MTH223A LECTURE NOTES CHAPTER 3

Yvette Fajardo-Lim

Mathematics and Statistics Department
De La Salle University - Manila

Outline

Outline

Cyclic Groups

Definition

Let $g \in G$, the elements of $< g >$ are the powers g^n of g for $n \in \mathbb{Z}$. Hence, the elements of $< g >$ are

$$\ldots g^{-5}, g^{-4}, g^{-3}, g^{-2}, g^{-1}, g^{0}, g^{1}, g^{2}, g^{3}, g^{4}, g^{5}, \ldots$$

However, not all of these need be distinct.

Example

Let $G = (\mathbb{Z}_6, +)$. Then $< 2 >= \{2^0, 2^1, 2^2\} = \{0, 2, 4\}$, the power 2^3 is equal to 0, while $2^{-1} = 4$. Also, $< 4 >= \{4^0, 4^1, 4^2\} = \{0, 4, 2\}$. Hence, $< 2 >=< 4 >$.

Cyclic Groups

Definition

Let $g \in G$, the elements of $< g >$ are the powers g^n of g for $n \in \mathbb{Z}$. Hence, the elements of $< g >$ are

$$\ldots g^{-5}, g^{-4}, g^{-3}, g^{-2}, g^{-1}, g^0, g^1, g^2, g^3, g^4, g^5, \ldots$$

However, not all of these need be distinct.

Example

Let $G = (\mathbb{Z}_6, +)$. Then $< 2 >= \{2^0, 2^1, 2^2\} = \{0, 2, 4\}$, the power 2^3 is equal to 0, while $2^{-1} = 4$. Also, $< 4 >= \{4^0, 4^1, 4^2\} = \{0, 4, 2\}$. Hence, $< 2 >=< 4 >$.

Cyclic Groups

Lemma

Suppose $n \in \mathbb{Z}^+$ with $g^n = e$. If $s, t \in \mathbb{Z}$ with $s \equiv t (mod\ n)$, then $g^s = g^t$.

Theorem

Let $g \in G$

1. *If $|g| = n < \infty$, then $< g >= \{e, g, g^2 \ldots, g^{n-1}\}$, and these elements are all distinct.*
2. *If $|g|$ is infinite, then all elements g^r for $r \in \mathbb{Z}$ are distinct.*

Cyclic Groups

Lemma

Suppose $n \in \mathbb{Z}^+$ with $g^n = e$. If $s, t \in \mathbb{Z}$ with $s \equiv t (mod\ n)$, then $g^s = g^t$.

Theorem

Let $g \in G$

1. *If $|g| = n < \infty$, then $< g >= \{e, g, g^2 \ldots, g^{n-1}\}$, and these elements are all distinct.*
2. *If $|g|$ is infinite, then all elements g^r for $r \in \mathbb{Z}$ are distinct.*

Cyclic Groups

Lemma

Suppose $n \in \mathbb{Z}^+$ with $g^n = e$. If $s, t \in \mathbb{Z}$ with $s \equiv t (mod\ n)$, then $g^s = g^t$.

Theorem

Let $g \in G$

1. *If $|g| = n < \infty$, then $< g >= \{e, g, g^2 \ldots, g^{n-1}\}$, and these elements are all distinct.*
2. *If $|g|$ is infinite, then all elements g^r for $r \in \mathbb{Z}$ are distinct.*

Cyclic Groups

Lemma

Suppose $n \in \mathbb{Z}^+$ with $g^n = e$. If $s, t \in \mathbb{Z}$ with $s \equiv t (mod\ n)$, then $g^s = g^t$.

Theorem

Let $g \in G$

1. *If $|g| = n < \infty$, then $< g >= \{e, g, g^2 \ldots, g^{n-1}\}$, and these elements are all distinct.*
2. *If $|g|$ is infinite, then all elements g^r for $r \in \mathbb{Z}$ are distinct.*

Cyclic Groups

Definition

A subgroup of G of the form $< g >$ for some $g \in G$ is called a **cyclic subgroup** *of G. If there is an element $g \in G$ such that $G =< g >$, we say that G is a* **cyclic group**; *any element g with $< g >= G$ is called a* **generator** *of G.*

Example

1. $(\mathbb{Z}_n, +)$ *is cyclic, as it is generated by* $[1]$.
2. $(\mathbb{Z}, +)$ *is cyclic, as it is generated by 1.*
3. $(\mathbb{Q}, +)$ *is not cyclic, as there is no $g \in \mathbb{Q}$ such that $\mathbb{Q}$ consists of the elements ng for $n \in \mathbb{Z}$.*

Cyclic Groups

Definition

A subgroup of G of the form $< g >$ for some $g \in G$ is called a **cyclic subgroup** *of G. If there is an element $g \in G$ such that $G =< g >$, we say that G is a* **cyclic group***; any element g with $< g >= G$ is called a* **generator** *of G.*

Example

1. $(\mathbb{Z}_n, +)$ *is cyclic, as it is generated by* $[1]$.
2. $(\mathbb{Z}, +)$ *is cyclic, as it is generated by 1.*
3. $(\mathbb{Q}, +)$ *is not cyclic, as there is no* $g \in \mathbb{Q}$ *such that* $\mathbb{Q}$ *consists of the elements ng for* $n \in \mathbb{Z}$.

