Group Theory

Vincent Macri

Table of Contents

1. Pure Math
2. The History of Group Theory
3. Examples of Groups
4. Group Definition
5. Uniqueness

What is pure math?

Pure Math

- Math for the sake of math
- Math is art
- Math is beautiful
- Accidental applications
- Chemistry is gross

Table of Contents

1 Pure Math

2 The History of Group Theory

3 Examples of Groups

4 Group Definition

5 Uniqueness

A quote

The History of Group Theory

“We need a super-mathematics in which the operations are as unknown as the quantities they operate on, and a super-mathematician who does not know what he is doing when he performs these operations. Such a super-mathematics is the Theory of Groups.” (Sir Arthur Stanley Eddington)

A quote

The History of Group Theory

“We need a super-mathematics in which the operations are as unknown as the quantities they operate on, and a super-mathematician who does not know what he is doing when he performs these operations. Such a super-mathematics is the Theory of Groups.” (Sir Arthur Stanley Eddington)

In other words, group theory is something so powerful that a proof using group theory will usually prove something in many other branches of mathematics at the same time.

The quadratic formula

The History of Group Theory

For $ax^2 + bx + c = 0$:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

There also exist similar formulas for cubic and quartic functions, but they are disgusting and won't fit on this slide. But they do exist, which means a computer can easily find the roots of cubic and quartic functions.

The quadratic formula

The History of Group Theory

For $ax^2 + bx + c = 0$:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

There also exist similar formulas for cubic and quartic functions, but they are disgusting and won't fit on this slide. But they do exist, which means a computer can easily find the roots of cubic and quartic functions.

Is there a formula for quintics, sextics, or for any n degree polynomial?

The quadratic formula

The History of Group Theory

For $ax^2 + bx + c = 0$:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

There also exist similar formulas for cubic and quartic functions, but they are disgusting and won't fit on this slide. But they do exist, which means a computer can easily find the roots of cubic and quartic functions.

Is there a formula for quintics, sextics, or for any n degree polynomial?

No! And this was proved by Évariste Galois using group theory.

A quote on group theory in science

The History of Group Theory

“The importance of group theory was emphasized very recently when some physicists using group theory predicted the existence of a particle that had never been observed before, and described the properties it should have. Later experiments proved that this particle really exists and has those properties.” (Irving Adler)

A quote on group theory in science

"The importance of group theory was emphasized very recently when some physicists using group theory predicted the existence of a particle that had never been observed before, and described the properties it should have. Later experiments proved that this particle really exists and has those properties." (Irving Adler)

Keeping this quote in mind, let's look at what a group is.

Table of Contents

1 Pure Math

2 The History of Group Theory

3 Examples of Groups

4 Group Definition

5 Uniqueness

What is a cat?

Examples of Groups

Instead of formally defining groups, let’s look at them intuitively first

What is a cat?

Examples of Groups

Instead of formally defining groups, let's look at them intuitively first

For now, what is a cat?

Group 1: $(\mathbb{Z}, +)$ examples

Examples of Groups

This group is the group of all integers. Other than the integers, we also have $+$, the addition operation.

Let's look at some examples of using $+$ on $\mathbb{Z}$:

$$2 + 2 = 4$$

$$4 + (-1) = 3$$

$$3 + 9 = 12$$

$$9 + 3 = 12$$

$$0 + 25 = 25$$

$$(-10) + 0 = -10$$

$$5 + (-5) = 0$$

$$(-14) + 14 = 0$$

$$0 + 0 = 0$$

Group 1: $(\mathbb{Z}, +)$ identity

Notice that for the group $(\mathbb{Z}, +)$ that:

$$a + 0 = a = 0 + a$$

For any element in $\mathbb{Z}$, adding 0 yields the same element.

Group 1: $(\mathbb{Z}, +)$ identity

Examples of Groups

Notice that for the group $(\mathbb{Z}, +)$ that:

$$a + 0 = a = 0 + a$$

For any element in $\mathbb{Z}$, adding 0 yields the same element.

Because of this, we will call 0 the identity element.

Group 1: $(\mathbb{Z}, +)$ inverse

Examples of Groups

Notice that for the group $(\mathbb{Z}, +)$, every element has an element such that the sum of the two elements is equal to the identity element.

In other words, for any $a \in \mathbb{Z}$, there exists $b \in \mathbb{Z}$ such that:

$$a + b = 0 \mid b = -a$$

We will call b the inverse of a. In this group, a is also the inverse of b.

