MTH223A

Yvette Fajardo-Lim

MTH223A LECTURE NOTES CHAPTER 2

Yvette Fajardo-Lim

Mathematics and Statistics Department
De La Salle University - Manila

Outline

Outline

Binary Operation

Definition

Let G be a nonempty set. A **binary operation *** *on G is a rule for combining two elements of G to produce another element of G; given $a, b \in G$ we write $a * b$ for the element produced by combining a with b. Thus, we can say that G is* **closed with respect to** $*$.

Binary Operation

Example

1. *If $G = \mathbb{R}$, then $a * b = a + b$ defines a binary operation on G since $a + b \in \mathbb{R}$.*
2. *If $G = \mathbb{Z}$, then $a * b = ab$ defines a binary operation on G since $ab \in \mathbb{Z}$.*
3. *If $G = \mathbb{Z}^+$, then $a * b = a - b$ does not define a binary operation on G, because if $b \geq a$ then $a - b \notin \mathbb{Z}^+$.*
4. *If $G = \mathbb{Z}$, then $a * b = \frac{a}{b}$ does not define a binary operation on G, because if b does not divide a exactly then $\frac{a}{b} \notin \mathbb{Z}$.*

Binary Operation

Example

1. *If $G = \mathbb{R}$, then $a * b = a + b$ defines a binary operation on G since $a + b \in \mathbb{R}$.*
2. *If $G = \mathbb{Z}$, then $a * b = ab$ defines a binary operation on G since $ab \in \mathbb{Z}$.*
3. *If $G = \mathbb{Z}^+$, then $a * b = a - b$ does not define a binary operation on G, because if $b \geq a$ then $a - b \notin \mathbb{Z}^+$.*
4. *If $G = \mathbb{Z}$, then $a * b = \frac{a}{b}$ does not define a binary operation on G, because if b does not divide a exactly then $\frac{a}{b} \notin \mathbb{Z}$.*

Binary Operation

Example

1. *If $G = \mathbb{R}$, then $a * b = a + b$ defines a binary operation on G since $a + b \in \mathbb{R}$.*
2. *If $G = \mathbb{Z}$, then $a * b = ab$ defines a binary operation on G since $ab \in \mathbb{Z}$.*
3. *If $G = \mathbb{Z}^+$, then $a * b = a - b$ does not define a binary operation on G, because if $b \geq a$ then $a - b \notin \mathbb{Z}^+$.*
4. *If $G = \mathbb{Z}$, then $a * b = \frac{a}{b}$ does not define a binary operation on G, because if b does not divide a exactly then $\frac{a}{b} \notin \mathbb{Z}$.*

Binary Operation

Example

1. *If $G = \mathbb{R}$, then $a * b = a + b$ defines a binary operation on G since $a + b \in \mathbb{R}$.*
2. *If $G = \mathbb{Z}$, then $a * b = ab$ defines a binary operation on G since $ab \in \mathbb{Z}$.*
3. *If $G = \mathbb{Z}^+$, then $a * b = a - b$ does not define a binary operation on G, because if $b \geq a$ then $a - b \notin \mathbb{Z}^+$.*
4. *If $G = \mathbb{Z}$, then $a * b = \frac{a}{b}$ does not define a binary operation on G, because if b does not divide a exactly then $\frac{a}{b} \notin \mathbb{Z}$.*

Binary Operation

Example

1. *If $G = \mathbb{R}$, then $a * b = a + b$ defines a binary operation on G since $a + b \in \mathbb{R}$.*
2. *If $G = \mathbb{Z}$, then $a * b = ab$ defines a binary operation on G since $ab \in \mathbb{Z}$.*
3. *If $G = \mathbb{Z}^+$, then $a * b = a - b$ does not define a binary operation on G, because if $b \geq a$ then $a - b \notin \mathbb{Z}^+$.*
4. *If $G = \mathbb{Z}$, then $a * b = \frac{a}{b}$ does not define a binary operation on G, because if b does not divide a exactly then $\frac{a}{b} \notin \mathbb{Z}$.*

Remark

The important things to note are:

1. $a * b$ must be defined for all $a, b \in G$;
2. $a * b$ must itself be an element of G for all $a, b \in G$.

Binary Operation

Remark

The important things to note are:

1. $a * b$ *must be defined for all* $a, b \in G$*;*
2. $a * b$ *must itself be an element of* G *for all* $a, b \in G$*.*

Binary Operation

Remark

The important things to note are:

1. $a * b$ *must be defined for all* $a, b \in G$;
2. $a * b$ *must itself be an element of* G *for all* $a, b \in G$.

Outline

Semigroup

Definition

A **semigroup** *is a set G together with a binary operation * which is associative. That is, for all* $a, b, c \in G, (a * b) * c = a * (b * c)$.

Example

1. $\mathbb{Z}$ *under addition is a semigroup.*
2. $\mathbb{Z}$ *under multiplication is a semigroup.*
3. *Subtraction on the set* $\mathbb{Z}$ *is not associative, hence,* $\mathbb{Z}$ *under subtraction is not a semigroup.*

Semigroup

Definition

A **semigroup** *is a set G together with a binary operation * which is associative. That is, for all* $a, b, c \in G, (a * b) * c = a * (b * c)$.

Example

1. $\mathbb{Z}$ *under addition is a semigroup.*
2. $\mathbb{Z}$ *under multiplication is a semigroup.*
3. *Subtraction on the set* $\mathbb{Z}$ *is not associative, hence,* $\mathbb{Z}$ *under subtraction is not a semigroup.*

Semigroup

Definition

A **semigroup** *is a set G together with a binary operation * which is associative. That is, for all* $a, b, c \in G, (a * b) * c = a * (b * c)$.

Example

1. $\mathbb{Z}$ *under addition is a semigroup.*
2. $\mathbb{Z}$ *under multiplication is a semigroup.*
3. *Subtraction on the set* $\mathbb{Z}$ *is not associative, hence,* $\mathbb{Z}$ *under subtraction is not a semigroup.*

Semigroup

Definition

A **semigroup** *is a set G together with a binary operation * which is associative. That is, for all* $a, b, c \in G, (a * b) * c = a * (b * c)$.