Cyclic Groups

Definition

A subgroup of G of the form $< g >$ for some $g \in G$ is called a **cyclic subgroup** *of G. If there is an element $g \in G$ such that $G =< g >$, we say that G is a* **cyclic group***; any element g with $< g >= G$ is called a* **generator** *of G.*

Example

1. $(\mathbb{Z}_n, +)$ *is cyclic, as it is generated by* $[1]$.
2. $(\mathbb{Z}, +)$ *is cyclic, as it is generated by 1.*
3. $(\mathbb{Q}, +)$ *is not cyclic, as there is no $g \in \mathbb{Q}$ such that $\mathbb{Q}$ consists of the elements ng for $n \in \mathbb{Z}$.*

Cyclic Groups

Definition

A subgroup of G of the form $< g >$ for some $g \in G$ is called a **cyclic subgroup** *of G. If there is an element $g \in G$ such that $G =< g >$, we say that G is a* **cyclic group***; any element g with $< g >= G$ is called a* **generator** *of G.*

Example

1. $(\mathbb{Z}_n, +)$ *is cyclic, as it is generated by* $[1]$.
2. $(\mathbb{Z}, +)$ *is cyclic, as it is generated by 1.*
3. $(\mathbb{Q}, +)$ *is not cyclic, as there is no $g \in \mathbb{Q}$ such that $\mathbb{Q}$ consists of the elements ng for $n \in \mathbb{Z}$.*

Cyclic Groups

Definition

A subgroup of G of the form $< g >$ for some $g \in G$ is called a **cyclic subgroup** *of G. If there is an element $g \in G$ such that $G =< g >$, we say that G is a* **cyclic group**; *any element g with $< g >= G$ is called a* **generator** *of G.*

Example

1. $(\mathbb{Z}_n, +)$ *is cyclic, as it is generated by* $[1]$.
2. $(\mathbb{Z}, +)$ *is cyclic, as it is generated by 1.*
3. $(\mathbb{Q}, +)$ *is not cyclic, as there is no $g \in \mathbb{Q}$ such that $\mathbb{Q}$ consists of the elements ng for $n \in \mathbb{Z}$.*

Cyclic Groups

Remark

A cyclic group is clearly abelian, because for all $r, s \in \mathbb{Z}$ we have

$$g^r \cdot g^s = g^{r+s} = g^{s+r} = g^s \cdot g^r.$$

Theorem

Any subgroup of a cyclic group is cyclic.

Cyclic Groups

Remark

A cyclic group is clearly abelian, because for all $r, s \in \mathbb{Z}$ we have

$$g^r \cdot g^s = g^{r+s} = g^{s+r} = g^s \cdot g^r .$$

Theorem

Any subgroup of a cyclic group is cyclic.

Cyclic Groups

Example

1. *The subgroup* $(4\mathbb{Z}, +)$ *of the cyclic group* $(\mathbb{Z}, +)$ *is cyclic, since it is generated by 4.*
2. *The subgroup* $(\{0, 2, 4\}, +)$, *of the cyclic group* $(\mathbb{Z}_6, +)$ *is cyclic, since it is generated by 2. It is also generated by 4.*

Cyclic Groups

Example

1. *The subgroup* $(4\mathbb{Z}, +)$ *of the cyclic group* $(\mathbb{Z}, +)$ *is cyclic, since it is generated by 4.*
2. *The subgroup* $(\{0, 2, 4\}, +)$*, of the cyclic group* $(\mathbb{Z}_6, +)$ *is cyclic, since it is generated by 2. It is also generated by 4.*

Cyclic Groups

Example

1. *The subgroup* $(4\mathbb{Z}, +)$ *of the cyclic group* $(\mathbb{Z}, +)$ *is cyclic, since it is generated by 4.*
2. *The subgroup* $(\{0, 2, 4\}, +)$*, of the cyclic group* $(\mathbb{Z}_6, +)$ *is cyclic, since it is generated by 2. It is also generated by 4.*

Definition

If $g \in G$, the **order** $o(g)$ *of g is the order of the subgroup $< g >$ generated by g; if $< g >$ is infinite, we say that g has* **infinite order**.

Example

1. *If $G = (\mathbb{Z}_n, +)$ then $o(1) = n$, because $< 1 >= \{0, 1, 2, \ldots, n-1\} = G$.*
2. *If $G = (\mathbb{Z}, +)$ then any non-identity element has infinite order.*
3. *From the group table you filled up, since $< z >= \{y, z, w, x, v\} = G$ then $o(z) = 5 = o(G)$. Likewise, $o(v) = o(w) = o(x) = o(z) = 5$. Hence, G has 4 generators, v, w, x and z.*

Cyclic Groups

Definition

If $g \in G$, the **order** $o(g)$ *of g is the order of the subgroup $< g >$ generated by g; if $< g >$ is infinite, we say that g has* **infinite order**.

Example

1. *If $G = (\mathbb{Z}_n, +)$ then $o(1) = n$, because $< 1 >= \{0, 1, 2, \ldots, n-1\} = G$.*
2. *If $G = (\mathbb{Z}, +)$ then any non-identity element has infinite order.*
3. *From the group table you filled up, since $< z >= \{y, z, w, x, v\} = G$ then $o(z) = 5 = o(G)$. Likewise, $o(v) = o(w) = o(x) = o(z) = 5$. Hence, G has 4 generators, v, w, x and z.*

Cyclic Groups

Definition

If $g \in G$, the **order** $o(g)$ *of g is the order of the subgroup $< g >$ generated by g; if $< g >$ is infinite, we say that g has* **infinite order**.

Example

1. *If $G = (\mathbb{Z}_n, +)$ then $o(1) = n$, because $< 1 >= \{0, 1, 2, \dots, n-1\} = G$.*
2. *If $G = (\mathbb{Z}, +)$ then any non-identity element has infinite order.*
3. *From the group table you filled up, since $< z >= \{y, z, w, x, v\} = G$ then $o(z) = 5 = o(G)$. Likewise, $o(v) = o(w) = o(x) = o(z) = 5$. Hence, G has 4 generators, v, w, x and z.*

Cyclic Groups

Definition

If $g \in G$, the **order** $o(g)$ *of g is the order of the subgroup $< g >$ generated by g; if $< g >$ is infinite, we say that g has* **infinite order**.

Example

1. *If $G = (\mathbb{Z}_n, +)$ then $o(1) = n$, because $< 1 >= \{0, 1, 2, \dots, n-1\} = G$.*
2. *If $G = (\mathbb{Z}, +)$ then any non-identity element has infinite order.*
3. *From the group table you filled up, since $< z >= \{y, z, w, x, v\} = G$ then $o(z) = 5 = o(G)$. Likewise, $o(v) = o(w) = o(x) = o(z) = 5$. Hence, G has 4 generators, v, w, x and z.*

Cyclic Groups

Definition

If $g \in G$, the **order** $o(g)$ *of g is the order of the subgroup $< g >$ generated by g; if $< g >$ is infinite, we say that g has* **infinite order**.