Group 1: $(\mathbb{Z}, +)$ inverse

Examples of Groups

Notice that for the group $(\mathbb{Z}, +)$, every element has an element such that the sum of the two elements is equal to the identity element.

In other words, for any $a \in \mathbb{Z}$, there exists $b \in \mathbb{Z}$ such that:

$$a + b = 0 \mid b = -a$$

We will call b the inverse of a. In this group, a is also the inverse of b.

What is the inverse of 5 in this group?

Group 1: $(\mathbb{Z}, +)$ inverse

Examples of Groups

Notice that for the group $(\mathbb{Z}, +)$, every element has an element such that the sum of the two elements is equal to the identity element.

In other words, for any $a \in \mathbb{Z}$, there exists $b \in \mathbb{Z}$ such that:

$$a + b = 0 \mid b = -a$$

We will call b the inverse of a. In this group, a is also the inverse of b.

What is the inverse of 5 in this group?

Is it true for any group that if the inverse of a is b, the inverse of b will be a?

Group 2: $(\mathbb{Q} \setminus \{0\}, \times)$ examples

Examples of Groups

Let's look at the group of rational numbers, not including 0, related to each other by multiplication:

$$\frac{4}{1} \times \frac{2}{3} = \frac{8}{3}$$

$$\frac{1}{1} \times \frac{3}{1} = \frac{3}{1}$$

$$\frac{3}{1} \times \frac{1}{3} = \frac{1}{1}$$

Group 2: $(\mathbb{Q} \setminus \{0\}, \times)$ identity

Examples of Groups

What is the identity element of $(\mathbb{Q} \setminus \{0\}, \times)$?

Group 2: $(\mathbb{Q} \setminus \{0\}, \times)$ identity

Examples of Groups

What is the identity element of $(\mathbb{Q} \setminus \{0\}, \times)$?

The identity element is $\frac{1}{1}$, as that is the only element b such that $a \times b = a$.

Group 2: $(\mathbb{Q} \setminus \{0\}, \times)$ inverse

Examples of Groups

What is the inverse element of $\frac{a}{b}$ in $(\mathbb{Q} \setminus \{0\}, \times)$?

Group 2: $(\mathbb{Q} \setminus \{0\}, \times)$ inverse

Examples of Groups

What is the inverse element of $\frac{a}{b}$ in $(\mathbb{Q} \setminus \{0\}, \times)$?

$$\frac{a}{b} \times \frac{?}{?} = \frac{1}{1}$$

Group 2: $(\mathbb{Q} \setminus \{0\}, \times)$ inverse

Examples of Groups

What is the inverse element of $\frac{a}{b}$ in $(\mathbb{Q} \setminus \{0\}, \times)$?

$$\frac{a}{b} \times \frac{?}{?} = \frac{1}{1}$$

The inverse of $\frac{a}{b}$ in this group is $\frac{b}{a}$.

We write this as c^{-1} is the inverse of c, and we will also use this notation for operations other than multiplication.

Group 3: $(\{-1, 1\}, \times)$ all at once

Examples of Groups

Let's look at a group with a finite number of elements. Since it's finite, we can draw out a multiplication table.

$\times$	-1	1
-1	1	-1
1	-1	1

Note that group this is a subset[1] of the last group we looked at.

[1] Not *technically* the right word, but we'll talk more about that later.

Group 3: $(\{-1, 1\}, \times)$ all at once

Examples of Groups

Let's look at a group with a finite number of elements. Since it's finite, we can draw out a multiplication table.

$\times$	-1	1
-1	1	-1
1	-1	1

Note that group this is a subset[1] of the last group we looked at.

What is the identity element?

[1] Not *technically* the right word, but we'll talk more about that later.

Group 3: $(\{-1, 1\}, \times)$ all at once

Examples of Groups

Let's look at a group with a finite number of elements. Since it's finite, we can draw out a multiplication table.

$\times$	-1	1
-1	1	-1
1	-1	1

Note that group this is a subset[1] of the last group we looked at.

What is the identity element? 1

[1] Not *technically* the right word, but we'll talk more about that later.

Group 3: $(\{-1, 1\}, \times)$ all at once

Examples of Groups

Let's look at a group with a finite number of elements. Since it's finite, we can draw out a multiplication table.

$\times$	-1	1
-1	1	-1
1	-1	1

Note that group this is a subset[1] of the last group we looked at.

What is the identity element? 1

What is the inverse of 1?

[1] Not *technically* the right word, but we'll talk more about that later.

