Abstract algebras

Yanhua Wang
Shanghai University of Finance and Economics

2022.9

1. Chapter II. Groups

2.1 Definitions of Groups

Definition

Definition

A binary operation of a set G is a function

$$G \times G \to G,$$

for any $(a, b) \in G \times G$ a unique element $a \circ b$ or ab in G.

Definition

Definition

A group $(G, \circ)$ is a set with a binary operation, $G \times G \to G$, that satisfies the following axioms:

- (1) The binary operation is associative. That is $(a \circ b) \circ c = a \circ (b \circ c)$.

Definition

Definition

A group $(G, \circ)$ is a set with a binary operation, $G \times G \to G$, that satisfies the following axioms:

- (1) The binary operation is associative. That is $(a \circ b) \circ c = a \circ (b \circ c)$.
- (2) There exists an element e, called the identity element, such that for any element $a \in G$, $a \circ e = a = e \circ a$.

Definition

Definition

A group $(G, \circ)$ is a set with a binary operation, $G \times G \to G$, that satisfies the following axioms:

- (1) The binary operation is associative. That is $(a \circ b) \circ c = a \circ (b \circ c)$.
- (2) There exists an element e, called the identity element, such that for any element $a \in G$, $a \circ e = a = e \circ a$.
- (3) For each element $a \in G$, there exists an inverse element in G, denoted by a^{-1}, such that $a \circ a^{-1} = e = a^{-1} \circ a$.

Definition

Definition

A group $(G, \circ)$ is a set with a binary operation, $G \times G \to G$, that satisfies the following axioms:

- (1) The binary operation is associative. That is $(a \circ b) \circ c = a \circ (b \circ c)$.
- (2) There exists an element e, called the identity element, such that for any element $a \in G$, $a \circ e = a = e \circ a$.
- (3) For each element $a \in G$, there exists an inverse element in G, denoted by a^{-1}, such that $a \circ a^{-1} = e = a^{-1} \circ a$.

- Then $(G, \circ)$ is called a group.

Definition

Definition

A group $(G, \circ)$ is a set with a binary operation, $G \times G \to G$, that satisfies the following axioms:

- (1) The binary operation is associative. That is $(a \circ b) \circ c = a \circ (b \circ c)$.
- (2) There exists an element e, called the identity element, such that for any element $a \in G$, $a \circ e = a = e \circ a$.
- (3) For each element $a \in G$, there exists an inverse element in G, denoted by a^{-1}, such that $a \circ a^{-1} = e = a^{-1} \circ a$.

- Then $(G, \circ)$ is called a group.

- A group G with the property that $a \circ b = b \circ a$ for all $a, b \in G$ is called abelian or commutative. Groups are not satisfying this property are said to be nonabelian or noncommutative.

Definition

- (1) $(\mathbb{Z}, +)$ is a group with identity 0, the inverse of $n \in \mathbb{Z}$ is $-n$, "+" is associative and commutative. $(\mathbb{Z}, +)$ is an abelian group.

Definition

- (1) $(\mathbb{Z}, +)$ is a group with identity 0, the inverse of $n \in \mathbb{Z}$ is $-n$, "+" is associative and commutative. $(\mathbb{Z}, +)$ is an abelian group.
- (2) Let $\mathbb{R}^*$ be the set of nonzero elements of $\mathbb{R}$. Then $\mathbb{R}^*$ is a group with multiplication. Multiplication is associative. The identity of this group is 1 and the inverse of any element $a \in \mathbb{R}^*$ is just $\frac{1}{a}$.

Definition

- (1) $(\mathbb{Z}, +)$ is a group with identity 0, the inverse of $n \in \mathbb{Z}$ is $-n$, "+" is associative and commutative. $(\mathbb{Z}, +)$ is an abelian group.
- (2) Let $\mathbb{R}^*$ be the set of nonzero elements of $\mathbb{R}$. Then $\mathbb{R}^*$ is a group with multiplication. Multiplication is associative. The identity of this group is 1 and the inverse of any element $a \in \mathbb{R}^*$ is just $\frac{1}{a}$.
- (3) Let $M_2(\mathbb{R})$ be the set of 2×2 matrices over $\mathbb{R}$. $GL_2(\mathbb{R})$ be the subset of $M_2(\mathbb{R})$ consisting of invertible matrices. Then $(GL_2(\mathbb{R}), \cdot)$ is a group with matrix product, called the *general linear group*.