Example

1. *If $G = (\mathbb{Z}_n, +)$ then $o(1) = n$, because $< 1 >= \{0, 1, 2, \ldots, n-1\} = G$.*
2. *If $G = (\mathbb{Z}, +)$ then any non-identity element has infinite order.*
3. *From the group table you filled up, since $< z >= \{y, z, w, x, v\} = G$ then $o(z) = 5 = o(G)$. Likewise, $o(v) = o(w) = o(x) = o(z) = 5$. Hence, G has 4 generators, v, w, x and z.*

Cyclic Groups

Example

Given the group table below,

$*$	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

the order of the elements are as follows:

g	a	b	c	d	e	f
$o(g)$	1	2	2	3	2	3

Cyclic Groups

Remark

There are various things we may observe about element orders. First, as defined earlier, $o(g)$ is the least natural number n such that $g^n = e$ or is ∞ if there is no such n. Clearly $o(g) = 1$ if and only if $g = e$, while if $e \neq e$ then $o(g) = 2$ if and only if $g^2 = e$ which implies that $g^{-1} = g$. Also, $o(g^{-1}) = o(g)$, because any power of g^{-1} is a power of g and vice versa, so that $< g^{-1} >=< g >$. Finally, a finite group of order n is cyclic if and only if it has an element g with $o(g) = n$.

MTH223A

Yvette Fajardo-Lim

Some Special Classes of Groups

Cyclic Groups

Groups of Permutations

The Sign of a Permutation

Dihedral Groups

Example

1. *In* $(\mathbb{Z}_6, +)$ *, 3 is its own inverse, and has order 2.*
2. *In* $(\mathbb{Z}_5, +)$ *the inverse of 1 is 4, with successive powers* $4, 3, 2, 1, 0$, *so* $o(4) = 5 = 0(1)$
3. *The group table below is not cyclic, since it has no element of order 6.*

$*$	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

Cyclic Groups

Example

1. *In $(\mathbb{Z}_6, +)$, 3 is its own inverse, and has order 2.*
2. *In $(\mathbb{Z}_5, +)$ the inverse of 1 is 4, with successive powers $4, 3, 2, 1, 0$, so $o(4) = 5 = 0(1)$*
3. *The group table below is not cyclic, since it has no element of order 6.*

$*$	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

Example

1. *In* $(\mathbb{Z}_6, +)$ *, 3 is its own inverse, and has order 2.*
2. *In* $(\mathbb{Z}_5, +)$ *the inverse of 1 is 4, with successive powers* $4, 3, 2, 1, 0$, *so* $o(4) = 5 = 0(1)$
3. *The group table below is not cyclic, since it has no element of order 6.*

$*$	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

Cyclic Groups

Example

1. *In* $(\mathbb{Z}_6, +)$ *, 3 is its own inverse, and has order 2.*
2. *In* $(\mathbb{Z}_5, +)$ *the inverse of 1 is 4, with successive powers* $4, 3, 2, 1, 0$, *so* $o(4) = 5 = 0(1)$
3. *The group table below is not cyclic, since it has no element of order 6.*

$*$	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

Cyclic Groups

Theorem

Take $g \in G$ with $o(g) = n$; then $g^s = g^t$ if and only if $s \equiv t (mod\ n)$.

Corollary

If $g \in G$, then $g^s = e$ if and only if $o(g) | s$.

Cyclic Groups

Theorem

Take $g \in G$ with $o(g) = n$; then $g^s = g^t$ if and only if $s \equiv t (mod\ n)$.

Corollary

If $g \in G$, then $g^s = e$ if and only if $o(g)|s$.

Outline

Let X be a finite set. Recall that a **permutation** of X is a bijective map from X to itself. Because the nature of the permutations of X depends only on the number of elements of X, rather than the particular elements themselves, we may as well assume that $X = \{1, 2, \ldots n\}$.

Definition

The group of permutations of the set $\{1, 2, \ldots n\}$ is called the **symmetric group of degree n**, *and is written S_n.*

Let X be a finite set. Recall that a **permutation** of X is a bijective map from X to itself. Because the nature of the permutations of X depends only on the number of elements of X, rather than the particular elements themselves, we may as well assume that $X = \{1, 2, \ldots n\}$.

Definition

The group of permutations of the set $\{1, 2, \ldots n\}$ is called the **symmetric group of degree n**, *and is written S_n.*

An element $\sigma \in S_n$ may be written as
$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$, where $a_i = \sigma(i)$ for $0 \leq i \leq n$.
Since there are n choices for a_1, then $n - 1$ choices for a_2 (as it must be different from a_1), then $n - 2$ choices for a_3 and so on, we see that there are $n!$ different permutations of $\{1, 2, \dots n\}$; thus S_n has $n!$ elements. There are also $n!$ different ways of writing a given permutation, since we may rearrange the columns in any order.

In S_3 we have

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \dots$$

The composite of two permutations is defined by

$$\begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$$

The identity permutation is $\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$, and the inverse of $\begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$ is $\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 1 & 2 & \dots & n \end{pmatrix}$.

It is clear that S_1, the trivial group and S_2 are abelian; however, if $n \geq 3$ then S_n is non-abelian.

Groups of Permutations

Definition

For any positive integer $r \leq n$, let $a_1, a_2, \ldots, a_r$ be distinct elements of the set $\{1, 2, \ldots n\}$. We denote by $(a_1\ a_2\ \ldots\ a_r)$ the permutation given by

$$\sigma(a_i) = a_{i+1} \text{ for } 1 \leq i \leq r-1, \quad \sigma(a_r) = a_1, \quad \sigma(a) = a \text{ for } a \notin$$

We call $(a_1\ a_2\ \ldots\ a_r)$ a **cycle of length r**, *or an* **r-cycle**.

Example

Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \ldots & n \\ 2 & 1 & 3 & 4 \ldots & n \end{pmatrix}, \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \ldots & n \\ 1 & 3 & 2 & 4 \ldots & n \end{pmatrix}$$

so that σ simply interchanges 1 and 2, and π interchanges 2 and 3, we have $\sigma = (1\ 2), \pi = (2\ 3), \sigma\pi = (1\ 3\ 2)$ and $\pi\sigma = (1\ 2\ 3)$; σ and $= \pi$ are 2-cycles, and $\sigma\pi$ and $\pi\sigma$ are 3-cycles.