Example

1. $\mathbb{Z}$ *under addition is a semigroup.*
2. $\mathbb{Z}$ *under multiplication is a semigroup.*
3. *Subtraction on the set* $\mathbb{Z}$ *is not associative, hence,* $\mathbb{Z}$ *under subtraction is not a semigroup.*

Monoid

Definition

A **monoid** *is a semigroup* $(G, *)$ *if there exists an element* e *of* G *where* $a * e = a = e * a$ *for all* $a \in G$*;* e *is called an* **identity element** *of* G*.*

Example

1. *Addition on the set* $\mathbb{Z}$ *has identity 0, the semigroup* $(\mathbb{Z}, +)$ *is a monoid.*
2. *Multiplication on the set* $\mathbb{Z}$ *has identity 1, the semigroup* $(\mathbb{Z}, \bullet)$ *is a monoid.*

Monoid

Definition

*A **monoid** is a semigroup $(G, *)$ if there exists an element e of G where $a * e = a = e * a$ for all $a \in G$; e is called an **identity element** of G.*

Example

1. *Addition on the set $\mathbb{Z}$ has identity 0, the semigroup $(\mathbb{Z}, +)$ is a monoid.*
2. *Multiplication on the set $\mathbb{Z}$ has identity 1, the semigroup $(\mathbb{Z}, \bullet)$ is a monoid.*

Monoid

Definition

A **monoid** *is a semigroup* $(G, *)$ *if there exists an element e of G where* $a * e = a = e * a$ *for all* $a \in G$*; e is called an* **identity element** *of G.*

Example

1. *Addition on the set* $\mathbb{Z}$ *has identity 0, the semigroup* $(\mathbb{Z}, +)$ *is a monoid.*
2. *Multiplication on the set* $\mathbb{Z}$ *has identity 1, the semigroup* $(\mathbb{Z}, \bullet)$ *is a monoid.*

Monoid

Definition

*A **monoid** is a semigroup $(G, *)$ if there exists an element e of G where $a * e = a = e * a$ for all $a \in G$; e is called an **identity element** of G.*

Example

1. *Addition on the set $\mathbb{Z}$ has identity 0, the semigroup $(\mathbb{Z}, +)$ is a monoid.*
2. *Multiplication on the set $\mathbb{Z}$ has identity 1, the semigroup $(\mathbb{Z}, \bullet)$ is a monoid.*

Group

Definition

A **group** *is a monoid $(G, *)$ if for all $a \in G$ there exists $a^{-1} \in G$ which satisfies the property $a * a^{-1} = e = a^{-1} * a$ for all $a \in G$; a^{-1} is called the* **inverse element of** *a.*

Example

1. *For addition on $\mathbb{Z}$, the inverse of the element a is $-a$, since $a + (-a) = 0 = (-a) + a$. Hence, the monoid $(\mathbb{Z}, +)$ is a group.*
2. *For multiplication on $\mathbb{Z}$, the only elements having inverses are 1 and -1 and in each case the inverse is the element itself. Hence, the monoid $(\mathbb{Z}, \bullet)$ is not a group.*

Group

Definition

*A **group** is a monoid $(G, *)$ if for all $a \in G$ there exists $a^{-1} \in G$ which satisfies the property $a * a^{-1} = e = a^{-1} * a$ for all $a \in G$; a^{-1} is called the **inverse element of** a.*

Example

1. *For addition on $\mathbb{Z}$, the inverse of the element a is $-a$, since $a + (-a) = 0 = (-a) + a$. Hence, the monoid $(\mathbb{Z}, +)$ is a group.*
2. *For multiplication on $\mathbb{Z}$, the only elements having inverses are 1 and -1 and in each case the inverse is the element itself. Hence, the monoid $(\mathbb{Z}, \bullet)$ is not a group.*

Group

Definition

A **group** *is a monoid $(G, *)$ if for all $a \in G$ there exists $a^{-1} \in G$ which satisfies the property $a * a^{-1} = e = a^{-1} * a$ for all $a \in G$; a^{-1} is called the* **inverse element of** *a.*

Example

1. *For addition on $\mathbb{Z}$, the inverse of the element a is $-a$, since $a + (-a) = 0 = (-a) + a$. Hence, the monoid $(\mathbb{Z}, +)$ is a group.*
2. *For multiplication on $\mathbb{Z}$, the only elements having inverses are 1 and -1 and in each case the inverse is the element itself. Hence, the monoid $(\mathbb{Z}, \bullet)$ is not a group.*

Group

Definition

A **group** *is a monoid $(G, *)$ if for all $a \in G$ there exists $a^{-1} \in G$ which satisfies the property $a * a^{-1} = e = a^{-1} * a$ for all $a \in G$; a^{-1} is called the* **inverse element of** *a.*

Example

1. *For addition on $\mathbb{Z}$, the inverse of the element a is $-a$, since $a + (-a) = 0 = (-a) + a$. Hence, the monoid $(\mathbb{Z}, +)$ is a group.*
2. *For multiplication on $\mathbb{Z}$, the only elements having inverses are 1 and -1 and in each case the inverse is the element itself. Hence, the monoid $(\mathbb{Z}, \bullet)$ is not a group.*

Group

Remark

A group is a set together with an associative operation such that every element has an inverse and any pair of elements can be combined without going outside the set. This latter condition is called **closure**. *To test if $(G, *)$ is a group, the following properties must be verified.*

1. **Closure.** *G is closed under $*$. That is, if $a, b \in G$ then $a * b \in G$;*
2. **Associativity.** *For all $a, b, c \in G, (a * b) * c = a * (b * c).$;*
3. **Identity.** *There is an e such that $a * e = a = e * a$ for all $a \in G$;*
4. **Inverses.** *For all $a \in G$ there exists $a^{-1} \in G$ such that $a * a^{-1} = e = a^{-1} * a$.*

Remark

A group is a set together with an associative operation such that every element has an inverse and any pair of elements can be combined without going outside the set. This latter condition is called **closure**. *To test if $(G, *)$ is a group, the following properties must be verified.*

1. **Closure.** *G is closed under $*$. That is, if $a, b \in G$ then $a * b \in G$;*
2. **Associativity.** *For all $a, b, c \in G, (a * b) * c = a * (b * c).$;*
3. **Identity.** *There is an e such that $a * e = a = e * a$ for all $a \in G$;*
4. **Inverses.** *For all $a \in G$ there exists $a^{-1} \in G$ such that $a * a^{-1} = e = a^{-1} * a$.*

Group

Remark

A group is a set together with an associative operation such that every element has an inverse and any pair of elements can be combined without going outside the set. This latter condition is called **closure**. *To test if $(G, *)$ is a group, the following properties must be verified.*

