Part I

Abstract Algebra

Definition

Given a set G and a binary operation $*$ on G. For any elements a, b, and c in G

1. Closure: $a * b \in G$
2. Associative: $(a * b) * c = a * (b * c)$
3. Identity: a unique element $e \in G$ such that
   - $a * e = e * a = a$
4. Inverse: an element $a' \in G$ of a, written as a^{-1}, such that
   - $a * a' = a' * a = e$, or
   - $a * a^{-1} = a^{-1} * a = e$
5. Commutative: $a * b = b * a$

Definition

Given a set G and a binary operation $*$ on G. For any elements a, b, and c in G

1. Closure: $a * b \in G$
2. Associative: $(a * b) * c = a * (b * c)$
3. Identity: a unique element $e \in G$ such that
   - $a * e = e * a = a$
4. Inverse: an element $a' \in G$ of a, written as a^{-1}, such that
   - $a * a' = a' * a = e$, or
   - $a * a^{-1} = a^{-1} * a = e$
5. Commutative: $a * b = b * a$

Definition

Given a set G and a binary operation $*$ on G. For any elements a, b, and c in G

1. Closure: $a * b \in G$
2. Associative: $(a * b) * c = a * (b * c)$
3. Identity: a unique element $e \in G$ such that
   - $a * e = e * a = a$
4. Inverse: an element $a' \in G$ of a, written as a^{-1}, such that
   - $a * a' = a' * a = e$, or
   - $a * a^{-1} = a^{-1} * a = e$
5. Commutative: $a * b = b * a$

Definition

Given a set G and a binary operation $*$ on G. For any elements a, b, and c in G

1. Closure: $a * b \in G$
2. Associative: $(a * b) * c = a * (b * c)$
3. Identity: a unique element $e \in G$ such that
   - $a * e = e * a = a$
4. Inverse: an element $a' \in G$ of a, written as a^{-1}, such that
   - $a * a' = a' * a = e$, or
   - $a * a^{-1} = a^{-1} * a = e$
5. Commutative: $a * b = b * a$

Definition

Given a set G and a binary operation $*$ on G. For any elements a, b, and c in G

1. Closure: $a * b \in G$
2. Associative: $(a * b) * c = a * (b * c)$
3. Identity: a unique element $e \in G$ such that
   - ♫ $a * e = e * a = a$
4. Inverse: an element $a' \in G$ of a, written as a^{-1}, such that
   - ☛ $a * a' = a' * a = e$, or
   - ☛ $a * a^{-1} = a^{-1} * a = e$
5. Commutative: $a * b = b * a$

Definition

Given a set G and a binary operation $*$ on G. For any elements a, b, and c in G

1. Closure: $a * b \in G$
2. Associative: $(a * b) * c = a * (b * c)$
3. Identity: a unique element $e \in G$ such that
   - $a * e = e * a = a$
4. Inverse: an element $a' \in G$ of a, written as a^{-1}, such that
   - $a * a' = a' * a = e$, or
   - $a * a^{-1} = a^{-1} * a = e$
5. Commutative: $a * b = b * a$

Definition

Given a set G and a binary operation $*$ on G. For any elements a, b, and c in G

1. Closure: $a * b \in G$
2. Associative: $(a * b) * c = a * (b * c)$
3. Identity: a unique element $e \in G$ such that
   - $a * e = e * a = a$
4. Inverse: an element $a' \in G$ of a, written as a^{-1}, such that
   - $a * a' = a' * a = e$, or
   - $a * a^{-1} = a^{-1} * a = e$
5. Commutative: $a * b = b * a$

Definition

Given a set G and a binary operation $*$ on G. For any elements a, b, and c in G

1. Closure: $a * b \in G$
2. Associative: $(a * b) * c = a * (b * c)$
3. Identity: a unique element $e \in G$ such that
   - $a * e = e * a = a$
4. Inverse: an element $a' \in G$ of a, written as a^{-1}, such that
   - $a * a' = a' * a = e$, or
   - $a * a^{-1} = a^{-1} * a = e$
5. Commutative: $a * b = b * a$