Remark

There are several things to note about cycles.

1. *An r-cycle can be written in r different ways, since* $(a_1\ a_2\ \ldots\ a_r) = (a_2\ \ldots a_r\ a_1) = \ldots = (a_r\ a_1\ \ldots\ a_{r-1})$
2. *Any 1-cycle is simply the identity permutation.*
3. *We can multiply two cycles by 'feeding in' elements from the left in turn; for example, if* $\sigma = (1\ 2\ 5)$ *and* $\pi = (2\ 3\ 4)$ *then* $\sigma\pi = (1\ 2\ 5)(2\ 3\ 1)$ *maps* $1 \to 2 \to 3, 3 \to 3 \to 4, 4 \to 4 \to 2, 2 \to 5 \to 5, 5 \to 1 \to 1$ *and so* $\sigma\pi = (1\ 3\ 4\ 2\ 5)$.
4. *The inverse of a cycle is obtained by simply writing its elements in reverse order; for example if* π *is as above then* $\pi^{-1} = (4\ 3\ 2)$. *We can check this by computing* $(2\ 3\ 4)(4\ 3\ 2) = 1$.

Remark

There are several things to note about cycles.

1. *An r-cycle can be written in r different ways, since* $(a_1\ a_2\ \ldots\ a_r) = (a_2\ \ldots a_r\ a_1) = \ldots = (a_r\ a_1\ \ldots\ a_{r-1})$
2. *Any 1-cycle is simply the identity permutation.*
3. *We can multiply two cycles by 'feeding in' elements from the left in turn; for example, if* $\sigma = (1\ 2\ 5)$ *and* $\pi = (2\ 3\ 4)$ *then* $\sigma\pi = (1\ 2\ 5)(2\ 3\ 1)$ *maps* $1 \to 2 \to 3, 3 \to 3 \to 4, 4 \to 4 \to 2, 2 \to 5 \to 5, 5 \to 1 \to 1$ *and so* $\sigma\pi = (1\ 3\ 4\ 2\ 5)$.
4. *The inverse of a cycle is obtained by simply writing its elements in reverse order; for example if* π *is as above then* $\pi^{-1} = (4\ 3\ 2)$. *We can check this by computing* $(2\ 3\ 4)(4\ 3\ 2) = 1$.

Groups of Permutations

Remark

There are several things to note about cycles.

1. *An r-cycle can be written in r different ways, since* $(a_1\ a_2\ \ldots\ a_r) = (a_2\ \ldots a_r\ a_1) = \ldots = (a_r\ a_1\ \ldots\ a_{r-1})$
2. *Any 1-cycle is simply the identity permutation.*
3. *We can multiply two cycles by 'feeding in' elements from the left in turn; for example, if* $\sigma = (1\ 2\ 5)$ *and* $\pi = (2\ 3\ 4)$ *then* $\sigma\pi = (1\ 2\ 5)(2\ 3\ 1)$ *maps* $1 \to 2 \to 3, 3 \to 3 \to 4, 4 \to 4 \to 2, 2 \to 5 \to 5, 5 \to 1 \to 1$ *and so* $\sigma\pi = (1\ 3\ 4\ 2\ 5)$.
4. *The inverse of a cycle is obtained by simply writing its elements in reverse order; for example if* π *is as above then* $\pi^{-1} = (4\ 3\ 2)$. *We can check this by computing* $(2\ 3\ 4)(4\ 3\ 2) = 1$.

Remark

There are several things to note about cycles.

1. *An r-cycle can be written in r different ways, since* $(a_1\ a_2\ \dots\ a_r) = (a_2\ \dots a_r\ a_1) = \dots = (a_r\ a_1\ \dots\ a_{r-1})$
2. *Any 1-cycle is simply the identity permutation.*
3. *We can multiply two cycles by 'feeding in' elements from the left in turn; for example, if* $\sigma = (1\ 2\ 5)$ *and* $\pi = (2\ 3\ 4)$ *then* $\sigma\pi = (1\ 2\ 5)(2\ 3\ 1)$ *maps* $1 \to 2 \to 3, 3 \to 3 \to 4, 4 \to 4 \to 2, 2 \to 5 \to 5, 5 \to 1 \to 1$ *and so* $\sigma\pi = (1\ 3\ 4\ 2\ 5)$.
4. *The inverse of a cycle is obtained by simply writing its elements in reverse order; for example if* π *is as above then* $\pi^{-1} = (4\ 3\ 2)$. *We can check this by computing* $(2\ 3\ 4)(4\ 3\ 2) = 1$.

Remark

The order of a cycle is simply given by its length, because applying $(a_1\ a_2\ \ldots\ a_r)$ *successively maps*

$$a_1 \to a_2 \to \ldots \to a_r \to a_1,$$

for example,$(2\ 3\ 4)$ *has order 3.*

Groups of Permutations

Remark

If $\sigma = (a_1 \; a_2 \; \ldots \; a_r)$ and $\pi = (b_1 \; b_2 \; \ldots \; b_r)$, where the sets $\{a_1, a_2, \ldots, a_r\}$ and $\{b_1, b_2, \ldots, b_r\}$ are disjoint, i.e., have empty intersection, then $\sigma\pi = \pi\sigma$; for example, if $\sigma = (4\;5\;6\;7)$ and $\pi = (1\;2\;3)$ in S_8, then

$$\sigma\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 & 8 \end{pmatrix}$$

We can see this because the elements moved by σ and π are different, so it does not matter whether σ or π is performed first.

Groups of Permutations

Remark

Not all permutations are cycles; for example, the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 & 8 \end{pmatrix}$$

from the previous slide is not a cycle. However, we obtained this permutation as a product of two cycles.

