



Groups

Jean Mark Gawron

Linguistics

San Diego State University

gawron@mail.sdsu.edu

<http://www.rohan.sdsu.edu/~gawron>



Preliminaries

What kind of a thing is a group?

- a kind of algebra with one operation.
 - a set of elements and a **binary** operation ○
 - Closure and Uniqueness

What kind of algebra?

- The operation \circ is associative
- There is an identity element.
- Every element has an inverse.

Groups and Equations

- The requirement that every element has an inverse means that groups have equations with unique solutions. [to be shown]
- Such equations will be solvable using familiar techniques from algebra.

Group Axioms

Definition 0.1. Group

A group $\langle \mathbf{G}, \circ \rangle$ is a set \mathbf{G} together with an operation \circ satisfying the following basic properties:

1. **Closure Axiom.** The result of combining any two elements of \mathbf{G} with \circ yields an element of \mathbf{G} .
2. **Associativity Axiom.** For any 3 elements a, b , and c :

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

3. **Identity Element Axiom.** There is a distinguished element e such that for any a in \mathbf{G} :

$$e \circ a = a \circ e = a$$

4. **Inverse Axiom.** For any element a , there exists an element a^{-1} , called its **inverse**, such that:

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

Example: \mathbb{Z} , \mathbb{N} , under addition

- \mathbb{N} is not a group under addition. We have closure under an operation element and we have an identity element 0 , but $0 \notin \mathbb{N}$. Further more, x cannot be a positive integer in

$$3 + x = 0$$

So 3 has no inverse in \mathbb{N} Nor does any other positive integer.

- \mathbb{Z} is a group under addition. We have closure under an associative operation and we have an identity element $0 \in \mathbb{Z}$. Also $x \in \mathbb{Z}$ in:

$$3 + x = 0$$

So 3 , like all positive integers has an inverse in \mathbb{Z} .

$\langle \mathbb{N}, + \rangle$ *is not a group*

The positive integers under addition (written $\langle \mathbb{N}, + \rangle$) are not a group.

1. We've illustrated closure and associativity.
2. Identity element: \mathbb{N} , the set of positive integers, includes no identity element for addition, since 0 is the identity element for addition. $\mathbb{N} \cup \{0\}$ does satisfy the identity element axiom.
3. Inverse. $\mathbb{N} \cup \{0\}$ under addition does not include inverses, since the inverse of a positive integer under addition is always a negative integer. \mathbb{N} does not satisfy the inverse axiom.

Theorem: $\langle \mathbb{Z}, + \rangle$ is a group

The integers under addition are a group (written $\langle \mathbb{Z}, + \rangle$).

1. Closure: The sum of two integers is an integer
2. Associativity: Addition is associative

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

3. Identity: 0 is the identity element.
4. The additive inverse of any integer i is $-i$.

Finding more groups

- Once an associative operation with an identity element is defined, the trick to defining a group is often to choose the right set. Consider multiplication, which has an identity element and is associative.
- $\langle \mathbb{Z}, * \rangle$ is not a group. The inverse of an integer under multiplication is generally not an integer.
- Consider \mathbb{Q} , the set of **rational numbers** (all numbers expressible as a ratio between integers), then fractions and whole numbers alike are included ($\frac{5}{1}$ is included along with its inverse $\frac{1}{5}$).
- There is still one element missing an inverse, 0. So the final trick to defining a group under multiplication is to exclude 0:

The set of rationals \mathbb{Q} excluding 0 is a group under multiplication (written $\langle \mathbb{Q} - \{0\}, * \rangle$).

$\langle \mathbb{Q} - \{0\}, * \rangle$ *is a group*

1. We know multiplication on non zero rational numbers is closed and associative.
2. Identity element: The identity element for multiplication is 1. $1 \in \mathbb{Q} - \{0\}$.
3. Inverse. $\mathbb{Q} \cup -\{0\}$ does include the inverses of every element, since for every p, q :

$$\left(\frac{p}{q}\right)^{-1} = \frac{q}{p}$$

4. $\langle \mathbb{Q} - \{0\}, * \rangle$ is a group.



Solving Equations

Theorem 1. *Cancellation*

(a) *If $a \circ b = a \circ c$ then $b = c$ Left Cancellation*

(b) *If $b \circ a = c \circ a$ then $b = c$ Right Cancellation*

We show the proof for case (a). Case (b) is symmetric.
Assume:

$$a \circ b = a \circ c$$

From this we have:

- | | | |
|-----|---|-------------------|
| (1) | $a^{-1} \circ a \circ b = a^{-1} \circ a \circ c$ | Inverse Axiom |
| (2) | $(a^{-1} \circ a) \circ b = (a^{-1} \circ a) \circ c$ | Associative Axiom |
| (3) | $e \circ b = e \circ c$ | Inverse Axiom |
| (4) | $b = c$ | Identity Axiom |

Q.E.D.

Theorem 1 tells us is that given an a and the result of combining a with any other element b , b is recoverable (the operation can be *cancelled*).

Theorem 1 depends crucially on the existence of inverses to go through. This property is also crucially what is required in solving an algebraic equation.