1. **Closure.** *G is closed under $*$. That is, if $a, b \in G$ then $a * b \in G$;*
2. **Associativity.** *For all $a, b, c \in G, (a * b) * c = a * (b * c).$;*
3. **Identity.** *There is an e such that $a * e = a = e * a$ for all $a \in G$;*
4. **Inverses.** *For all $a \in G$ there exists $a^{-1} \in G$ such that $a * a^{-1} = e = a^{-1} * a$.*

Remark

A group is a set together with an associative operation such that every element has an inverse and any pair of elements can be combined without going outside the set. This latter condition is called **closure**. *To test if* $(G, *)$ *is a group, the following properties must be verified.*

1. **Closure.** *G is closed under $*$. That is, if $a, b \in G$ then $a * b \in G$;*
2. **Associativity.** *For all $a, b, c \in G, (a * b) * c = a * (b * c).$;*
3. **Identity.** *There is an e such that $a * e = a = e * a$ for all $a \in G$;*
4. **Inverses.** *For all $a \in G$ there exists $a^{-1} \in G$ such that $a * a^{-1} = e = a^{-1} * a$.*

Group

Remark

A group is a set together with an associative operation such that every element has an inverse and any pair of elements can be combined without going outside the set. This latter condition is called **closure**. *To test if $(G, *)$ is a group, the following properties must be verified.*

1. **Closure.** *G is closed under $*$. That is, if $a, b \in G$ then $a * b \in G$;*
2. **Associativity.** *For all $a, b, c \in G, (a * b) * c = a * (b * c).$;*
3. **Identity.** *There is an e such that $a * e = a = e * a$ for all $a \in G$;*
4. **Inverses.** *For all $a \in G$ there exists $a^{-1} \in G$ such that $a * a^{-1} = e = a^{-1} * a$.*

Group

Example

Which is a group?

1. $(\mathbb{Z}, *)$ *where* $a * b = a + b + 1, a, b \in \mathbb{Z}$
2. $(\mathbb{Z}, *)$ *where* $a * b = 2a + 2b, a, b \in \mathbb{Z}$
3. $(\mathbb{Z}, *)$ *where* $a * b = ab^2 + a + b, a, b \in \mathbb{Z}$

Group

Example

Which is a group?

1. $(\mathbb{Z}, *)$ where $a * b = a + b + 1, a, b \in \mathbb{Z}$
2. $(\mathbb{Z}, *)$ where $a * b = 2a + 2b, a, b \in \mathbb{Z}$
3. $(\mathbb{Z}, *)$ where $a * b = ab^2 + a + b, a, b \in \mathbb{Z}$

Group

Example

Which is a group?

1. $(\mathbb{Z}, *)$ *where* $a * b = a + b + 1$, $a, b \in \mathbb{Z}$
2. $(\mathbb{Z}, *)$ *where* $a * b = 2a + 2b$, $a, b \in \mathbb{Z}$
3. $(\mathbb{Z}, *)$ *where* $a * b = ab^2 + a + b$, $a, b \in \mathbb{Z}$

Group

Example

Which is a group?

1. $(\mathbb{Z}, *)$ *where* $a * b = a + b + 1$, $a, b \in \mathbb{Z}$
2. $(\mathbb{Z}, *)$ *where* $a * b = 2a + 2b$, $a, b \in \mathbb{Z}$
3. $(\mathbb{Z}, *)$ *where* $a * b = ab^2 + a + b$, $a, b \in \mathbb{Z}$

Abelian Group

Definition

A group $(G, *)$ whose binary operation is commutative is called **abelian**. *That is, $a * b = b * a$ for all $a, b \in G$.*

Example

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *are abelian groups under addition.*
2. $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$ *are abelian groups under multiplication.*

Abelian Group

Definition

A group $(G, *)$ whose binary operation is commutative is called **abelian**. *That is, $a * b = b * a$ for all $a, b \in G$.*

Example

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *are abelian groups under addition.*
2. $\mathbb{Q} \backslash \{0\}, \mathbb{R} \backslash \{0\}, \mathbb{C} \backslash \{0\}$ *are abelian groups under multiplication.*

Abelian Group

Definition

A group $(G, *)$ whose binary operation is commutative is called **abelian**. *That is, $a * b = b * a$ for all $a, b \in G$.*

Example

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *are abelian groups under addition.*
2. $\mathbb{Q}\backslash\{0\}, \mathbb{R}\backslash\{0\}, \mathbb{C}\backslash\{0\}$ *are abelian groups under multiplication.*

Abelian Group

Definition

A group $(G, *)$ whose binary operation is commutative is called **abelian**. *That is, $a * b = b * a$ for all $a, b \in G$.*

Example

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *are abelian groups under addition.*
2. $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$ *are abelian groups under multiplication.*

Cayley Table

Remark

If G is a finite group its **Cayley table** *or* **multiplication table** *or* **group table** *can be formed. The rows and columns of the table are labeled by the elements, and the entry in row a and column b is the element $a * b$.*

Example

The Cayley tables for $G = \{1, -1, i, -i\}$ under multiplication and $(Z_4, +)$ are as follows:

$\bullet$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	$-i$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Cayley Table

Remark

If G is a finite group its **Cayley table** *or* **multiplication table** *or* **group table** *can be formed. The rows and columns of the table are labeled by the elements, and the entry in row a and column b is the element $a * b$.*

Example

The Cayley tables for $G = \{1, -1, i, -i\}$ under multiplication and $(Z_4, +)$ are as follows:

$\bullet$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	$-i$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Cayley Table

Remark

A Cayley table for a set G can be used to determine if $(G, *)$ *is a group. Consider for example the set* $G = \{\ a,\ b,\ c,\ d\ \}$ *whose Cayley table is shown below:*

*	a	b	c	d
a	b	c	b	a
b	a	c	b	d
c	c	b	a	d
d	d	a	c	b

Clearly, G is closed under $*$ *since every entry in each row and column is an element of G. However, there is no identity element in G.*

Outline

Theorem

(Uniqueness of the Identity Element): *In a group G, the identity element is unique.*

Theorem

(Uniqueness of the Inverse): *If G is a group, then each element of G has a unique inverse.*

Elementary Properties of Groups

Theorem

(Uniqueness of the Identity Element): *In a group G, the identity element is unique.*

Theorem

(Uniqueness of the Inverse): *If G is a group, then each element of G has a unique inverse.*

Elementary Properties of Groups

Theorem

(Uniqueness of Solutions): *If G is a group and $a, b \in G$, then the equation $ax = b$ has the unique solution $x = a^{-1}b$; similarly the equation $xa = b$ has the unique solution $x = ba^{-1}$.*

Corollary

(Cancelation Laws): *If G is a group and $a, b, c \in G$ with $ab = ac$ or $ba = ca$, then $b = c$.*

Theorem

(Uniqueness of Solutions): *If G is a group and $a, b \in G$, then the equation $ax = b$ has the unique solution $x = a^{-1}b$; similarly the equation $xa = b$ has the unique solution $x = ba^{-1}$.*

Corollary

(Cancelation Laws): *If G is a group and $a, b, c \in G$ with $ab = ac$ or $ba = ca$, then $b = c$.*

Elementary Properties of Groups

Corollary

If G is a group with identity e, and $a, b \in G$ with $ab = e$, then $b = a^{-1}$ and $a = b^{-1}$.