Definition

- (4) $(\mathbb{Z}_5, +)$ is a group.

Definition

- (4) $(\mathbb{Z}_5, +)$ is a group.
- The Cayley table of $(\mathbb{Z}_5, +)$ is the following.

Table: Cayley Table $(\mathbb{Z}_5, +)$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Definition

- (5). Let $n \in \mathbb{N}$, define a set $U(n) = \{a \mid \gcd(a, n) = 1\}$. Then $(U(n), \cdot)$ is a group called the *group of units* of $\mathbb{Z}_n$.

Definition

- (5). Let $n \in \mathbb{N}$, define a set $U(n) = \{a|\, \gcd(a, n) = 1\}$. Then $(U(n), \cdot)$ is a group called the *group of units* of $\mathbb{Z}_n$.
- $(U_8 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}, \cdot)$.

Definition

- (5). Let $n \in \mathbb{N}$, define a set $U(n) = \{a |\, \gcd(a, n) = 1\}$. Then $(U(n), \cdot)$ is a group called the *group of units* of $\mathbb{Z}_n$.
- $(U_8 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}, \cdot)$.
- Cayley table for $(U_8, \cdot)$ is

Table: Caley Table $(U(8), \cdot)$

$\cdot$	**1**	**3**	**5**	**7**
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Definition

- Let $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$ where $i^2 = -1$ the imaginary number, and

$$I^2 = J^2 = K^2 = -1,$$
$$IJ = K, JK = I, KI = J,$$
$$JI = -K, KJ = -I, IK = -J.$$

Definition

- Let $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$ where $i^2 = -1$ the imaginary number, and

$$\begin{aligned} I^2 &= J^2 = K^2 = -1, \\ IJ &= K, JK = I, KI = J, \\ JI &= -K, KJ = -I, IK = -J. \end{aligned}$$

- The set $(Q_8 = \{\pm 1, \pm I, \pm J, \pm K\}, \cdot)$ is a group which called the *quaternion group*.

Definition

- Let $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$ where $i^2 = -1$ the imaginary number, and

$$\begin{aligned} &I^2 = J^2 = K^2 = -1, \\ &IJ = K, JK = I, KI = J, \\ &JI = -K, KJ = -I, IK = -J. \end{aligned}$$

- The set $(Q_8 = \{\pm 1, \pm I, \pm J, \pm K\}, \cdot)$ is a group which called the *quaternion group*.
- Q_8 is unabelian. The first nonabelian algebra.

Definition

Denote $\mathcal{Q} = \{a + bI + cJ + dK | a, b, c, d \in \mathbb{R}\}$. Note that

- (i) If $c = d = 0$, then $\mathcal{Q} = \mathbb{C}$.

Definition

Denote $\mathcal{Q} = \{a + bI + cJ + dK | a, b, c, d \in \mathbb{R}\}$. Note that

- (i) If $c = d = 0$, then $\mathcal{Q} = \mathbb{C}$.
- (ii) If $b = c = d = 0$, then $\mathcal{Q} = \mathbb{R}$

Definition

Denote $\mathcal{Q} = \{a + bI + cJ + dK | a, b, c, d \in \mathbb{R}\}$. Note that

- (i) If $c = d = 0$, then $\mathcal{Q} = \mathbb{C}$.
- (ii) If $b = c = d = 0$, then $\mathcal{Q} = \mathbb{R}$
- The conjugate of an element $q \in \mathcal{Q}$ is $\overline{q} = a - bI - cJ - dK$, and $|q| = \sqrt{q\overline{q}} = \sqrt{a^2 + b^2 + c^2 + d^2}$.