To solve: $5 * x = 20$

- | | | |
|-----|------------------------------------|-------------------|
| (1) | $5^{-1} * 5 * x = 5^{-1} * 20$ | Inverse Axiom |
| (2) | $(5^{-1} * 5) * x = (5^{-1} * 20)$ | Associative Axiom |
| (3) | $1 * x = 4$ | Inverse Axiom |
| (4) | $x = 4$ | Identity Axiom |

If we know the result of multiplying 5 times x , x is recoverable and unique.

Equations and grouphood

Note that grouphood guarantees us that *all* equations of the form:

$$a \circ x = b$$

have unique solutions as long we stick to group members on both sides. This goes along with the idea that the set we are performing operations on has to be “big enough” to be a group. If it is big enough to be a group it is big enough to contain all the solutions to such equations. The set of integers wasn't big enough to be a group under multiplication and indeed, it isn't big enough to include all the solutions to equations involving multiplication, even multiplication with integers. For example, the solution to

$$2x = 5$$

isn't an integer.



Cyclic Groups

Order of a Group

Definition 0.2. *The number of elements in a finite group $\langle \mathbf{G}, \circ \rangle$ is called the **order** of \mathbf{G} and is denoted by $|\mathbf{G}|$.*

Definition 0.3. Iterated Group Operations

It follows from the axioms that

$$a \circ a \in \mathbf{G}$$

It also follows that

$$(a \circ a) \circ a = a \circ (a \circ a) \in \mathbf{G}$$

We write a^2 for

$$a \circ a$$

and a^3 for

$$a \circ a \circ a$$

and in general we write a^i for i repeated applications of \circ to a .

Cyclic Group, Group Generator

Definition 0.4. . A group \mathbf{G} is cyclic if there exists $a \in \mathbf{G}$ such that for any $b \in \mathbf{G}$, there is an integer $i \geq 0$ such that

$$a^i = b$$

Thus every element of \mathbf{G} is some power of a . Element a is called the generator of \mathbf{G} , which we write $\mathbf{G} = \langle a \rangle$

Example

- -1 in $\langle \{1, -1\}, * \rangle$. Consider the operation of multiplication over the set $\{-1, 1\}$. This is a group with 1 as the identity element. -1 is its own inverse and it is also the generator of the group since

$$(-1)^2 = 1$$

$$(-1)^3 = -1$$

Note that 1 is not a generator because no amount of multiplying 1 by itself yields -1 .

- In $\langle \mathbb{Z}, + \rangle$, 1 generates the entire set of positive integers:

$$1^1 = 1 \quad 1^2 = 2 \quad \dots \quad 1^n = n$$

but it does not generate the entire group because it does not generate the negative integers. Is there a generator?

Subgroups

Definition 0.5. *A subgroup of a group $\langle \mathbf{G}, \circ \rangle$ is a nonempty subset \mathbf{H} of \mathbf{G} which is itself a group under \circ . We write $\mathbf{H} \subseteq \mathbf{G}$ to denote that \mathbf{H} is a subgroup of \mathbf{G} .*

Example

The set of even integers forms a subgroup of the set of integers under addition.

1. The sum of two even numbers is even; the inverses of even numbers are even, and the identity element, 0, the identity element, is even.
2. The set of odd integers does not form a subgroup under addition because closure fails (the sum of odd integers is even); note also the identity element 0, is not odd. In general, the set of numbers divisible by any integer n will form a subgroup of the integers under addition. The reader should verify this.

As a final example, consider a group $\langle \mathbf{G}, \circ \rangle$ and a member a , and consider the smallest integer i such that:

$$a^i = e$$

where e is the identity element.

Definition 0.6. *If i exists we call i the order of a . If not, we say a has infinite order.*

The set

$$\mathbf{H} = \{x \mid x = a^j \text{ for some integer } j\}$$

is a subgroup of \mathbf{A} under \circ .

Note that

$$\begin{aligned}a^i &= e = a^0 \\a^{i+1} &= a = a^1 \\a^{i+2} &= a^2 \\&\vdots \\a^{i+n} &= a^n\end{aligned}$$

and for all higher values of j , we cycle through previously encountered values. Clearly closure is satisfied. Every power of a combined with another power of a gives a power of a . Note also that:

$$a^{-1} = a^{i-1} \text{ because } a \circ a^{i-1} = a^i = e$$

This is called a **cyclic group**. Why?

Important property of subgroups

Notice that each subgroup must include the identity element in order to be a group

Exercises

1. Refute or verify the grouphood of $\langle \mathbf{G}, \circ \rangle$. You may assume \circ is associative.

$$\mathbf{G} = \{a, b, c, d, e, f\}$$

and \circ is defined by the following table (note e in this case is not necessarily the identity element):

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

More exercises

2. Using the definition of \circ from example 1, compute e^5 .
3. Using the definition of \circ in example 1, refute or verify the grouphood of $\langle \mathbf{G}', \circ \rangle$ where

$$\mathbf{G}' = \{a, b, d\}$$

More exercises

4. Axiom 3 guarantees there's an identity element that is the identity element for every element of the group. But it doesn't say there is only one such element. Prove that the identity element is unique. That is, prove that if $\langle \mathbf{G}, \circ \rangle$ is a group then if $a, b \in \mathbf{G}$ and $a \circ b = a$, then $b = e$.

5. Show that

$$(a^{-1})^{-1} = a$$

That is, show that the inverse of the inverse of a is a again.

6. Show that

$$\text{If } a^{-1} = b^{-1} \text{ then } a = b$$