Corollary

Given an element a of a group G, as x runs through the elements of G, the elements ax are just the elements of G in some order, without repetitions; the same is true of the elements xa.

Elementary Properties of Groups

Corollary

If G is a group with identity e, and $a, b \in G$ with $ab = e$, then $b = a^{-1}$ and $a = b^{-1}$.

Corollary

Given an element a of a group G, as x runs through the elements of G, the elements ax are just the elements of G in some order, without repetitions; the same is true of the elements xa.

Elementary Properties of Groups

Example

Fill up the following Cayley table.

$*$	v	w	x	y	z
v			w		
w	z				x
x		y			
y					
z					

Theorem

(Inverse of a Product): *If a and b are elements of a group G, then*

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

Outline

Finite Groups

Definition

If a group G has a finite number of elements, G is called a **finite group***, or a* **group of finite order.** *The number of elements in G is called the* **order** *of G, and is denoted by $|G|$ or by $o(G)$. If G does not have a finite number of elements, G is called an* **infinite order** *or a* **group of infinite order***.*

Finite Groups

Example

1. $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+)$ *and* $(\mathbb{C},+)$ *are groups of infinite order.*
2. $G=\{1,-1,i,-i\}$ *under multiplication is a group of order 4.*
3. $G=(Z_6,+)$ *is a finite group of order 6.*
4. *The Klein 4-group with the group table below is of order 4.*

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Example

1. $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+)$ *and* $(\mathbb{C},+)$ *are groups of infinite order.*
2. $G=\{1,-1,i,-i\}$ *under multiplication is a group of order 4.*
3. $G=(Z_6,+)$ *is a finite group of order 6.*
4. *The Klein 4-group with the group table below is of order 4.*

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Finite Groups

Example

1. $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+)$ *and* $(\mathbb{C},+)$ *are groups of infinite order.*
2. $G=\{1,-1,i,-i\}$ *under multiplication is a group of order 4.*
3. $G=(Z_6,+)$ *is a finite group of order 6.*
4. *The Klein 4-group with the group table below is of order 4.*

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Finite Groups

Example

1. $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+)$ *and* $(\mathbb{C},+)$ *are groups of infinite order.*
2. $G=\{1,-1,i,-i\}$ *under multiplication is a group of order 4.*
3. $G=(Z_6,+)$ *is a finite group of order 6.*
4. *The Klein 4-group with the group table below is of order 4.*

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Example

1. $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+)$ *and* $(\mathbb{C},+)$ *are groups of infinite order.*
2. $G=\{1,-1,i,-i\}$ *under multiplication is a group of order 4.*
3. $G=(Z_6,+)$ *is a finite group of order 6.*
4. *The Klein 4-group with the group table below is of order 4.*

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Definition

Let G be a group, $a \in G$ *and* $n \in \mathbb{Z}^+$. *Then we write*

$$\begin{aligned} a^n &= a \cdot a \cdots a \ (n \text{ terms}) \\ a^0 &= e \\ a^{-n} &= (a^{-1})^n = (a^{-1}) \cdot (a^{-1}) \cdots (a^{-1}) \ (n \text{ terms}) \end{aligned}$$

Then clearly $a^m \cdot a^n = a^{m+n}$ *and* $a^m \cdot a^{-n} = a^{m-n}$ *and* $(a^n)^{-1} = a^{-n}$. *The elements* a^n *for* $n \in \mathbb{Z}^+$ *are called* **powers** *of a. In an additive group we write na instead of* a^n, *and call such elements* **multiples** *of a.*

Finite Groups

Example

Let $G = (Z_4, +)$ *and let* $a = 3$. *Then*

$$\begin{aligned}
3^0 &= e = 0 \\
3^1 &= 3 \\
3^2 &= 3 + 3 = 2 \\
3^3 &= 3 + 3 + 3 = 1 \\
3^4 &= 3 + 3 + 3 + 3 = 0 \\
3^{-3} &= (3^{-1})^3 = 1^3 = 1 + 1 + 1 = 3 \\
3^2 + 3^2 &= 2 + 2 = 0 = 3^4 \\
3^2 + 3^{-3} &= 2 + 3 = 1 = 3^{-1}
\end{aligned}$$

Finite Groups

Definition

Let G be a group and let $a \in G$. The smallest positive integer n such that

$$a^n = e$$

is called the **order** *of a. This is denoted by $|a|$ or by $o(a)$. If no such integer exists, then a is said to be of* **infinite order**.

Example

Let $G = (Z_4, +)$. Then $e = 0$ and we have

1. $0^1 = 0$, *so* $o(0) = 1$
2. $1^1 = 1, 1^2 = 2, 1^3 = 3, 1^4 = 0$, *so* $o(1) = 4$
3. $2^1 = 2, 2^2 = 0$, *and* $o(2) = 2$
4. $3^1 = 3, 3^2 = 2, 3^3 = 1, 3^4 = 0$, *and* $o(3) = 4$

Finite Groups

Definition

Let G be a group and let $a \in G$. The smallest positive integer n such that

$$a^n = e$$

is called the **order** *of a. This is denoted by $|a|$ or by $o(a)$. If no such integer exists, then a is said to be of* **infinite order**.

Example

Let $G = (Z_4, +)$. Then $e = 0$ and we have

1. $0^1 = 0$, *so* $o(0) = 1$
2. $1^1 = 1, 1^2 = 2, 1^3 = 3, 1^4 = 0$, *so* $o(1) = 4$
3. $2^1 = 2, 2^2 = 0$, *and* $o(2) = 2$
4. $3^1 = 3, 3^2 = 2, 3^3 = 1, 3^4 = 0$, *and* $o(3) = 4$

Finite Groups

Definition

Let G be a group and let $a \in G$. The smallest positive integer n such that

$$a^n = e$$

is called the **order** *of a. This is denoted by $|a|$ or by $o(a)$. If no such integer exists, then a is said to be of* **infinite order**.