Definition

Let $\sigma = (a_1 \ a_2 \ \dots \ a_r)$ and $\pi = (b_1 \ b_2 \ \dots \ b_r)$ be cycles of S_n. If the sets $\{a_1, a_2, \dots, a_r\}$ and $\{b_1, b_2, \dots, b_r\}$ are disjoint, we say that σ and π are **disjoint cycles**. *This terminology is extended in the obvious way to sets of more than two cycles.*

Example

For the permutation $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 & 8 \end{pmatrix}$ *above, it is easy to recover the cycles* $(4\ 5\ 6\ 7)$ *and* $(1\ 2\ 3)$ *of which it is a product.*

Definition

Let $\sigma = (a_1\ a_2\ \ldots\ a_r)$ and $\pi = (b_1\ b_2\ \ldots\ b_r)$ be cycles of S_n. If the sets $\{a_1, a_2, \ldots, a_r\}$ and $\{b_1, b_2, \ldots, b_r\}$ are disjoint, we say that σ and π are **disjoint cycles***. This terminology is extended in the obvious way to sets of more than two cycles.*

Example

For the permutation $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 & 8 \end{pmatrix}$ *above, it is easy to recover the cycles* $(4\ 5\ 6\ 7)$ *and* $(1\ 2\ 3)$ *of which it is a product.*

Theorem

Every permutation in S_n can be written as a product of disjoint cycles; moreover this expression is unique up to

1. *the order in which the cycles occur,*
2. *the different ways of writing each cycle, and*
3. *the presence or absence of 1-cycles.*

Groups of Permutations

Theorem

Every permutation in S_n can be written as a product of disjoint cycles; moreover this expression is unique up to

1. *the order in which the cycles occur,*
2. *the different ways of writing each cycle, and*
3. *the presence or absence of 1-cycles.*

Groups of Permutations

Theorem

Every permutation in S_n can be written as a product of disjoint cycles; moreover this expression is unique up to

1. *the order in which the cycles occur,*
2. *the different ways of writing each cycle, and*
3. *the presence or absence of 1-cycles.*

Groups of Permutations

Theorem

Every permutation in S_n can be written as a product of disjoint cycles; moreover this expression is unique up to

1. *the order in which the cycles occur,*
2. *the different ways of writing each cycle, and*
3. *the presence or absence of 1-cycles.*

Definition

A permutation which is written as a product of disjoint cycles is said to be in **cycle notation***; if all 1-cycles are included, it is said to be in* **full cycle notation**.

Example

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 6 & 9 & 7 & 2 & 3 & 8 & 4 \end{pmatrix}$ *and* $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 8 & 6 & 1 & 7 & 4 & 9 & 2 & 5 \end{pmatrix}$*; then the expressions for* $\sigma, \pi, \sigma\pi$ *and* σ^{-1} *in (full) cycle notation are as follows:*

$\sigma = (2\ 5\ 7\ 3\ 6)(4\ 9) = (2\ 5\ 7\ 3\ 6)(4\ 9)(1)(8)$

$\pi = (1\ 3\ 6\ 4)(2\ 8)(5\ 7\ 9)$

$\sigma\pi = (2\ 5\ 7\ 3\ 6)(4\ 9)(1\ 3\ 6\ 4)(2\ 8)(5\ 7\ 9)$

$\quad = (1\ 3\ 4\ 5\ 9)(2\ 7\ 6\ 8)$

$\sigma^{-1} = (6\ 3\ 7\ 5\ 2)(9\ 4) = (3\ 7\ 5\ 2\ 6)(4\ 9)$

Theorem

If $\sigma = \alpha_1\alpha_2 \ldots \alpha_k$, where the α_i are disjoint cycles, then the order of σ is the least common multiple of the lengths of the cycles α_i.

Example

If $\pi = (1\ 3\ 6\ 4)(2\ 8)(5\ 7\ 9)$, then the order of π is the least common multiple of 4,3 and 2 which is 12.

Groups of Permutations

Theorem

If $\sigma = \alpha_1\alpha_2\ldots\alpha_k$, where the α_i are disjoint cycles, then the order of σ is the least common multiple of the lengths of the cycles α_i.

Example

If $\pi = (1\ 3\ 6\ 4)(2\ 8)(5\ 7\ 9)$, then the order of π is the least common multiple of 4,3 and 2 which is 12.

Groups of Permutations

Definition

A 2-cycle is called a **transposition**.

Theorem

If $n > 1$, every permutation in S_n can be written as a product of transpositions.

Example

In S_8 we have

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 2 & 8 & 3 & 6 & 1 & 7 \end{pmatrix} = (1\ 4)(1\ 8)(1\ 7)(2\ 5)(2\ 3).$$

In general there will be many ways of expressing a given permutation as a product of transpositions.

Groups of Permutations

Definition

A 2-cycle is called a **transposition**.

Theorem

If $n > 1$, every permutation in S_n can be written as a product of transpositions.

Example

In S_8 we have

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 2 & 8 & 3 & 6 & 1 & 7 \end{pmatrix} = (1\ 4)(1\ 8)(1\ 7)(2\ 5)(2\ 3).$$

In general there will be many ways of expressing a given permutation as a product of transpositions.

Groups of Permutations

Definition

A 2-cycle is called a **transposition**.

Theorem

If $n > 1$, every permutation in S_n can be written as a product of transpositions.

Example

In S_8 we have

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 2 & 8 & 3 & 6 & 1 & 7 \end{pmatrix} = (1\ 4)(1\ 8)(1\ 7)(2\ 5)(2\ 3).$$

In general there will be many ways of expressing a given permutation as a product of transpositions.

Groups of Permutations

Definition

A 2-cycle is called a **transposition**.

Theorem

If $n > 1$, every permutation in S_n can be written as a product of transpositions.

Example

In S_8 we have

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 2 & 8 & 3 & 6 & 1 & 7 \end{pmatrix} = (1\ 4)(1\ 8)(1\ 7)(2\ 5)(2\ 3).$$

In general there will be many ways of expressing a given permutation as a product of transpositions.

Outline

The Sign of a Permutation

Let $\sigma \in S_n$, and suppose that $\sigma = \alpha_1\alpha_2 \ldots \alpha_k$ with the α_i disjoint cycles. Set

$$v(\sigma) = \sum_1^k (|\alpha_i| - 1)$$

where $|\alpha_i|$ denotes the length of the cycle α_i . Note that $v(\sigma)$ is well-defined because of the uniqueness in theorem 3.4, in particular, cycles of length 1 contribute 0 to the sum, and so may be ignored.