Definition $(G, *)$

A nonempty set G with a binary operation $*$ is called

- Groupoid,
  - if (1) is true
- Semigroup,
  - if (1)-(2) are true
- Monoid,
  - if (1)-(3) are true
- Group,
  - if (1)-(4) are true
- Abelian groupoid (semigroup, monoid, group),
  - if (5) is true

Definition $(G, *)$

A nonempty set G with a binary operation $*$ is called

- Groupoid,
  - if (1) is true
- Semigroup,
  - if (1)-(2) are true
- Monoid,
  - if (1)-(3) are true
- Group,
  - if (1)-(4) are true
- Abelian groupoid (semigroup, monoid, group),
  - if (5) is true

Definition $(G, *)$

A nonempty set G with a binary operation $*$ is called

- Groupoid,
  - if (1) is true
- Semigroup,
  - if (1)-(2) are true
- Monoid,
  - if (1)-(3) are true
- Group,
  - if (1)-(4) are true
- Abelian groupoid (semigroup, monoid, group),
  - if (5) is true

Definition $(G, *)$

A nonempty set G with a binary operation $*$ is called

- Groupoid,
  - if (1) is true
- Semigroup,
  - if (1)-(2) are true
- Monoid,
  - if (1)-(3) are true
- Group,
  - if (1)-(4) are true
- Abelian groupoid (semigroup, monoid, group),
  - if (5) is true

Definition $(G, *)$

A nonempty set G with a binary operation $*$ is called

- Groupoid,
  - if (1) is true
- Semigroup,
  - if (1)-(2) are true
- Monoid,
  - if (1)-(3) are true
- Group,
  - if (1)-(4) are true
- Abelian groupoid (semigroup, monoid, group),
  - if (5) is true

Definition $(G, *)$

A nonempty set G with a binary operation $*$ is called

- Groupoid,
  - if (1) is true
- Semigroup,
  - if (1)-(2) are true
- Monoid,
  - if (1)-(3) are true
- Group,
  - if (1)-(4) are true
- Abelian groupoid (semigroup, monoid, group),
  - if (5) is true

Definition $(G, *)$

A nonempty set G with a binary operation $*$ is called

- Groupoid,
  - if (1) is true
- Semigroup,
  - if (1)-(2) are true
- Monoid,
  - if (1)-(3) are true
- Group,
  - if (1)-(4) are true
- Abelian groupoid (semigroup, monoid, group),
  - if (5) is true

Definition $(G, *)$

A nonempty set G with a binary operation $*$ is called

- Groupoid,
  - if (1) is true
- Semigroup,
  - if (1)-(2) are true
- Monoid,
  - if (1)-(3) are true
- Group,
  - if (1)-(4) are true
- Abelian groupoid (semigroup, monoid, group),
  - if (5) is true

Definition $(G, *)$

A nonempty set G with a binary operation $*$ is called

- Groupoid,
  - if (1) is true
- Semigroup,
  - if (1)-(2) are true
- Monoid,
  - if (1)-(3) are true
- Group,
  - if (1)-(4) are true
- Abelian groupoid (semigroup, monoid, group),
  - if (5) is true

Definition $(G, *)$

A nonempty set G with a binary operation $*$ is called

- Groupoid,
  - if (1) is true
- Semigroup,
  - if (1)-(2) are true
- Monoid,
  - if (1)-(3) are true
- Group,
  - if (1)-(4) are true
- Abelian groupoid (semigroup, monoid, group),
  - if (5) is true

Theorem (Associativity)

- *If $a_1, a_2, \ldots, a_n, n \geqslant 3$, are arbitrary elements of a semigroup, then all products of the elements $a_1, a_2, \ldots, a_n$ that can be formed by inserting meaningful parentheses arbitrarily are equal.*

Notice

- The Theorem shows that the products are all equal.
  - $((a_1 * a_2) * a_3) * a_4$
  - $a_1 * (a_2 * (a_3 * a_4))$
  - $(a_1 * (a_2 * a_3)) * a_4$
- If $a_1, a_2, \ldots, a_n$ are elements in a semigroup $(S, *)$, then the product can be written as
  - $a_1 * a_2 * \cdots * a_n$

Theorem (Associativity)