Definition

Denote $\mathcal{Q} = \{a + bI + cJ + dK | a, b, c, d \in \mathbb{R}\}$. Note that

- (i) If $c = d = 0$, then $\mathcal{Q} = \mathbb{C}$.
- (ii) If $b = c = d = 0$, then $\mathcal{Q} = \mathbb{R}$
- The conjugate of an element $q \in \mathcal{Q}$ is $\overline{q} = a - bI - cJ - dK$, and $|q| = \sqrt{q\overline{q}} = \sqrt{a^2 + b^2 + c^2 + d^2}$.
- Define " + " and " $\cdot$ " of $\mathcal{Q}$ as following:

$$
\begin{aligned}
q_1 + q_2 &= (a_1 + a_2) + (b_1 + b_2)I + (c_1 + c_2)J + (d_1 + d_2)K, \\
q_1 q_2 &= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) \\
&\quad +(a_1 b_2 + b_1 a_2 + c_1 d_2 - c_2 d_1)I \\
&\quad +(a_1 c_2 + a_2 c_1 + b_2 d_1 - d_2 b_1)J \\
&\quad +(a_1 d_2 + d_1 a_2 + b_1 c_2 - b_2 c_1)K.
\end{aligned}
$$

Definition

Denote $\mathcal{Q} = \{a + bI + cJ + dK | a, b, c, d \in \mathbb{R}\}$. Note that

- (i) If $c = d = 0$, then $\mathcal{Q} = \mathbb{C}$.
- (ii) If $b = c = d = 0$, then $\mathcal{Q} = \mathbb{R}$
- The conjugate of an element $q \in \mathcal{Q}$ is $\overline{q} = a - bI - cJ - dK$, and $|q| = \sqrt{q\overline{q}} = \sqrt{a^2 + b^2 + c^2 + d^2}$.
- Define " + " and " $\cdot$ " of $\mathcal{Q}$ as following:

$$
\begin{aligned}
q_1 + q_2 &= (a_1 + a_2) + (b_1 + b_2)I + (c_1 + c_2)J + (d_1 + d_2)K, \\
q_1 q_2 &= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) \\
&\quad +(a_1 b_2 + b_1 a_2 + c_1 d_2 - c_2 d_1)I \\
&\quad +(a_1 c_2 + a_2 c_1 + b_2 d_1 - d_2 b_1)J \\
&\quad +(a_1 d_2 + d_1 a_2 + b_1 c_2 - b_2 c_1)K.
\end{aligned}
$$

- $\mathcal{Q}$ is uncommutative under " $\cdot$ ".

Definition

Definition

A group is finite or has finite order if it contains a finite number of elements. Otherwise, the group is called infinite.

-

Definition

Definition

A group is finite or has finite order if it contains a finite number of elements. Otherwise, the group is called infinite.

-

Proposition

The identity element in a group G is unique. i.e. there exists a unique element e s.t. $eg = ge = e, \forall g \in G$.

-

Definition

Definition

A group is finite or has finite order if it contains a finite number of elements. Otherwise, the group is called infinite.

-

Proposition

The identity element in a group G is unique. i.e. there exists a unique element e s.t. $eg = ge = e, \forall g \in G$.

-
- Proof: Assume that e and e' are identities of G. If e is the identity of G, for $e' \in G$, then $ee' = e'$. If e' is the identity of G, then $ee' = e$, so $e = e'$.

Definition

Proposition

If g is any element in a group G, then the inverse of g is unique.

-

Definition

Proposition

If g is any element in a group G, then the inverse of g is unique.

-
- Proof: For $g \in G$, assume that g' and g'' are inverses of g, we have $gg' = g'g = e$ and $gg'' = g''g = e$. Then

$$g' = g'e = g'(gg'') = (g'g))g'' = eg'' = g''.$$

Definition

Proposition

Let G be a group. For any $a \in G$, then $(a^{-1})^{-1}$=a.

- Observe that $a^{-1}(a^{-1})^{-1} = e$. Consequently, multiplying both sides of this equation by a, we have $(a^{-1})^{-1} = e(a^{-1})^{-1} = aa^{-1}(a^{-1})^{-1} = ae = a$.

Definition

Proposition

Let G be a group and a and b be any two elements in G, then the equations $ax = b$ and $ya = b$ have unique solution in G.