Group 3: $(\{-1, 1\}, \times)$ all at once

Let's look at a group with a finite number of elements. Since it's finite, we can draw out a multiplication table.

$\times$	-1	1
-1	1	-1
1	-1	1

Note that group this is a subset[1] of the last group we looked at.

What is the identity element? 1

What is the inverse of 1? 1

[1] Not *technically* the right word, but we'll talk more about that later.

Group 3: $(\{-1, 1\}, \times)$ all at once

Examples of Groups

Let's look at a group with a finite number of elements. Since it's finite, we can draw out a multiplication table.

$\times$	-1	1
-1	1	-1
1	-1	1

Note that group this is a subset[1] of the last group we looked at.

What is the identity element? 1

What is the inverse of 1? 1

What is the inverse of -1?

[1] Not *technically* the right word, but we'll talk more about that later.

Group 3: $(\{-1, 1\}, \times)$ all at once

Let's look at a group with a finite number of elements. Since it's finite, we can draw out a multiplication table.

$\times$	-1	1
-1	1	-1
1	-1	1

Note that group this is a subset[1] of the last group we looked at.

What is the identity element? 1

What is the inverse of 1? 1

What is the inverse of -1? -1

[1] Not *technically* the right word, but we'll talk more about that later.

Modular arithmetic

Examples of Groups

All of our groups so far have had the property that the operation performed on any two elements in the group yields a third element also in the group. What else has this property?

All of our groups so far have had the property that the operation performed on any two elements in the group yields a third element also in the group. What else has this property? Hint: there's one on the wall of every classroom.)

Modular arithmetic

Examples of Groups

All of our groups so far have had the property that the operation performed on any two elements in the group yields a third element also in the group. What else has this property? Hint: there's one on the wall of every classroom.)

Clocks do! On a clock, $11 + 2 = 1$. This is called modular arithmetic, because we do this kind of math using the modulo operation. You can think of modular arithmetic as wrapping around. Modular arithmetic is only defined for the integers.

Modular arithmetic

Examples of Groups

All of our groups so far have had the property that the operation performed on any two elements in the group yields a third element also in the group. What else has this property? Hint: there's one on the wall of every classroom.)

Clocks do! On a clock, $11 + 2 = 1$. This is called modular arithmetic, because we do this kind of math using the modulo operation. You can think of modular arithmetic as wrapping around. Modular arithmetic is only defined for the integers.

Simply put, $a = b \mod c$ means that the remainder of $a \div c$ is equal to the remainder of $b \div c$. Or, more formally:

$$a = b \mod c \iff a - b = kc \mid k \in \mathbb{Z}$$

Some people will use $\equiv$ (equivalent) instead of $=$ when talking about modulo. Both notations are acceptable.

Group 4: $(\mathbb{Z}_{12}, +)$ definition

We start by defining the set that makes up the elements of our group:

$$\mathbb{Z}_{12} \coloneqq \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

And we define $+$ to work as normal, but with the additional property that:

$$a + b = a + b \mod 12$$

Group 4: $(\mathbb{Z}_{12}, +)$ examples

Examples of Groups

Let's go through some examples of our new addition in this group:

$$1 + 4 = 5 \mod 12$$

$$3 + 0 = 3 \mod 12$$

$$11 + 3 = 2 \mod 12$$

We can think of performing $+$ in $(\mathbb{Z}_{12}, +)$ to be the same as performing $+$ in $(\mathbb{Z}, +)$, except if the result is outside of $\mathbb{Z}_{12}$, we repeatedly add or subtract 12 until our answer is in $\mathbb{Z}_{12}$. With this definition, we can show that we can convert numbers that are outside of $\mathbb{Z}_{12}$ to be inside of $\mathbb{Z}_{12}$.

Group 4: $(\mathbb{Z}_{12}, +)$ examples

Examples of Groups

Let's go through some examples of our new addition in this group:

$$1 + 4 = 5 \mod 12$$

$$3 + 0 = 3 \mod 12$$

$$11 + 3 = 2 \mod 12$$

We can think of performing $+$ in $(\mathbb{Z}_{12}, +)$ to be the same as performing $+$ in $(\mathbb{Z}, +)$, except if the result is outside of $\mathbb{Z}_{12}$, we repeatedly add or subtract 12 until our answer is in $\mathbb{Z}_{12}$. With this definition, we can show that we can convert numbers that are outside of $\mathbb{Z}_{12}$ to be inside of $\mathbb{Z}_{12}$.