- *If* $a_1, a_2, \ldots, a_n, n \geqslant 3$, *are arbitrary elements of a semigroup, then all products of the elements* $a_1, a_2, \ldots, a_n$ *that can be formed by inserting meaningful parentheses arbitrarily are equal.*

Notice

- The Theorem shows that the products are all equal.
  - $((a_1 * a_2) * a_3) * a_4$
  - $a_1 * (a_2 * (a_3 * a_4))$
  - $(a_1 * (a_2 * a_3)) * a_4$
- If $a_1, a_2, \ldots, a_n$ are elements in a semigroup $(S, *)$, then the product can be written as
  - $a_1 * a_2 * \cdots * a_n$

$(\mathbb{Z}, +)$

- $\mathbb{Z}$: the set of all integers
- $+$: ordinary addition

$(\mathbb{Z}, -)$

- $\mathbb{Z}$: the set of all integers
- $-$: ordinary subtraction

$(\mathscr{P}(S), \cup)$

- $(\mathscr{P}(S)$: the powerset of S
- $\cup$: union operation on sets

$(\mathbb{Z}, +)$

- $\mathbb{Z}$: the set of all integers
- $+$: ordinary addition

$(\mathbb{Z}, -)$

- $\mathbb{Z}$: the set of all integers
- $-$: ordinary subtraction

$(\mathscr{P}(S), \cup)$

- $(\mathscr{P}(S)$: the powerset of S
- $\cup$: union operation on sets

$(\mathbb{Z}, +)$

- $\mathbb{Z}$: the set of all integers
- $+$: ordinary addition

$(\mathbb{Z}, -)$

- $\mathbb{Z}$: the set of all integers
- $-$: ordinary subtraction

$(\mathscr{P}(S), \cup)$

- $(\mathscr{P}(S)$: the powerset of S
- $\cup$: union operation on sets

Definition (Let $A = \{a_1, a_2, ..., a_n\}$ be an alphabet)

- Let
  - A^* is the set of all finite sequences of elements of A.
  - α, β, and γ be elements of A^*.
- The catenation is a binary operation $\cdot$ on A^*.
  - if $\alpha = a_{i_1} a_{i_2} \ldots a_{i_s}$ and $\beta = a_{j_1} a_{j_2} \ldots a_{j_t}$, then
    - $\alpha \cdot \beta = a_{i_1} a_{i_2} \ldots a_{i_s} a_{j_1} a_{j_2} \ldots a_{j_t}$
  - $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$

Definition (Let $A = \{a_1, a_2, ..., a_n\}$ be an alphabet)

- Let
  - A^* is the set of all finite sequences of elements of A.
  - α, β, and γ be elements of A^*.
- The catenation is a binary operation $\cdot$ on A^*.
  - if $\alpha = a_{i_1} a_{i_2} \ldots a_{i_s}$ and $\beta = a_{j_1} a_{j_2} \ldots a_{j_t}$, then
    - $\alpha \cdot \beta = a_{i_1} a_{i_2} \ldots a_{i_s} a_{j_1} a_{j_2} \ldots a_{j_t}$
  - $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$

Definition (Let $A = \{a_1, a_2, ..., a_n\}$ be an alphabet)

- Let
  - A^* is the set of all finite sequences of elements of A.
  - α, β, and γ be elements of A^*.
- The catenation is a binary operation $\cdot$ on A^*.
  - if $\alpha = a_{i_1} a_{i_2} \dots a_{i_s}$ and $\beta = a_{j_1} a_{j_2} \dots a_{j_t}$, then
    - $\alpha \cdot \beta = a_{i_1} a_{i_2} \dots a_{i_s} a_{j_1} a_{j_2} \dots a_{j_t}$
  - ☛ $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$

Theorem (Free Semigroup)

- $(A^*, \cdot)$ *is a semigroup*
    - *called the free semigroup generated by* A

Example

- Let
  - G be the set of all nonzero real numbers, and
  - $a * b = ab/2$
- Show
  - $(G, *)$ is an Abelian group

Proof. $*$ is a binary operation.

- If a and b are elements of G, then $ab/2$ is a nonzero real number and hence is in G.