Example

Let $G = (Z_4, +)$. Then $e = 0$ and we have

1. $0^1 = 0$, *so* $o(0) = 1$
2. $1^1 = 1, 1^2 = 2, 1^3 = 3, 1^4 = 0$, *so* $o(1) = 4$
3. $2^1 = 2, 2^2 = 0$, *and* $o(2) = 2$
4. $3^1 = 3, 3^2 = 2, 3^3 = 1, 3^4 = 0$, *and* $o(3) = 4$

Finite Groups

Definition

Let G be a group and let $a \in G$. The smallest positive integer n such that

$$a^n = e$$

is called the **order** *of a. This is denoted by $|a|$ or by $o(a)$. If no such integer exists, then a is said to be of* **infinite order**.

Example

Let $G = (Z_4, +)$. Then $e = 0$ and we have

1. $0^1 = 0$, *so* $o(0) = 1$
2. $1^1 = 1, 1^2 = 2, 1^3 = 3, 1^4 = 0$, *so* $o(1) = 4$
3. $2^1 = 2, 2^2 = 0$, *and* $o(2) = 2$
4. $3^1 = 3, 3^2 = 2, 3^3 = 1, 3^4 = 0$, *and* $o(3) = 4$

Finite Groups

Definition

Let G be a group and let $a \in G$. The smallest positive integer n such that

$$a^n = e$$

is called the **order** *of a. This is denoted by $|a|$ or by $o(a)$. If no such integer exists, then a is said to be of* **infinite order**.

Example

Let $G = (Z_4, +)$. Then $e = 0$ and we have

1. $0^1 = 0$, *so* $o(0) = 1$
2. $1^1 = 1, 1^2 = 2, 1^3 = 3, 1^4 = 0$, *so* $o(1) = 4$
3. $2^1 = 2, 2^2 = 0$, *and* $o(2) = 2$
4. $3^1 = 3, 3^2 = 2, 3^3 = 1, 3^4 = 0$, *and* $o(3) = 4$

Finite Groups

Definition

Let G be a group and let $a \in G$. The smallest positive integer n such that

$$a^n = e$$

is called the **order** *of a. This is denoted by $|a|$ or by $o(a)$. If no such integer exists, then a is said to be of* **infinite order**.

Example

Let $G = (Z_4, +)$. Then $e = 0$ and we have

1. $0^1 = 0$, *so* $o(0) = 1$
2. $1^1 = 1, 1^2 = 2, 1^3 = 3, 1^4 = 0$, *so* $o(1) = 4$
3. $2^1 = 2, 2^2 = 0$, *and* $o(2) = 2$
4. $3^1 = 3, 3^2 = 2, 3^3 = 1, 3^4 = 0$, *and* $o(3) = 4$

Finite Groups

Example

Given the Cayley table below, we have $e = y$.

$*$	v	w	x	y	z
v	x	z	w	v	y
w	z	v	y	w	x
x	w	y	z	x	v
y	v	w	x	y	z
z	y	x	v	z	w

1. $v^1 = v, v^2 = x, v^3 = w, v^4 = z, v^5 = y$, and $o(v) = 5$
2. $w^1 = w, w^2 = v, w^3 = z, w^4 = x, w^5 = y$, and $o(w) = 5$
3. $x^1 = x, x^2 = z, x^3 = v, x^4 = w, x^5 = y$, and $o(x) = 5$
4. $y^1 = y$, and $o(y) = 1$
5. $z^1 = z, z^2 = w, z^3 = x, z^4 = v, z^5 = y$, and $o(z) = 5$

Finite Groups

Example

Given the Cayley table below, we have $e = y$.

$*$	v	w	x	y	z
v	x	z	w	v	y
w	z	v	y	w	x
x	w	y	z	x	v
y	v	w	x	y	z
z	y	x	v	z	w

1. $v^1 = v, v^2 = x, v^3 = w, v^4 = z, v^5 = y$, and $o(v) = 5$
2. $w^1 = w, w^2 = v, w^3 = z, w^4 = x, w^5 = y$, and $o(w) = 5$
3. $x^1 = x, x^2 = z, x^3 = v, x^4 = w, x^5 = y$, and $o(x) = 5$
4. $y^1 = y$, and $o(y) = 1$
5. $z^1 = z, z^2 = w, z^3 = x, z^4 = v, z^5 = y$, and $o(z) = 5$

Example

Given the Cayley table below, we have $e = y$.

$*$	v	w	x	y	z
v	x	z	w	v	y
w	z	v	y	w	x
x	w	y	z	x	v
y	v	w	x	y	z
z	y	x	v	z	w

1. $v^1 = v, v^2 = x, v^3 = w, v^4 = z, v^5 = y$, and $o(v) = 5$
2. $w^1 = w, w^2 = v, w^3 = z, w^4 = x, w^5 = y$, and $o(w) = 5$
3. $x^1 = x, x^2 = z, x^3 = v, x^4 = w, x^5 = y$, and $o(x) = 5$
4. $y^1 = y$, and $o(y) = 1$
5. $z^1 = z, z^2 = w, z^3 = x, z^4 = v, z^5 = y$, and $o(z) = 5$

Example

Given the Cayley table below, we have $e = y$.

$*$	v	w	x	y	z
v	x	z	w	v	y
w	z	v	y	w	x
x	w	y	z	x	v
y	v	w	x	y	z
z	y	x	v	z	w

1. $v^1 = v, v^2 = x, v^3 = w, v^4 = z, v^5 = y$, *and* $o(v) = 5$
2. $w^1 = w, w^2 = v, w^3 = z, w^4 = x, w^5 = y$, *and* $o(w) = 5$
3. $x^1 = x, x^2 = z, x^3 = v, x^4 = w, x^5 = y$, *and* $o(x) = 5$
4. $y^1 = y$, *and* $o(y) = 1$
5. $z^1 = z, z^2 = w, z^3 = x, z^4 = v, z^5 = y$, *and* $o(z) = 5$

Example

Given the Cayley table below, we have $e = y$.

$*$	v	w	x	y	z
v	x	z	w	v	y
w	z	v	y	w	x
x	w	y	z	x	v
y	v	w	x	y	z
z	y	x	v	z	w

1. $v^1 = v, v^2 = x, v^3 = w, v^4 = z, v^5 = y$, and $o(v) = 5$
2. $w^1 = w, w^2 = v, w^3 = z, w^4 = x, w^5 = y$, and $o(w) = 5$
3. $x^1 = x, x^2 = z, x^3 = v, x^4 = w, x^5 = y$, and $o(x) = 5$
4. $y^1 = y$, and $o(y) = 1$
5. $z^1 = z, z^2 = w, z^3 = x, z^4 = v, z^5 = y$, and $o(z) = 5$

Finite Groups

Example

Given the Cayley table below, we have $e = y$.