For example, since $4 = 52 \mod 12$ and $5 = 53 \mod 12$, we can write that:

$$52 + 53 = 105 = 9 \mod 12 \qquad \text{or} \qquad 4 + 5 = 9 \mod 12$$

So it doesn't matter if we perform modulo before or after the addition. We get the same answer. Cool!

Group 4: $(\mathbb{Z}_{12}, +)$ identity

Examples of Groups

What is the identity in $\mathbb{Z}_{12}$?

Group 4: $(\mathbb{Z}_{12}, +)$ identity

What is the identity in $\mathbb{Z}_{12}$?

With this, multiple numbers satisfy the property for an identity. For example:

$$5 + 12 = 5 \mod 12$$

$$5 + 24 = 5 \mod 12$$

$$5 + 0 = 5 \mod 12$$

And this works for any multiple of 12. Are there multiple identities?

Group 4: $(\mathbb{Z}_{12}, +)$ identity

What is the identity in $\mathbb{Z}_{12}$?

With this, multiple numbers satisfy the property for an identity. For example:

$$5 + 12 = 5 \mod 12$$

$$5 + 24 = 5 \mod 12$$

$$5 + 0 = 5 \mod 12$$

And this works for any multiple of 12. Are there multiple identities?

No. Because of these, **only** $0 \in \mathbb{Z}_{12}$. So 0 is the identity.

Group 4: $(\mathbb{Z}_{12}, +)$ identity

Examples of Groups

What is the identity in $\mathbb{Z}_{12}$?

With this, multiple numbers satisfy the property for an identity. For example:

$$5 + 12 = 5 \mod 12$$

$$5 + 24 = 5 \mod 12$$

$$5 + 0 = 5 \mod 12$$

And this works for any multiple of 12. Are there multiple identities?

No. Because of these, **only** $0 \in \mathbb{Z}_{12}$. So 0 is the identity.

The reason all multiple of 12 work is that $0 = 12k \mod 12 \mid k \in \mathbb{Z}$. In other words, in $\mathbb{Z}_{12}$, all multiples of 12 are equivalent to 0.

Group 4: $(\mathbb{Z}_{12}, +)$ inverse

What is the general form for the inverse of a in $(\mathbb{Z}_{12}, +)$?

$$a + a^{-1} = 0 \mod 12$$

Group 4: $(\mathbb{Z}_{12}, +)$ inverse

Examples of Groups

What is the general form for the inverse of a in $(\mathbb{Z}_{12}, +)$?

$$a + a^{-1} = 0 \mod 12$$

At first, you might think that $a^{-12} = 12 - a$. It seems to work:

$$4 + (12 - 4) = 4 + 8 = 12 = 0 \mod 12$$

But what if $a = 0$? Does it still work?

$$0 + 12 = 12 = 0 \mod 12$$

Group 4: $(\mathbb{Z}_{12}, +)$ inverse

What is the general form for the inverse of a in $(\mathbb{Z}_{12}, +)$?

$$a + a^{-1} = 0 \mod 12$$

At first, you might think that $a^{-12} = 12 - a$. It seems to work:

$$4 + (12 - 4) = 4 + 8 = 12 = 0 \mod 12$$

But what if $a = 0$? Does it still work?

$$0 + 12 = 12 = 0 \mod 12$$

But 12 is outside of $\mathbb{Z}_{12}$!

That's okay. Remember that in $\mathbb{Z}_{12}$, $12 = 0$. So, the inverse of 0 is 0!

We can draw out a table of inverses:

a	0	1	2	3	4	5	6	7	8	9	10	11
a^{-1}	0	11	10	9	8	7	6	5	4	3	2	1

Group 5: $(\mathbb{Z}_5^*, \times)$ all at once

Examples of Groups

Ignore the * in the group name, let's look at $(\mathbb{Z}_5, \times)$ for now.

Group 5: $(\mathbb{Z}_5^*, \times)$ all at once

Ignore the * in the group name, let's look at $(\mathbb{Z}_5, \times)$ for now.

What is the identity?

Group 5: $(\mathbb{Z}_5^*, \times)$ all at once

Ignore the * in the group name, let's look at $(\mathbb{Z}_5, \times)$ for now.

What is the identity? 1

Group 5: $(\mathbb{Z}_5^*, \times)$ all at once

Ignore the * in the group name, let's look at $(\mathbb{Z}_5, \times)$ for now.

