Group theory
(and some applications in Computer Science)

Mai Hoàng Biên

Faculty of Mathematics and Computer Science, University of Science, VNUHCM

Chapter 3. Subgroups of Groups

1. 3.1. Dihedral groups (in computer visions)
2. 3.2. Braid group Cryptography
3. 3.3. Linear groups (in Neural Networks)
4. 3.4. Groups of points (of Elliptic Curve Cryptography)

3.1. Dihedral groups (in computer visions)

1.1. Motivation

A regular polygon with n sides has $2n$ different symmetries: n rotational symmetries and n reflection symmetries.

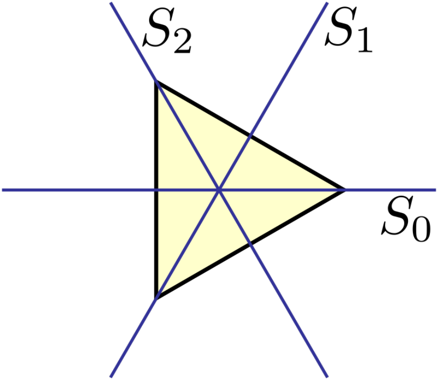
Stop sign

These rotations and reflections make up a group (will be called D_8).

Snowflake

These rotations and reflections "make" up a group (will be called D_6).

Regular triangle



These rotations and reflections "make" up a group (will be called D_3).

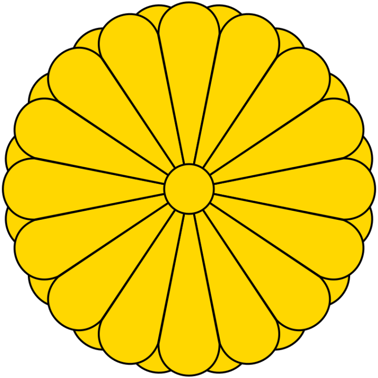
Dihedral group

1.2. Definition

Let n be a natural number. The *dihedral group* D_n is defined as the *rigid motions* taking a regular n-gon back to itself, with the operation being composition.

Dihedral group D_{16}

Imperial Seal of Japan, representing eightfold chrysanthemum with sixteen petals.

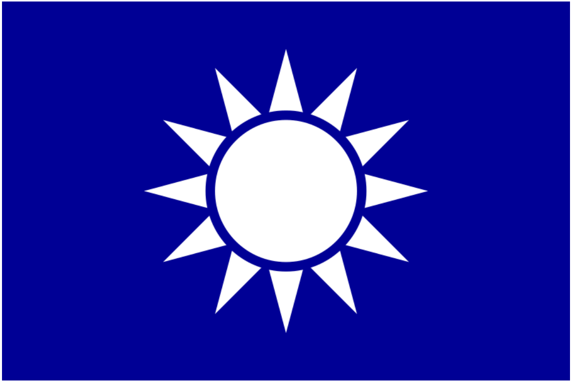


Dihedral group D_6

The Red Star of David

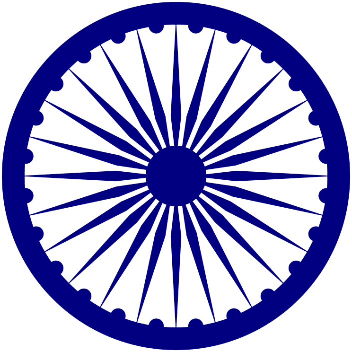
Dihedral group D_{12}

The Naval Jack of the Republic of China (White Sun)



Dihedral group D_{24}

Ashoka Chakra, as depicted on the National flag of the Republic of India.



Dihedral group

Let n be a positive integer and a regular polygon with n sides. Let r be the (counter-clockwise) rotation by $\frac{2\pi}{n}$ radian. Then, denote by r^i the counter-clockwise rotation by $\frac{2i\pi}{n}$ radian for every $i \in \mathbb{Z}$.

1.2. Theorem

The n rotations in D_n are $1, r, \cdots, r^{n-1}$.

Dihedral group

Let n be a positive integer and a regular polygon with n sides. Let r be the (counter-clockwise) rotation by $\frac{2\pi}{n}$ radian. Then, denote by r^i the counter-clockwise rotation by $\frac{2i\pi}{n}$ radian for every $i \in \mathbb{Z}$.

1.2. Theorem

The n rotations in D_n are $1, r, \cdots, r^{n-1}$.

Look at the first line.

Dihedral group

Let n be a positive integer and a regular polygon with n sides. Let s be a reflection across a line through a vertex.

1.3. Theorem

The n reflections in D_n are $s, rs, \cdots, r^{n-1}s$.

Dihedral group

Let n be a positive integer and a regular polygon with n sides. Let s be a reflection across a line through a vertex.

1.3. Theorem

The n reflections in D_n are $s, rs, \cdots, r^{n-1}s$.

Look at the second line.