$*$	v	w	x	y	z
v	x	z	w	v	y
w	z	v	y	w	x
x	w	y	z	x	v
y	v	w	x	y	z
z	y	x	v	z	w

1. $v^1 = v, v^2 = x, v^3 = w, v^4 = z, v^5 = y$, *and* $o(v) = 5$
2. $w^1 = w, w^2 = v, w^3 = z, w^4 = x, w^5 = y$, *and* $o(w) = 5$
3. $x^1 = x, x^2 = z, x^3 = v, x^4 = w, x^5 = y$, *and* $o(x) = 5$
4. $y^1 = y$, *and* $o(y) = 1$
5. $z^1 = z, z^2 = w, z^3 = x, z^4 = v, z^5 = y$, *and* $o(z) = 5$

Finite Groups

Example

Let $G = (\mathbb{R}^*, \bullet)$, so that $e = 1$. Then $o(1) = 1$. If $a \in \mathbb{R}^*$ and $a \neq 1$, then $a^n = aa \cdots a \neq 1$ for any positive integer n, so that $o(a) = +\infty$. This shows that in G, there is one element of order 1 and all the other elements are of infinite order.

Outline

Subgroups

Definition

Let G be a group with respect to the binary operation $*$. A nonempty subset H of G is called a **subgroup** *of G if H forms a group with respect to the binary operation $*$ that is defined in G.*

Example

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *are groups under addition. Hence,* $(\mathbb{Z}, +)$ *is a subgroup of* $(\mathbb{Q}, +)$ *and both are subgroups of* $(\mathbb{R}, +)$ *.*
2. $\mathbb{C}^*$ *is a group under multiplication, and* $G = \{1, -1, i, -i\}$ *is a subgroup of this group.*
3. *Let* $G = (Z_4, +)$ *and let* $H = \{0, 2\}$*. Given the group table for* $(H, +)$ *as shown below, it is clear that* H *is a subgroup of* G*.*

+	0	2
0	0	2
2	2	0

However, H *under this binary operation is not a subgroup of* $(\mathbb{Z}, +)$ *since the binary operations are different.*

Subgroups

Example

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *are groups under addition. Hence,* $(\mathbb{Z}, +)$ *is a subgroup of* $(\mathbb{Q}, +)$ *and both are subgroups of* $(\mathbb{R}, +)$ *.*
2. $\mathbb{C}^*$ *is a group under multiplication, and* $G = \{1, -1, i, -i\}$ *is a subgroup of this group.*
3. *Let* $G = (Z_4, +)$ *and let* $H = \{0, 2\}$*. Given the group table for* $(H, +)$ *as shown below, it is clear that H is a subgroup of G.*

+	0	2
0	0	2
2	2	0

However, H under this binary operation is not a subgroup of $(\mathbb{Z}, +)$ *since the binary operations are different.*

Subgroups

Example

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *are groups under addition. Hence,* $(\mathbb{Z}, +)$ *is a subgroup of* $(\mathbb{Q}, +)$ *and both are subgroups of* $(\mathbb{R}, +)$ *.*
2. $\mathbb{C}^*$ *is a group under multiplication, and* $G = \{1, -1, i, -i\}$ *is a subgroup of this group.*
3. *Let* $G = (Z_4, +)$ *and let* $H = \{0, 2\}$*. Given the group table for* $(H, +)$ *as shown below, it is clear that* H *is a subgroup of* G*.*

+	0	2
0	0	2
2	2	0

However, H *under this binary operation is not a subgroup of* $(\mathbb{Z}, +)$ *since the binary operations are different.*

Example

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *are groups under addition. Hence,* $(\mathbb{Z}, +)$ *is a subgroup of* $(\mathbb{Q}, +)$ *and both are subgroups of* $(\mathbb{R}, +)$ *.*
2. $\mathbb{C}^*$ *is a group under multiplication, and* $G = \{1, -1, i, -i\}$ *is a subgroup of this group.*
3. *Let* $G = (Z_4, +)$ *and let* $H = \{0, 2\}$*. Given the group table for* $(H, +)$ *as shown below, it is clear that H is a subgroup of G.*

+	0	2
0	0	2
2	2	0

However, H under this binary operation is not a subgroup of $(\mathbb{Z}, +)$ *since the binary operations are different.*

Subgroups

Example

Let $G = (Z_4, +)$ *and let* $H = \{1, 3\}$. *Since* $1 + 3 = 4 \notin H$, *addition modulo 4 is* **not** *a binary operation in* H. *Thus,* H *is not a subgroup of* G.

Subgroups

Definition

The subsets $H = \{e\}$ and $H = G$ are always subgroups of the group G. They are referred to as **trivial** *subgroups and other subgroups of G are called* **nontrivial**. *If $H \neq G$, then H is a* **proper subgroup** *of G and we write $H < G$*

Subgroups

Example

1. $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +)$.
2. $G = (\{1, -1, i, -i\}, \bullet)$ *is a nontrivial subgroup of* $(\mathbb{C}^*, \bullet)$.
3. $H = (\{0, 2\}, +) < G = (Z_4, +)$.

Subgroups

Example

1. $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +)$.
2. $G = (\{1, -1, i, -i\}, \bullet)$ *is a nontrivial subgroup of* $(\mathbb{C}^*, \bullet)$.
3. $H = (\{0, 2\}, +) < G = (Z_4, +)$.

Subgroups

Example

1. $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +)$.
2. $G = (\{1, -1, i, -i\}, \bullet)$ *is a nontrivial subgroup of* $(\mathbb{C}^*, \bullet)$.
3. $H = (\{0, 2\}, +) < G = (Z_4, +)$.

Subgroups

Example

1. $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +)$.
2. $G = (\{1, -1, i, -i\}, \bullet)$ *is a nontrivial subgroup of* $(\mathbb{C}^*, \bullet)$.
3. $H = (\{0, 2\}, +) < G = (Z_4, +)$.

Outline

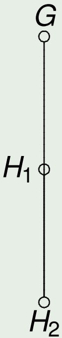
Subgroup Lattice

The relationship between the various subgroups of a group can be illustrated with a **subgroup lattice** of the group. This is a diagram that includes all the subgroups of the group and connects a subgroups H_i at one level to a subgroup H_k at a higher level with a sequence of line segments if and only if H_i is a proper subgroup of H_j.