- Proof: Suppose that $ax = b$, then $x = ex = a^{-1}ax = a^{-1}b$. Suppose that x_1 and x_2 are both solutions of $ax = b$; then $ax_1 = b = ax_2$. So $x_1 = a^{-1}ax_1 = a^{-1}ax_2 = x_2$.

Definition

Proposition

Let G be a group and a and b be any two elements in G, then the equations $ax = b$ and $ya = b$ have unique solution in G.

- Proof: Suppose that $ax = b$, then $x = ex = a^{-1}ax = a^{-1}b$. Suppose that x_1 and x_2 are both solutions of $ax = b$; then $ax_1 = b = ax_2$. So $x_1 = a^{-1}ax_1 = a^{-1}ax_2 = x_2$.

Proposition

If G is a group, and $a, b, c \in G$, then $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$. Here, $ba = ca$ implies $b = c$ is called right cancellation. $ab = ac$ implies $b = c$ is called left cancellation.

-

Definition

Theorem

In a group, denote $g^n = g \circ g \circ \cdots \circ g$ *and* $g^{-n} = g^{-1} \circ g^{-1} \circ \cdots \circ g^{-1}$, *then we have usual laws of exponents hold.*

$$
\begin{aligned}
&g^m g^n = g^{m+n},\\
&(g^m)^n = g^{mn},\\
&(gh)^n = ((gh)^{-1})^{-n} = ((h^{-1})(g^{-1}))^{-n}.
\end{aligned}
$$

- In general $gh \neq hg$, $(gh)^n \neq g^n h^n$.

Definition

Theorem

In a group, denote $g^n = g \circ g \circ \cdots \circ g$ *and* $g^{-n} = g^{-1} \circ g^{-1} \circ \cdots \circ g^{-1}$*, then we have usual laws of exponents hold.*

$$\begin{aligned} & g^m g^n = g^{m+n}, \\ & (g^m)^n = g^{mn}, \\ & (gh)^n = ((gh)^{-1})^{-n} = ((h^{-1})(g^{-1}))^{-n}. \end{aligned}$$

- In general $gh \neq hg$, $(gh)^n \neq g^n h^n$.
- If the operation of a group is "+", $m, n \in \mathbb{Z}, g, h \in G$, then

$$ng = g + \cdots + g, \; mg + ng = (m+n)g,$$

$$m(ng) = (mn)g, \; m(g+h) = mg + mh.$$

2.2 Subgroups

Subgroups

Definition

A subgroup H of a group $(G, \circ)$ to be a subset H of G such that H is a group under the group operation of G.

Example

Let $\mathbb{Q}^* = \{\frac{p}{q} | p, q$ are nonzero integers$\}$. Then $\mathbb{Q}^*$ is a proper subgroup of $\mathbb{R}^*$.

-

Subgroups

Definition

A subgroup H of a group $(G, \circ)$ to be a subset H of G such that H is a group under the group operation of G.

Example

Let $\mathbb{Q}^* = \{\frac{p}{q} | p, q$ are nonzero integers$\}$. Then $\mathbb{Q}^*$ is a proper subgroup of $\mathbb{R}^*$.

-

Example

Recall that $\mathbb{C}^*$ is the multiplicative group of nonzero complex numbers. Let $H = \{1, -1, i, -i\} \subseteq \mathbb{C}^*$. H is a subgroup of $\mathbb{C}^*$.

-

Subgroups

Example

Let $SL_2(\mathbb{R}) = \{A | A \in Gl_2(\mathbb{R}), |A| = 1\}$ be the subset of $GL_2(\mathbb{R})$. The group $SL_2(\mathbb{R})$ is called the *special linear group*. $SL_2(\mathbb{R}) \subseteq GL_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$.

Proposition

A subset H of G is a subgroup if and only if it satisfies the following conditions.
(1). The identity e of G is in H.
(2). If $h_1, h_2 \in H$, then $h_1 h_2 \in H$.
(3). If $h \in H$, then $h^{-1} \in H$.