Example

- Let
  - G be the set of all nonzero real numbers, and
  - $a * b = ab/2$
- Show
  - $(G, \ *)$ is an Abelian group

Proof. Associativity.

- $(a * b) * c = (ab/2) * c = (ab)c/4$
- $a * (b * c) = a * (bc/2) = a(bc)/4 = (ab)c/4$
- $*$ is associative

Example

- Let
  - G be the set of all nonzero real numbers, and
  - $a * b = ab/2$
- Show
  - $(G, *)$ is an Abelian group

Proof. 2 is the identity.

- $a * 2 = (a)(2)/2 = a = (2)(a)/2 = 2 * a$

Example

- Let
  - G be the set of all nonzero real numbers, and
  - $a * b = ab/2$
- Show
  - $(G, \ *)$ is an Abelian group

Proof. $a' = 4/a$ is an inverse of a.

- $a * a' = a * 4/a = a(4/a)/2 = 2 = (4/a)(a)/2 = (4/a) * a = a' * a$

Example

- Let
  - G be the set of all nonzero real numbers, and
  - $a * b = ab/2$
- Show
  - $(G, *)$ is an Abelian group

Proof. Abelian.

- $a * b = ab/2 = ba/2 = b * a$

Example

- Let
  - G be the set of all nonzero real numbers, and
  - $a * b = ab/2$
- Show
  - $(G, *)$ is an Abelian group

Proof.

- So, G is an Abelian group.

Theorem (Uniqueness of Inverse)

- *Let G be a group. Each element $a \in G$ has only one inverse in G.*

Proof.

- Let
  - a' and a'' be inverses of a
- Then

$$a' = a'e = a'(aa'') = a'aa'' = (a'a)a'' = ea'' = a''$$

Theorem (Uniqueness of Inverse)

- *Let G be a group. Each element $a \in G$ has only one inverse in G.*

Proof.

- Let
  - a' and a'' be inverses of a
- Then

$$a' = a'e = a'(aa'') = a'aa'' = (a'a)a'' = ea'' = a''$$

Theorem (Uniqueness of Inverse)

- *Let G be a group. Each element $a \in G$ has only one inverse in G.*

Proof.

- Let
  - a' and a'' be inverses of a
- Then

$$a' = a'e = a'(aa'') = a'aa'' = (a'a)a'' = ea'' = a''$$

Theorem (Uniqueness of Inverse)

- *Let G be a group. Each element $a \in G$ has only one inverse in G.*

Proof.

- Let
  - a' and a'' be inverses of a
- Then

$$a' = a'e = a'(aa'') = a'aa'' = (a'a)a'' = ea'' = a''$$

Theorem (Left/Right Cancellation)

- *Let*
  - G *be a group, and* a, b, *and* c *be elements of* G
- *Then*
  - $ab = ac$ *implies* $b = c$
  - $ba = ca$ *implies* $b = c$

Proof: Left Cancellation. Suppose that $ab = ac$.

- $a^{-1}(ab) = a^{-1}(ac)$
- $(a^{-1}a)b = (a^{-1}a)c$, by associativity
- $eb = ec$, by the def. of an inverse
- $b = c$ by definition of an identity

Theorem (Left/Right Cancellation)

- *Let*
  - *G be a group, and a, b, and c be elements of G*
- *Then*
  - *$ab = ac$ implies $b = c$*
  - *$ba = ca$ implies $b = c$*

Proof: Left Cancellation. Suppose that $ab = ac$.

- $a^{-1}(ab) = a^{-1}(ac)$
- $(a^{-1}a)b = (a^{-1}a)c$, by associativity
- $eb = ec$, by the def. of an inverse
- $b = c$ by definition of an identity

Theorem (Left/Right Cancellation)

- *Let*
  - G *be a group, and* a, b*, and* c *be elements of* G
- *Then*
  - $ab = ac$ *implies* $b = c$
  - $ba = ca$ *implies* $b = c$

Proof: Left Cancellation. Suppose that $ab = ac$.