Subgroup Lattice

Example

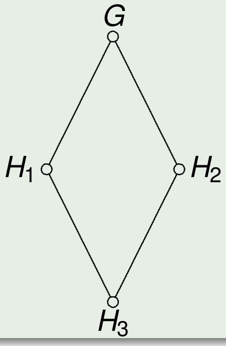
Let $G = (\{1, -1, i, -i\}, \bullet)$. *Then the subgroups of* G *are* G, $H_1 = \{1, -1\}$, *and* $H_2 = \{1\}$. *Hence,* $H_2 < H_1 < G$ *and the subgroup lattice is*



Subgroup Lattice

Example

Let $G = (Z_6, +)$. Then the subgroups of G are G, $H_1 = \{0, 2, 4\}$, $H_2 = \{0, 3\}$, and $H_3 = \{0\}$. Hence, $H_3 < H_1 < G$ and $H_3 < H_2 < G$. The subgroup lattice is



Outline

Tests for Subgroups

Theorem

(Two-Step Test): *A nonempty subset H of a group G is a subgroup of G if and only if*

1. $a, b \in H$ *implies that* $ab \in H$.
2. $a \in H$ *implies that* $a^{-1} \in H$.

Theorem

(One-Step Test): *A nonempty subset H of a group G is a subgroup of G if and only if for all* $a, b \in H$, $ab^{-1} \in H$.

Tests for Subgroups

Theorem

(Two-Step Test): *A nonempty subset H of a group G is a subgroup of G if and only if*

1. $a, b \in H$ *implies that* $ab \in H$.
2. $a \in H$ *implies that* $a^{-1} \in H$.

Theorem

(One-Step Test): *A nonempty subset H of a group G is a subgroup of G if and only if for all* $a, b \in H$, $ab^{-1} \in H$.

Example

Let G be an abelian group and $H = \{x \in G | x^2 = e\}$. Using the Two-Step Test, $H \leq G$.

1. Let $x, y \in H$. Then $x^2 = e, y^2 = e$.

$$\begin{aligned} (xy)^2 &= (xy)(xy) \\ &= x(yx)y && \text{by associativity} \\ &= x(xy)y && \text{since } G \text{ is abelian} \\ &= x^2y^2 \\ &= e && \text{Hence, } xy \in H. \end{aligned}$$

2. Let $x \in H$.

$$\begin{aligned} (x^{-1})^2 &= (x^2)^{-1} \\ &= e && \text{Then, } x^{-1} \in H. \end{aligned}$$

Tests for Subgroups

Example

Let G be an abelian group and $H = \{x \in G | x^2 = e\}$. Using the Two-Step Test, $H \leq G$.

1. *Let $x, y \in H$. Then $x^2 = e, y^2 = e$.*

$$\begin{aligned} (xy)^2 &= (xy)(xy) \\ &= x(yx)y && \text{by associativity} \\ &= x(xy)y && \text{since } G \text{ is abelian} \\ &= x^2y^2 \\ &= e && \text{Hence, } xy \in H. \end{aligned}$$

2. *Let $x \in H$.*

$$\begin{aligned} (x^{-1})^2 &= (x^2)^{-1} \\ &= e && \text{Then, } x^{-1} \in H. \end{aligned}$$

Example

Let G be an abelian group and $H = \{x \in G | x^2 = e\}$. Using the Two-Step Test, $H \leq G$.

1. *Let $x, y \in H$. Then $x^2 = e, y^2 = e$.*

$$\begin{aligned}(xy)^2 &= (xy)(xy) && \\ &= x(yx)y && \text{by associativity} \\ &= x(xy)y && \text{since } G \text{ is abelian} \\ &= x^2y^2 && \\ &= e && \text{Hence, } xy \in H.\end{aligned}$$

2. *Let $x \in H$.*

$$\begin{aligned}(x^{-1})^2 &= (x^2)^{-1} && \\ &= e && \text{Then, } x^{-1} \in H.\end{aligned}$$

Example

We now show that $H \leq G$ using the One-Step Test where G is an abelian group and $H = \{x \in G | x^2 = e\}$.

Let $x, y \in H$.

$$\begin{aligned} (xy^{-1})^2 &= (xy^{-1})(xy^{-1}) & \\ &= x(y^{-1}x)y^{-1} & \text{by associativity} \\ &= x(xy^{-1})y^{-1} & \text{since } G \text{ is abelian} \\ &= x^2(y^{-1})^2 & \\ &= e & \end{aligned}$$

Therefore, $xy^{-1} \in H$.

Example

We now show that $H \leq G$ using the One-Step Test where G is an abelian group and $H = \{x \in G | x^2 = e\}$.

Let $x, y \in H$.

$$
\begin{aligned}
(xy^{-1})^2 &= (xy^{-1})(xy^{-1}) && \\
&= x(y^{-1}x)y^{-1} && \text{by associativity} \\
&= x(xy^{-1})y^{-1} && \text{since } G \text{ is abelian} \\
&= x^2(y^{-1})^2 && \\
&= e &&
\end{aligned}
$$

Therefore, $xy^{-1} \in H$.

Example

We show that $4\mathbb{Z}$ is a subgroup of the additive group $\mathbb{Z}$ by the one-step test. Let $x, y \in 4\mathbb{Z}$, then $x = 4m, y = 4n$ where $m, n \in \mathbb{Z}$. Given $4n \in \mathbb{Z}$, then its inverse is $-4n = 4(-n)$. Hence, $4m + (-4n) = 4m + 4(-n) = 4(m - n) \in 4\mathbb{Z}$.

Tests for Subgroups

Theorem

The intersection of any family of subgroups of G is itself a subgroup of G.

Example

If $G = \mathbb{Z}$, the intersection of the subgroups $3\mathbb{Z}$ and $4\mathbb{Z}$ is the subgroup $12\mathbb{Z}$, since the numbers which are multiples of both 3 and 4 are the multiples of 12; the intersection of all subgroups $m\mathbb{Z}$ for $m \in \mathbb{Z}^+$ is the identity subgroup $\{0\}$, as no non-zero number is a multiple of all positive integers.

Tests for Subgroups

Theorem

The intersection of any family of subgroups of G is itself a subgroup of G.

Example

If $G = \mathbb{Z}$, the intersection of the subgroups $3\mathbb{Z}$ and $4\mathbb{Z}$ is the subgroup $12\mathbb{Z}$, since the numbers which are multiples of both 3 and 4 are the multiples of 12; the intersection of all subgroups $m\mathbb{Z}$ for $m \in \mathbb{Z}^+$ is the identity subgroup $\{0\}$, as no non-zero number is a multiple of all positive integers.