-

Subgroups

- Proof: First suppose that H is a subgroup of G. Let e is the identity of G.
  (1). Since H is a group, it must have an identity e_H. We must show that $e_H = e$. We know that $e_H e_H = e_H$ and that $ee_H = e_H e = e_H$; hence, $ee_H = e_H e_H$. By right-hand cancellation, $e = e_H$.

Subgroups

- Proof: First suppose that H is a subgroup of G. Let e is the identity of G.
  (1). Since H is a group, it must have an identity e_H. We must show that $e_H = e$. We know that $e_H e_H = e_H$ and that $ee_H = e_H e = e_H$; hence, $ee_H = e_H e_H$. By right-hand cancellation, $e = e_H$.
- (2) Since a subgroup H is a group. For any $h_1, h_2 \in H$, then $h_1 h_2 \in H$.

Subgroups

- Proof: First suppose that H is a subgroup of G. Let e is the identity of G.
  (1). Since H is a group, it must have an identity e_H. We must show that $e_H = e$. We know that $e_H e_H = e_H$ and that $ee_H = e_H e = e_H$; hence, $ee_H = e_H e_H$. By right-hand cancellation, $e = e_H$.
- (2) Since a subgroup H is a group. For any $h_1, h_2 \in H$, then $h_1 h_2 \in H$.
- (3) Let $h \in H$. Since H is a group, there is an element $g \in H$ such that $hg = gh = e$. By the uniqueness of the inverse in G, $g = h^{-1}$.

Subgroups

- Proof: First suppose that H is a subgroup of G. Let e is the identity of G.
  (1). Since H is a group, it must have an identity e_H. We must show that $e_H = e$. We know that $e_H e_H = e_H$ and that $ee_H = e_H e = e_H$; hence, $ee_H = e_H e_H$. By right-hand cancellation, $e = e_H$.
- (2) Since a subgroup H is a group. For any $h_1, h_2 \in H$, then $h_1 h_2 \in H$.
- (3) Let $h \in H$. Since H is a group, there is an element $g \in H$ such that $hg = gh = e$. By the uniqueness of the inverse in G, $g = h^{-1}$.
- Conversely, if (1)-(3) hold, we must show that H is a group under the same operation as G; however, these conditions plus the associativity of the binary operation are exactly the axioms stated in the definition of a group.

Subgroups

Proposition

Let H be a subset of a group G. Then H is a subgroup of G if and only if H is nonempty, and whenever $g, h \in H$, then $gh^{-1} \in H$.

Subgroups

- Proof: First assume that H is a subgroup of G. Since h is in H, its inverse $h^{-1} \in H$. Because of the closure of the group operation, $gh^{-1} \in H$.

Subgroups

- Proof: First assume that H is a subgroup of G. Since h is in H, its inverse $h^{-1} \in H$. Because of the closure of the group operation, $gh^{-1} \in H$.
- Conversely, suppose that $H \subset G$ such that H is nonempty and $gh^{-1} \in H$ whenever $g, h \in H$. If $g \in H$, then $gg^{-1} = e \in H$. If $g \in H$, then $eg^{-1} = g^{-1} \in H$.

Subgroups

- Proof: First assume that H is a subgroup of G. Since h is in H, its inverse $h^{-1} \in H$. Because of the closure of the group operation, $gh^{-1} \in H$.
- Conversely, suppose that $H \subset G$ such that H is nonempty and $gh^{-1} \in H$ whenever $g, h \in H$. If $g \in H$, then $gg^{-1} = e \in H$. If $g \in H$, then $eg^{-1} = g^{-1} \in H$.
- Now let $h_1, h_2 \in H$. We must show that their product is also in H. However, $h_1(h_2^{-1})^{-1} = h_1 h_2 \in H$. Hence, H is a subgroup of G.

2.3 Cyclic groups

Cyclic group

Theorem

Let G be a group, $g \in G$. Then the set $\langle g \rangle = \{g^k | k \in \mathbb{Z}\}$ is the smallest subgroup of G. Furthermore, $\langle g \rangle$ is the smallest subgroup of G contains g.