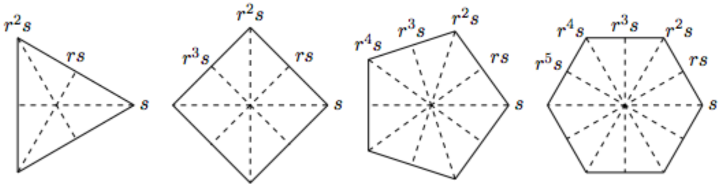
Dihedral group

1.4. Theorem

Let n be a positive integer and a regular polygon with n sides. Let a be the (counter-clockwise) rotation by $\frac{2\pi}{n}$ radian and b a reflection across a line through a vertex. Then

$$D_n = \{1, r, \cdots, r^{n-1}, s, rs, \cdots, r^{n-1}s\}.$$

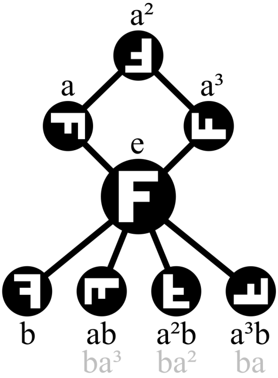
In particular, D_n has exactly $2n$ elements.



Lines of reflections.

Dihedral group D_4

$$D_4 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$$



Dihedral group

1.5. Theorem

Let n be a natural number. The *dihedral group* D_n is defined as the group with presentation

$$D_n = \langle a, b \mid a^n = 1, b^2 = 1, bab^{-1} = a^{-1} \rangle.$$

Dihedral group

1.5. Theorem

Let n be a natural number. The *dihedral group* D_n is defined as the group with presentation

$$D_n = \langle a, b \mid a^n = 1, b^2 = 1, bab^{-1} = a^{-1} \rangle.$$

Examples

write tables of elements of D_3 and D_4 with operations.

1.6. Theorem

$$D_n = \langle a, b \mid a^n = 1, b^2 = 1, (ab)^2 = 1 \rangle.$$

Exercises

1.1

Find the center of D_5, that is, find the set of all elements $a \in D_5$ such that $ab = ba$ for every $b \in D_5$.

1.2

Find the center of D_6, that is, find the set of all elements $a \in D_6$ such that $ab = ba$ for every $b \in D_6$.

1.3

Find the center of D_n for $n \geq 3$.

1.4

Show that $\langle a \rangle$ is a normal subgroup of D_n for $n \geq 3$.

Exercises

1.5

Find all subgroups of D_n for $n \geq 3$.

1.6

Find all normal subgroups of D_n for $n \geq 3$.

Semidirect products of subgroups

1.7. Definition

Let $(G, \cdot)$ be a group. Assume that A, B are subgroups of G and A is normal in G. If $G = AB$, that is, $G = \{ab \mid a \in A, b \in B\}$, and $A \cap B = \{1\}$, then G is called the semidirect product of A and B.

Semidirect products of subgroups

1.7. Definition

Let $(G, \cdot)$ be a group. Assume that A, B are subgroups of G and A is normal in G. If $G = AB$, that is, $G = \{ab \mid a \in A, b \in B\}$, and $A \cap B = \{1\}$, then G is called the semidirect product of A and B.

1.8. Theorem

$D_n = \langle a, b \mid a^n = b^2 = 1, bab^{-1} = a^{-1} \rangle$ is the semidirect product of $\langle a \rangle$ and $\langle b \rangle$.

Proof.

Infinite dihedral group

Recall that for element a in a group G, the order of a, denoted by $o(a)$, the smallest positive integer k in case there exists a positive integer n such that $a^n = 1$. Otherwise, we write $o(a) = \infty$.

Infinite dihedral group

Recall that for element a in a group G, the order of a, denoted by $o(a)$, the smallest positive integer k in case there exists a positive integer n such that $a^n = 1$. Otherwise, we write $o(a) = \infty$.

1.9. Definition

The infinite dihedral group, denoted by D_∞, is defined as the group with presentation

$$D_\infty = \langle a, b \mid o(a) = \infty, b^2 = 1, bab^{-1} = a^{-1} \rangle.$$

Example

An example of infinite dihedral symmetry is in aliasing of real-valued signals.

Semidirect products of subgroups

1.11. Theorem

$D_\infty = \langle a, b \mid o(a) = \infty, b^2 = 1, bab^{-1} = a^{-1} \rangle$ is the semidirect product of $\langle a \rangle$ and $\langle b \rangle$.

Proof.

Another definition of D_∞

1.12. Theorem

Let $\mathbb{Z}$ be the set of integers and $S_{\mathbb{Z}}$ the group of permutations on $\mathbb{Z}$. Then, D_∞ the set of all permutations $\sigma \in S_{\mathbb{Z}}$ such that $|\sigma(i) - \sigma(j)| = |i - j|$ for every $i, j \in \mathbb{Z}$.

Proof.

Another definition of D_∞

1.12. Theorem

Let $\mathbb{Z}$ be the set of integers and $S_\mathbb{Z}$ the group of permutations on $\mathbb{Z}$. Then, D_∞ the set of all permutations $\sigma \in S_\mathbb{Z}$ such that $|\sigma(i) - \sigma(j)| = |i - j|$ for every $i, j \in \mathbb{Z}$.

Proof.

1.13. Theorem

Let $\mathbb{Z}$ be the set of integers and $S_\mathbb{Z}$ the group of permutations on $\mathbb{Z}$. Then, an element $\sigma \in S_\mathbb{Z}$ in D_∞ if and only if there exists $n > 0$, either $\sigma(i) = i + n$ or $\sigma(i) = -i + n$ for every $i \in \mathbb{Z}$.

Proof.