Outline

1. Groups and Subgroups
   - Binary Operations
   - Groups: Definition and Examples
   - Elementary Properties of Groups
   - Finite Groups
   - Subgroups
   - Subgroup Lattice
   - Tests for Subgroups
   - Centers and Centralizers

Centers and Centralizers

Definition

If $g, h \in G$ and $gh = hg$, we say that g and h **commute** *or* **centralize** *each other.*

Example

1. *In an abelian group any two elements commute.*
2. *In any group G, e commutes with every element of G.*

Centers and Centralizers

Definition

If $g, h \in G$ and $gh = hg$, we say that g and h **commute** *or* **centralize** *each other.*

Example

1. *In an abelian group any two elements commute.*
2. *In any group G, e commutes with every element of G.*

Centers and Centralizers

Definition

If $g, h \in G$ and $gh = hg$, we say that g and h **commute** *or* **centralize** *each other.*

Example

1. *In an abelian group any two elements commute.*
2. *In any group G, e commutes with every element of G.*

Centers and Centralizers

Definition

If $g, h \in G$ and $gh = hg$, we say that g and h **commute** *or* **centralize** *each other.*

Example

1. *In an abelian group any two elements commute.*
2. *In any group G, e commutes with every element of G.*

Centers and Centralizers

Theorem

If $g, h \in G$ commute then $gh^n = h^n g$ and $(gh)^n = g^n h^n$ for all $n \in \mathbb{Z}^+$.

Definition

Given $g \in G$, the **centralizer** *of g in G is the set $C(a) = \{x \in G | xg = gx\}$ of all elements of G which commute with g.*

Example

In any abelian group G, $C(a) = G$ for all $a \in G$.

Centers and Centralizers

Theorem

If $g, h \in G$ commute then $gh^n = h^n g$ and $(gh)^n = g^n h^n$ for all $n \in \mathbb{Z}^+$.

Definition

Given $g \in G$, the **centralizer** *of g in G is the set $C(a) = \{x \in G | xg = gx\}$ of all elements of G which commute with g.*

Example

In any abelian group G, $C(a) = G$ for all $a \in G$.

Theorem

If $g, h \in G$ commute then $gh^n = h^n g$ and $(gh)^n = g^n h^n$ for all $n \in \mathbb{Z}^+$.

Definition

Given $g \in G$, the **centralizer** *of g in G is the set $C(a) = \{x \in G | xg = gx\}$ of all elements of G which commute with g.*

Example

In any abelian group G, $C(a) = G$ for all $a \in G$.

Centers and Centralizers

Example

Given the group table for $(G, *)$,

$*$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	f	e	d	c
c	c	d	a	b	f	e
d	d	c	e	f	b	a
e	e	f	d	c	a	b
f	f	e	b	a	c	d

1. $C(a) = G$
2. $C(b) = \{a, b\}$
3. $C(c) = \{a, c\}$
4. $C(d) = \{a, d, f\}$
5. $C(e) = \{a, e\}$
6. $C(f) = \{a, d, f\}$

Centers and Centralizers

Example

Given the group table for $(G, *)$,

$*$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	f	e	d	c
c	c	d	a	b	f	e
d	d	c	e	f	b	a
e	e	f	d	c	a	b
f	f	e	b	a	c	d

1. $C(a) = G$
2. $C(b) = \{a, b\}$
3. $C(c) = \{a, c\}$
4. $C(d) = \{a, d, f\}$
5. $C(e) = \{a, e\}$
6. $C(f) = \{a, d, f\}$

Centers and Centralizers

Example

Given the group table for $(G, *)$,

$*$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	f	e	d	c
c	c	d	a	b	f	e
d	d	c	e	f	b	a
e	e	f	d	c	a	b
f	f	e	b	a	c	d

1. $C(a) = G$
2. $C(b) = \{a, b\}$
3. $C(c) = \{a, c\}$
4. $C(d) = \{a, d, f\}$
5. $C(e) = \{a, e\}$
6. $C(f) = \{a, d, f\}$

Centers and Centralizers

Example

Given the group table for $(G, *)$,

$*$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	f	e	d	c
c	c	d	a	b	f	e
d	d	c	e	f	b	a
e	e	f	d	c	a	b
f	f	e	b	a	c	d

1. $C(a) = G$
2. $C(b) = \{a, b\}$
3. $C(c) = \{a, c\}$
4. $C(d) = \{a, d, f\}$
5. $C(e) = \{a, e\}$
6. $C(f) = \{a, d, f\}$

Centers and Centralizers

Example

Given the group table for $(G, *)$,

$*$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	f	e	d	c
c	c	d	a	b	f	e
d	d	c	e	f	b	a
e	e	f	d	c	a	b
f	f	e	b	a	c	d

1. $C(a) = G$
2. $C(b) = \{a, b\}$
3. $C(c) = \{a, c\}$
4. $C(d) = \{a, d, f\}$
5. $C(e) = \{a, e\}$
6. $C(f) = \{a, d, f\}$

Centers and Centralizers

Example

Given the group table for $(G, *)$,

$*$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	f	e	d	c
c	c	d	a	b	f	e
d	d	c	e	f	b	a
e	e	f	d	c	a	b
f	f	e	b	a	c	d

1. $C(a) = G$
2. $C(b) = \{a, b\}$
3. $C(c) = \{a, c\}$
4. $C(d) = \{a, d, f\}$
5. $C(e) = \{a, e\}$
6. $C(f) = \{a, d, f\}$

Example

Given the group table for $(G, *)$,

$*$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	f	e	d	c
c	c	d	a	b	f	e
d	d	c	e	f	b	a
e	e	f	d	c	a	b
f	f	e	b	a	c	d

1. $C(a) = G$
2. $C(b) = \{a, b\}$
3. $C(c) = \{a, c\}$
4. $C(d) = \{a, d, f\}$
5. $C(e) = \{a, e\}$
6. $C(f) = \{a, d, f\}$

Centers and Centralizers

Theorem

If $g \in G$ then $C(g)$ is a subgroup of G.

Definition

The **center** *$Z(G)$ of G is the intersection of all subgroups $C(g)$ as g runs through G.*

Example

$Z(G) = G$ for any abelian group G since $C(a) = G$ for all $a \in G$.

Remark

By theorem 2.7, we see that $Z(G)$ is also a subgroup of G; it consists of those elements which commute with every element of G. It is clear that G is abelian if and only if $Z(G) = G$.