- $a^{-1}(ab) = a^{-1}(ac)$
- $(a^{-1}a)b = (a^{-1}a)c$, by associativity
- $eb = ec$, by the def. of an inverse
- $b = c$ by definition of an identity

Theorem (Left/Right Cancellation)

- *Let*
  - G *be a group, and* a, b*, and* c *be elements of* G
- *Then*
  - $ab = ac$ *implies* $b = c$
  - $ba = ca$ *implies* $b = c$

Proof: Left Cancellation. Suppose that $ab = ac$.

- $a^{-1}(ab) = a^{-1}(ac)$
- $(a^{-1}a)b = (a^{-1}a)c$, by associativity
- $eb = ec$, by the def. of an inverse
- $b = c$ by definition of an identity

Theorem (Left/Right Cancellation)

- *Let*
  - G *be a group, and* $a, b,$ *and* c *be elements of* G
- *Then*
  - $ab = ac$ *implies* $b = c$
  - $ba = ca$ *implies* $b = c$

Proof: Left Cancellation. Suppose that $ab = ac$.

- $a^{-1}(ab) = a^{-1}(ac)$
- $(a^{-1}a)b = (a^{-1}a)c$, by associativity
- $eb = ec$, by the def. of an inverse
- ☞ $b = c$ by definition of an identity

Theorem (Inverse of Inverse)

- *Let*
  - G *be a group, and* a *and* b *be elements of* G
- *Then*
  - $(a^{-1})^{-1} = a$ *and* $(ab)^{-1} = b^{-1}a^{-1}$

Proof.

Theorem (Inverse of Inverse)

- *Let*
  - G *be a group, and* a *and* b *be elements of* G
- *Then*
  - $(a^{-1})^{-1} = a$ *and* $(ab)^{-1} = b^{-1}a^{-1}$

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

- $a^{-1}a = aa^{-1} = e$
- the inverse of an element is unique,
- So, $(a^{-1})^{-1} = a$

Theorem (Inverse of Inverse)

- *Let*
  - G *be a group, and* a *and* b *be elements of* G
- *Then*
  - $(a^{-1})^{-1} = a$ *and* $(ab)^{-1} = b^{-1}a^{-1}$

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

- $(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) = a((bb^{-1})a^{-1}) = a(ea^{-1}) = aa^{-1} = e$
- Similarly, $(b^{-1}a^{-1})(ab) = e$
- So $(ab)^{-1} = b^{-1}a^{-1}$

❀

Theorem (Solution to Equation)

- *Let*
  - G *be a group, and* a *and* b *be elements of* G
- *Then*
  - *The equation* $ax = b$ *has a unique solution in* G
  - *The equation* $ya = b$ *has a unique solution in* G

Proof.

- Omitted

Definition

- If G is a group that has a finite number of elements, G is said to be a finite group, and the order of G is the number of elements $|G|$ in G.

Notice

- A finite group can be represented in the form of the multiplication table.

Definition

- If G is a group that has a finite number of elements, G is said to be a finite group, and the order of G is the number of elements $|G|$ in G.

Notice

- A finite group can be represented in the form of the multiplication table.

Group of Order 1

$(\{e\}, *)$

$*$	e
e	e

Group of Order 2

$(\{e, a\}, *)$

$*$	e	a
e	e	a
a	a	e

Group of Order 3

$(\{e, a, b\}, *)$

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

Group of Order 1

$(\{e\}, *)$

$*$	e
e	e

Group of Order 2

$(\{e, a\}, *)$

$*$	e	a
e	e	a
a	a	e

Group of Order 3

$(\{e, a, b\}, *)$

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

Group of Order 1

$(\{e\}, *)$

$*$	e
e	e

Group of Order 2

$(\{e, a\}, *)$

$*$	e	a
e	e	a
a	a	e

Group of Order 3

$(\{e, a, b\}, *)$

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

Group of Order 1

$(\{e\}, *)$

$*$	e
e	e

Group of Order 2

$(\{e, a\}, *)$

$*$	e	a
e	e	a
a	a	e

Group of Order 3

$(\{e, a, b\}, *)$

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

Group of Order 1

$(\{e\}, *)$

$*$	e
e	e

Group of Order 2

$(\{e, a\}, *)$

$*$	e	a
e	e	a
a	a	e

Group of Order 3

$(\{e, a, b\}, *)$

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

Group of Order 1

$(\{e\}, *)$

$*$	e
e	e

Group of Order 2

$(\{e, a\}, *)$

$*$	e	a
e	e	a
a	a	e

Group of Order 3

$(\{e, a, b\}, *)$

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

Group 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

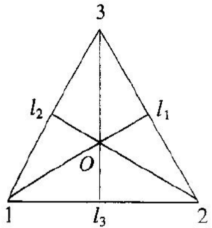
$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