Example

If $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 2 & 8 & 3 & 6 & 1 & 7 \end{pmatrix} =$ $(1\ 4)(1\ 8)(1\ 7)(2\ 5)(2\ 3) = (1\ 4\ 8\ 7)(2\ 5\ 3)(6)$, *then* $v(\sigma) = 3 + 2 + 0 = 5$.

The Sign of a Permutation

Let $\sigma \in S_n$, and suppose that $\sigma = \alpha_1 \alpha_2 \dots \alpha_k$ with the α_i disjoint cycles. Set

$$v(\sigma) = \sum_1^k (|\alpha_i| - 1)$$

where $|\alpha_i|$ denotes the length of the cycle α_i . Note that $v(\sigma)$ is well-defined because of the uniqueness in theorem 3.4, in particular, cycles of length 1 contribute 0 to the sum, and so may be ignored.

Example

If $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 2 & 8 & 3 & 6 & 1 & 7 \end{pmatrix} =$ $(1\ 4)(1\ 8)(1\ 7)(2\ 5)(2\ 3) = (1\ 4\ 8\ 7)(2\ 5\ 3)(6)$, *then* $v(\sigma) = 3 + 2 + 0 = 5.$

The Sign of a Permutation

Note that because σ^{-1} has the same cycle lengths as σ, we have $v(\sigma^{-1}) = v(\sigma)$.

Example

If $\sigma = (1\ 4\ 8\ 7)(2\ 5\ 3)(6)$, *then* $\sigma^{-1} = (7\ 8\ 4\ 1)(3\ 5\ 2)(6)$, *so* $v(\sigma^{-1}) = 3 + 2 + 0 = 5$.

The Sign of a Permutation

Note that because σ^{-1} has the same cycle lengths as σ, we have $v(\sigma^{-1}) = v(\sigma)$.

Example

If $\sigma = (1\ 4\ 8\ 7)(2\ 5\ 3)(6)$, *then* $\sigma^{-1} = (7\ 8\ 4\ 1)(3\ 5\ 2)(6)$, *so* $v(\sigma^{-1}) = 3 + 2 + 0 = 5$ *.*

$v(\sigma) = 1$ if and only if σ is a transposition. In fact we may interpret $v(\sigma)$ as follows: if all possible 1-cycles are included in the expression $\sigma = \alpha_1\alpha_2\ldots\alpha_k$, then $\sum_1^k(|\alpha_i| - 1)$ is the number of entries in the domain minus the number of cycles; thus $v(\sigma) = n - k$, i.e., $v(\sigma)$ is the difference between n and the number of cycles in the full cycle notation.

Example

If $\sigma = (1\ 4\ 8\ 7)(2\ 5\ 3)(6)$, then $n = 8$ and $k = 3$, so $v(\sigma^{-1}) = 8 - 3 = 5$.

The Sign of a Permutation

$v(\sigma) = 1$ if and only if σ is a transposition. In fact we may interpret $v(\sigma)$ as follows: if all possible 1-cycles are included in the expression $\sigma = \alpha_1\alpha_2 \ldots \alpha_k$, then $\sum_1^k(|\alpha_i| - 1)$ is the number of entries in the domain minus the number of cycles; thus $v(\sigma) = n - k$, i.e., $v(\sigma)$ is the difference between n and the number of cycles in the full cycle notation.

Example

If $\sigma = (1\ 4\ 8\ 7)(2\ 5\ 3)(6)$, *then* $n = 8$ *and* $k = 3$, *so* $v(\sigma^{-1}) = 8 - 3 = 5$.

The Sign of a Permutation

Definition

Given $\sigma \in S_n$, the **sign** *of σ is defined by*

$$sign(\sigma) = (-1)^{v(\sigma)}$$

Thus $sign(\sigma) = \pm 1$; if $sign(\sigma) = 1$ we call σ an **even permutation***, while if $sign(\sigma) = -1$ we call σ) an* **odd permutation***.*

Example

If $\sigma = (1\ 4\ 8\ 7)(2\ 5\ 3)(6)$, we have $sign(\sigma) = (-1)^5 = -1$, and so σ is odd. Note that because $v(\sigma^{-1}) = v(\sigma)$, we have $sign(\sigma^{-1}) = sign(\sigma)$.

The Sign of a Permutation

Definition

Given $\sigma \in S_n$, the **sign** *of σ is defined by*

$$sign(\sigma) = (-1)^{v(\sigma)}$$

Thus $sign(\sigma) = \pm 1$; if $sign(\sigma) = 1$ we call σ an **even permutation***, while if $sign(\sigma) = -1$ we call σ) an* **odd permutation***.*

Example

If $\sigma = (1\ 4\ 8\ 7)(2\ 5\ 3)(6)$, we have $sign(\sigma) = (-1)^5 = -1$, and so σ is odd. Note that because $v(\sigma^{-1}) = v(\sigma)$, we have $sign(\sigma^{-1}) = sign(\sigma)$.

The Sign of a Permutation

Lemma

Let $\sigma \in S_n$, and take τ a transposition; then $sign(\tau\sigma) = -sign(\sigma)$.

Example

Let $\sigma = (1\ 4\ 7\ 8)(2\ 5\ 3)$ as above, so that $sign(\sigma) = -1$. If $\tau = (4\ 5)$ then $\tau\sigma = (4\ 5)(1\ 4\ 7\ 8)(2\ 5\ 3) = (1\ 4\ 3\ 2\ 5\ 7\ 8)$

$v(\tau\sigma) = 6$; $sign(\tau\sigma) = (-1)^6 = 1 = -sign(\sigma)$.

On the other hand, if $\tau = (4\ 8)$ then

$\tau\sigma = (4\ 8)(1\ 4\ 7\ 8)(2\ 5\ 3) = (1\ 4\ 7)(2\ 5\ 3)$

$v(\tau\sigma) = 4$; $sign(\tau\sigma) = (-1)^4 = 1 = -sign(\sigma)$.

The Sign of a Permutation

Lemma

Let $\sigma \in S_n$, and take τ a transposition; then $sign(\tau\sigma) = -sign(\sigma)$.