What is the identity? 1

What are the inverses?
Let's draw out a table:

a	0	1	2	3	4
a^{-1}	$*$	1	$*$	2	4

0 does not have an inverse! We will define something to deal with this:

Unit

Let a be a number in a set G.
We will call a a **unit** if a^{-1} exists. The set of units of G will be called G^*.

Group 6: $(\mathrm{Sym}(4), *)$.

Examples of Groups

This group is different. It's made up of diagrams with 4 points on the top, 4 points on the bottom, and lines between the points.

Group 6: $(\mathrm{Sym}(4), *)$.

Examples of Groups

This group is different. It's made up of diagrams with 4 points on the top, 4 points on the bottom, and lines between the points.

Let's look at this on the board.

Group 6: $(\mathrm{Sym}(4), *)$.

Examples of Groups

This group is different. It's made up of diagrams with 4 points on the top, 4 points on the bottom, and lines between the points.

Let's look at this on the board.

Interesting! With this group, $a * b \neq b * a$.

Table of Contents

1 Pure Math

2 The History of Group Theory

3 Examples of Groups

4 Group Definition

5 Uniqueness

Definition

Group Definition

A group is made of a set and an operation that acts on the elements of that set. In general, we denote a group as $(G, \cdot)$, where G is the set, and $\cdot$ is the operation.

A group also satisfies the four group axioms: identity, invertibility, associativity, and closure.

The identity axiom

Group Definition

The identity axiom says that:
There exists an element $e \in G$, called the identity, such that:

$$a \cdot e = e \cdot a = a$$

for all $a \in G$.

The invertibility axiom

Group Definition

The invertibility axiom states that for all $a \in G$, there exists a^{-1} such that:

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

We refer to a^{-1} as the inverse of a.

The associativity axiom

Group Definition

The associativity axiom states that for all $a, b, c \in G$:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

The closure axiom

Group Definition

The closure axiom states that for all $a, b \in G$ where $a \cdot b = c$, $c \in G$.

Or, performing the group's operation on any two elements in G will yield a third element also in G.

The power of sets

Group Definition

Now, behold the almighty power of sets as we are about to simultaneously prove infinite things.

Table of Contents

1. Pure Math
2. The History of Group Theory
3. Examples of Groups
4. Group Definition
5. Uniqueness

Uniqueness of the identity element

Uniqueness

Is the identity element of a group unique?

Uniqueness of the identity element

Uniqueness

Is the identity element of a group unique? Yes.

Proof.

Take the group $(G, \cdot)$.
Assume there are two identity elements, e and f, and $e \neq f$. Then:

$$\begin{aligned} e \cdot f &= f \cdot e \\ e \cdot f &= e \\ f \cdot e &= f \\ \therefore e &= f \end{aligned}$$

We have a contradiction. Therefore our original statement must be false, and there is only one identity element. □

Uniqueness of the inverse element

Uniqueness

Is the inverse of an element in a group unique?

Uniqueness of the inverse element

Uniqueness

Is the inverse of an element in a group unique? Yes.

Proof.

Take the group $(G, \cdot)$ with the identity element e.
Assume a has two inverses, b and c, and $b \neq c$:

$$a \cdot b = e \qquad a \cdot c = e$$

$$\begin{aligned} b &= b \cdot e \\ b &= b \cdot (a \cdot c) \\ b &= (b \cdot a) \cdot c \\ b &= e \cdot c \\ \therefore b &= c \end{aligned}$$

We have a contradiction. Therefore our original statement must be false, and there is only one inverse of a. □

What did we just do?

Uniqueness

We just proved for **all** groups that there is only one identity element, and only one inverse element for all $a \in G$.

This means that we just proved:

1. If $a \in \mathbb{Z}$, there is only one $b \in \mathbb{Z}$ such that $a + b = 0$.
2. If $a \in \mathbb{R}$, there is only one $b \in \mathbb{R}$ such that $a + b = 0$.
3. For all $a \in \mathbb{R}^*$ there is exactly one a^{-1} such that $a \times a^{-1} = 1$.
4. For all n: for all $a \in \mathbb{Z}_n$ there is only one b such that $a + b = 0$.
5. For all n: for all $a \in \mathbb{Z}_n^*$, there is exactly one a^{-1} such that $a \times a^{-1} = 1$.
6. There is no more than one correct answer when rearranging a linear equation.
7. While $(\mathbb{R}, -)$, is not a group, subtraction is the inverse of addition.
8. While $(\mathbb{R}, \div)$, is not a group, multiplication is the inverse of multiplication.
9. Division by 0 is undefined.