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

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

Problem Description

- Given the equilateral triangle with vertices 1, 2, and 3. Consider it's symmetries.
  - Rotation about the triangle center
  - Reflection about the angle bisector



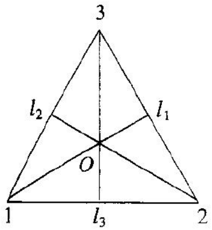
Definition (Symmetries of the Triangle)

- Three counter-clockwise rotations f_1, f_2, f_3 of the triangle about O through 0°, 120°, 240°, respectively.

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

- Three reflections g_1, g_2, g_3 of the triangle about the lines l_1, l_2, l_3, respectively.

$$g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$



Theorem

- $(S_3, *)$ *is a group, where*
  - $S_3 = \{f_1, f_2, f_3, g_1, g_2, g_3\}$
  - *the operation* $*$, *followed by*, *on the set* S_3 *is defined as follows:*

$*$	f_1	f_2	f_3	g_1	g_2	g_3
f_1	f_1	f_2	f_3	g_1	g_2	g_3
f_2	f_2	f_3	f_1	g_3	g_1	g_2
f_3	f_3	f_1	f_2	g_2	g_3	g_1
g_1	g_1	g_2	g_3	f_1	f_2	f_3
g_2	g_2	g_3	g_1	f_3	f_1	f_2
g_3	g_3	g_1	g_2	f_2	f_3	f_1

Compute $f_2 * g_2$ Algebraically

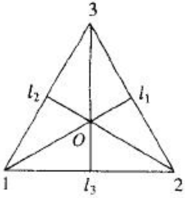
- To compute $f_2 * g_2$ algebraically, we compute $f_2 \circ g_2$

$$f_2 \circ g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = g_1$$

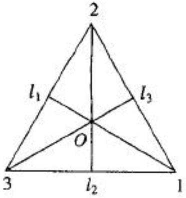
- Therefore
  - $f_2 * g_2 = g_1$

Compute $f_2 * g_2$ Geometrically

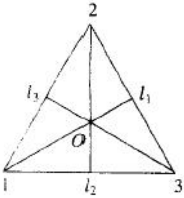
- We can also compute $f_2 * g_2$ geometrically by rotating or flipping the triangle.



Given triangle



Triangle resulting after applying f_2



Triangle resulting after applying g_2 to the triangle at the left

Definition (Permutation Group)

- The set of all permutations of n elements is a group of order $n!$ under the operation of composition.
  - called the symmetric group on n letters, denoted by S_n.
  - permutation group: a group with some permutations of n elements

Theorem (Cayley's Group Theorem)

- *Every Finite Group of order n can be represented as a Permutation Group on n letters.*

Example

♪ A Cyclic Group

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

Definition (Cyclic Group)

♪ Check the Table on the left, we have

- ♫ $a^0 = e$
- ♫ $a^1 = a$
- ♫ $a^2 = b$
- ♫ $a^3 = c$

♪ Such a group is called a cyclic group.

Homework

- 20,28 @page 323-324
- 12,16 @page 348

1. Let G be a group. For $a, b \in G$, we say that b is conjugate to a, written $b \sim a$, if there exists $g \in G$ such that $b = gag^{-1}$. Show that $\sim$ is an equivalence relation on G. The equivalence classes of $\sim$ are called the conjugacy classes of G.
2. Let G be a group, and suppose that a and b are any elements of G. Show that if $(ab)^2 = a^2b^2$, then $ba = ab$.
3. Let $G = \{x \in R | x > 1\}$ be the set of all real numbers greater than 1. For $x, y \in G$, define $x * y = xy - x - y + 2$. Show that $(G, *)$ is a group.