Example

Let $\sigma = (1\ 4\ 7\ 8)(2\ 5\ 3)$ *as above, so that* $sign(\sigma) = -1$. *If* $\tau = (4\ 5)$ *then* $\tau\sigma = (4\ 5)(1\ 4\ 7\ 8)(2\ 5\ 3) = (1\ 4\ 3\ 2\ 5\ 7\ 8)$
$v(\tau\sigma) = 6; sign(\tau\sigma) = (-1)^6 = 1 = -sign(\sigma)$.
On the other hand, if $\tau = (4\ 8)$ *then*
$\tau\sigma = (4\ 8)(1\ 4\ 7\ 8)(2\ 5\ 3) = (1\ 4\ 7)(2\ 5\ 3)$
$v(\tau\sigma) = 4; sign(\tau\sigma) = (-1)^4 = 1 = -sign(\sigma)$.

The Sign of a Permutation

Corollary

If $\tau_1, \ldots \tau_r \in S_n$ are transpositions, then $sign(\tau_1 \ \ldots \ \tau_r) = (-1)^r$.

Theorem

Let $\sigma, \pi \in S_n$, then $sign(\sigma)sign(\pi) = sign(\sigma\pi)$.

The Sign of a Permutation

Corollary

If $\tau_1, \ldots \tau_r \in S_n$ *are transpositions, then* $sign(\tau_1 \ \ldots \ \tau_r) = (-1)^r$.

Theorem

Let $\sigma, \pi \in S_n$ *, then* $sign(\sigma)sign(\pi) = sign(\sigma\pi)$.

The Sign of a Permutation

Example

In S_8, *let* $\sigma = (1\ 4\ 8)(2\ 3\ 7)(5\ 6)$ *and* $\pi = (1\ 6)(3\ 7\ 8)(4\ 5)$; *then* $\sigma\pi = (1\ 4\ 8)(2\ 3\ 7)(5\ 6)(1\ 6)(3\ 7\ 8)(4\ 5) = (1\ 5)(2\ 7)(3\ 8\ 6\ 4)$ *Here*

$$\begin{aligned} v(\sigma) &= 2+2+1=5 \text{ so } sign(\sigma) = -1 \\ v(\pi) &= 1+2+1=4 \text{ so } sign(\pi) = 1 \\ v(\sigma\pi) &= 1+1+3=5 \text{ so } sign(\sigma\pi) = -1 \end{aligned}$$

Theorem

The subgroup of S_n *consisting of all the even permutations is called the* **alternating group of degree** n, *and is written* A_n. *The order of* A_n *is* $\frac{n!}{2}$.

The Sign of a Permutation

Example

In S_8, let $\sigma = (1\ 4\ 8)(2\ 3\ 7)(5\ 6)$ and $\pi = (1\ 6)(3\ 7\ 8)(4\ 5)$; then $\sigma\pi = (1\ 4\ 8)(2\ 3\ 7)(5\ 6)(1\ 6)(3\ 7\ 8)(4\ 5) = (1\ 5)(2\ 7)(3\ 8\ 6\ 4)$ Here

$$\begin{aligned} v(\sigma) &= 2+2+1=5 \text{ so } sign(\sigma) = -1 \\ v(\pi) &= 1+2+1=4 \text{ so } sign(\pi) = 1 \\ v(\sigma\pi) &= 1+1+3=5 \text{ so } sign(\sigma\pi) = -1 \end{aligned}$$

Theorem

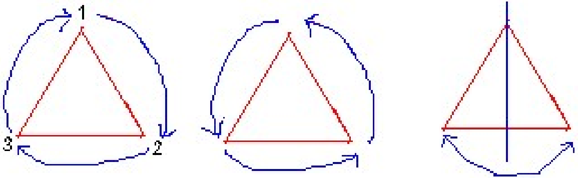
The subgroup of S_n consisting of all the even permutations is called the **alternating group of degree** n*, and is written A_n. The order of A_n is $\frac{n!}{2}$.*

Outline

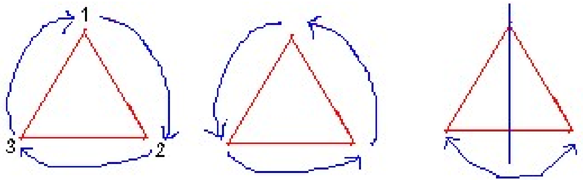
Dihedral Groups

The **Dihedral groups** are the groups, D_n, of the possible symmetry operations on n-sided Regular Polygons.

The smallest n-sided regular polygon is the triangle, so we will start with D_3. A symmetry operation on a geometrical object is rotations and reflection that leaves the object in the same shape. This will, for a triangle, mean a rotation to the left or right by a third of a turn, or no rotation at all, or a reflection through any of its 'heights'. If we name the corners 1,2 and 3 we can see that this is the same as permutations of these corners.



Dihedral Groups



The first of the two rotations will move 1 to 2, 2 to 3 and 3 to 1, which is the cyclic permutation (1 2 3), the other rotation will be the cyclic rotation (1 3 2). The three reflections will exchange two corners and will be the same as the three possible cyclic permutation of three objects that exchange two objects, (1 2),(2 3) , and (1 3). Then we have left the 'do nothing' operation (1).

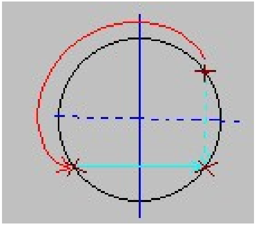
Dihedral Groups

The symmetry group n-sided regular polygon will have one identity element, 'do nothing', $n-1$ rotational elements with rotations of 1 to $n-1$ of a $\frac{1}{n}$-turn. For polygons with an odd number of corners, there will be n reflections, one through each corner to the midpoint of the opposite edge. For polygons with an even number of sides, there will be $\frac{n}{2}$ reflections, with the axis through each opposite pair of corners, and $\frac{n}{2}$ through the midpoints of opposite edges, n in total. This means that the number of elements in the symmetry group for a n-sided regular polygon will be $1+n-1+n=2n$, and this will be the order of this group. Hence, the order of the Dihedral group D_n is $2n$.

