 f(h) \quad \forall g, h \in G_1$$

Formally:

Definition 4.1: Isomorphism

Let $(S, *)$ and $(S', *')$ be binary algebraic structures. An **isomorphic of** S with S' is a one-to-one function Φ mapping S onto S' such that:

$$\Phi(x * y) = \Phi(y) *' \Phi(y) \quad \forall x, y \in S$$

If two groups have an isomorphism, then we say that they are isomorphic (essentially the same group).

Corollary 4.1

It follows that:

$$f^{-1}(k *_2 l) = f^{-1}(k) *_1 f^{-1}(l) \quad \forall k, l \in G_2$$

Proof. We begin by noting □

[7] These aren't really meaningfully different since we just swapped a and b.

4.2.1 Example: Isomorphism

Consider the set $G = \{a, b\}$ with the corresponding table:

G	a	b
a	a	b
b	b	a

This group G is isomorphic to $\mathbb{Z}_2 = \{0, 1\}$ (where the operation is addition modulo 2). Our isomorphism is:

$$f(a) = 0$$

$$f(b) = 1$$

The table corresponding to $\mathbb{Z}_2$ is:

$\mathbb{Z}_2$	0	1
0	0	1
1	1	0

It follows that f is isomorphic.