Dihedral Groups

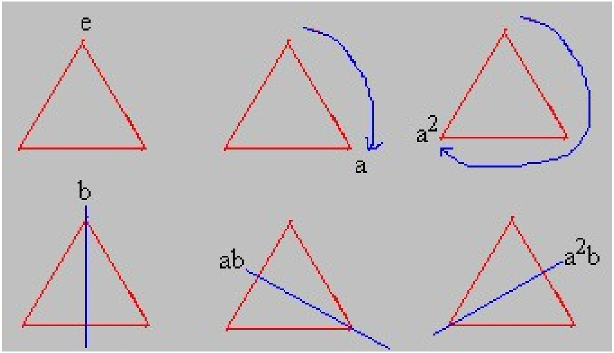
D_n is a dihedral group. By the theorem on the properties of functions, the composition of functions is associative. The inverse of a rotation will simply be a new rotation that together with the first one make a full turn. If the first one was by $\frac{p}{n}$ turn, then the new one need to be $\frac{n-p}{n}$ turn, together making $\frac{p}{n} + \frac{n-p}{n} = 1$ turn. The inverse of a reflection will simply be the reflection itself. The identity element will be the 'do nothing' operator.

Dihedral Groups



All elements of a dihedral group can be described as $a^p b^r$, where p describes the angle, 0 to $n-1$, and r is a binary value, 0 or 1 (for no reflection or a reflection).

The elements of D3 are



The Cayley table for group D_3:

$*$	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

Dihedral Groups

e = rotation through 0° about the centroid =
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1)$$

a = rotation through 120° about the centroid =
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3)$$

a^2 = rotation through 240° about the centroid =
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2)$$

Dihedral Groups

e = rotation through 0° about the centroid =

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1)$$

a = rotation through 120° about the centroid =

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3)$$

a^2 = rotation through 240° about the centroid =

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2)$$

Dihedral Groups

e = rotation through 0° about the centroid =
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1)$$
a = rotation through 120° about the centroid =
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3)$$
a^2 = rotation through 240° about the centroid =
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2)$$

Dihedral Groups

b = reflection about the altitude through vertex 1 = $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3)$

ab = reflection about the altitude through vertex 2 = $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3)$

a^2b = reflection about the altitude through vertex 3 = $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2)$

The order of a is n and the order of b is 2.

MTH223A

Yvette Fajardo-Lim

Some Special Classes of Groups

Cyclic Groups

Groups of Permutations

The Sign of a Permutation

Dihedral Groups

b = reflection about the altitude through vertex 1 =
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3)$$

ab = reflection about the altitude through vertex 2 =
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3)$$

a^2b = reflection about the altitude through vertex 3 =
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2)$$

The order of a is n and the order of b is 2.

Dihedral Groups

b = reflection about the altitude through vertex 1 =
$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3)$

ab = reflection about the altitude through vertex 2 =
$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3)$

a^2b = reflection about the altitude through vertex 3 =
$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2)$

The order of a is n and the order of b is 2.

Dihedral Groups

b = reflection about the altitude through vertex 1 = $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3)$

ab = reflection about the altitude through vertex 2 = $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3)$

a^2b = reflection about the altitude through vertex 3 = $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2)$

The order of a is n and the order of b is 2.

Dihedral Groups

The subgroups of D_3 are as follows:

1. $G = \{e, a, a^2, b, ab, a^2b\}$
2. $H_1 = \{e, a, a^2\}$
3. $H_2 = \{e, a^2b\}$
4. $H_3 = \{e, ab\}$
5. $H_4 = \{e, b\}$
6. $H_5 = \{e\}$

Hence, we have

$$
\begin{aligned}
H_5 <\ & H_1 < G \\
H_5 <\ & H_2 < G \\
H_5 <\ & H_3 < G \\
H_5 <\ & H_4 < G
\end{aligned}
$$

Dihedral Groups

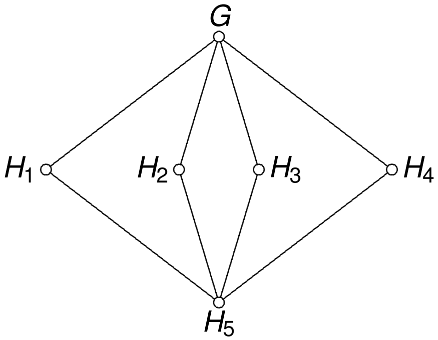
The subgroups of D_3 are as follows:

1. $G = \{e, a, a^2, b, ab, a^2b\}$
2. $H_1 = \{e, a, a^2\}$
3. $H_2 = \{e, a^2b\}$
4. $H_3 = \{e, ab\}$
5. $H_4 = \{e, b\}$
6. $H_5 = \{e\}$

Hence, we have

$$\begin{aligned} H_5 < \quad & H_1 \quad < G \\ H_5 < \quad & H_2 \quad < G \\ H_5 < \quad & H_3 \quad < G \\ H_5 < \quad & H_4 \quad < G \end{aligned}$$

The subgroup lattice for D_3 will be



Dihedral Groups

What are the elements of D_n?

Note that $ba = a^2b = a^{-1}b$. This can be used to perform any operation. For example, $aba = a(ba) = a(a^{-1}b) = aa^{-1}b = eb = b$.

For dihedral groups, we have $a^pa^q = a^{(p+q)(mod\ n)}$.
Hence,
$a^pba^q = a^p(ba)a^{q-1} = a^p(a^{-1}b)a^{q-1} = a^{p-1}ba^{q-1} = a^{p-1-1}ba^{q-2} = \ldots = a^{(p-q)(mod\ n)}b$,
and,
$a^pba^qb = a^{(p-q)(mod\ n)}bb = a^{(p-q)(mod\ n)}e = a^{(p-q)(mod\ n)}$.

Dihedral Groups

In general all elements of the dihedral groups will be of this form. Hence, the group table for D_4 can be obtained as below.

$*$	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	ab^2
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

Dihedral Groups

Definition

Let n be a positive integer, $n \geq 3$, D_n is called the **dihedral group of order** $2n$ *under composition of symmetries.*

$$D_n = \{a^r b^s | r = 0, 1, \ldots, n-1, s = 0, 1\}$$

where

$$\begin{aligned} a^p a^q &= a^{(p+q)(mod\ n)} \\ a^p b a^q &= a^{(p-q)(mod\ n)} b \\ a^p b a^q b &= a^{(p-q)(mod\ n)}. \end{aligned}$$