- Proof: Since $a^0 = e$, thus the identity in G. If h and f are any two elements in $\langle g \rangle$, then by the definition of $\langle g \rangle$, we can write $h = g^m$ and $f = g^n$ for some integers m and n. So $hf = g^m g^n = g^{m+n}$ is again in $\langle g \rangle$.

Cyclic group

Theorem

Let G be a group, $g \in G$. Then the set $\langle g \rangle = \{g^k | k \in \mathbb{Z}\}$ is the smallest subgroup of G. Furthermore, $\langle g \rangle$ is the smallest subgroup of G contains g.

- Proof: Since $a^0 = e$, thus the identity in G. If h and f are any two elements in $\langle g \rangle$, then by the definition of $\langle g \rangle$, we can write $h = g^m$ and $f = g^n$ for some integers m and n. So $hf = g^m g^n = g^{m+n}$ is again in $\langle g \rangle$.
- Finally, if $h = g^n$ in $\langle g \rangle$, then the inverse $h^{-1} = g^{-n}$ is also in $\langle g \rangle$.

Cyclic group

Theorem

Let G be a group, $g \in G$. Then the set $\langle g \rangle = \{g^k | k \in \mathbb{Z}\}$ is the smallest subgroup of G. Furthermore, $\langle g \rangle$ is the smallest subgroup of G contains g.

- Proof: Since $a^0 = e$, thus the identity in G. If h and f are any two elements in $\langle g \rangle$, then by the definition of $\langle g \rangle$, we can write $h = g^m$ and $f = g^n$ for some integers m and n. So $hf = g^m g^n = g^{m+n}$ is again in $\langle g \rangle$.
- Finally, if $h = g^n$ in $\langle g \rangle$, then the inverse $h^{-1} = g^{-n}$ is also in $\langle g \rangle$.
- Clearly, any subgroup H of G containing g must contain all the powers of g by closure property of group, hence H contains $\langle g \rangle$. Therefore, $\langle g \rangle$ is the smallest subgroup of G containing g.

Cyclic group

Definition

$\langle g \rangle$ is called the *cyclic subgroup* generated by g. If $G = \langle g \rangle$, then G is called a cyclic group, g is a generator of G.

- G is a cyclic group, then $G = \{\cdots, g^{-2}, g^{-1}, g^0, g^1, g^2, \cdots\}$ under multiplication or $G = \{\cdots, -2g, -g, 0, g, 2g, \cdots\}$ under addition.

Cyclic group

Definition

$\langle g \rangle$ is called the *cyclic subgroup* generated by g. If $G = \langle g \rangle$, then G is called a cyclic group, g is a generator of G.

- G is a cyclic group, then $G = \{\cdots, g^{-2}, g^{-1}, g^0, g^1, g^2, \cdots\}$ under multiplication or $G = \{\cdots, -2g, -g, 0, g, 2g, \cdots\}$ under addition.
- If $g \in G$, we define the *order* of g to be the smallest positive number n, such that $g^n = e$, and we write $|g| = n$.

Cyclic group

Definition

$\langle g \rangle$ is called the *cyclic subgroup* generated by g. If $G = \langle g \rangle$, then G is called a cyclic group, g is a generator of G.

- G is a cyclic group, then $G = \{\cdots, g^{-2}, g^{-1}, g^0, g^1, g^2, \cdots\}$ under multiplication or $G = \{\cdots, -2g, -g, 0, g, 2g, \cdots\}$ under addition.
- If $g \in G$, we define the *order* of g to be the smallest positive number n, such that $g^n = e$, and we write $|g| = n$.
- If there is no such integer n, we say that the order of g is infinite and write $|a| = \infty$ to denote the order of g.

Cyclic group

Example

The groups $\mathbb{Z}$ and $\mathbb{Z}_n$ are cyclic groups. And $\mathbb{Z} = \langle 1 \rangle$, $\mathbb{Z}_n = \langle \overline{1} \rangle$. Moreover, $\mathbb{Z} = \langle -1 \rangle$, $\mathbb{Z}_n = \langle \overline{-1} \rangle$. Notice that a cyclic group can have more than a single generator.

-

Cyclic group

Example

The groups $\mathbb{Z}$ and $\mathbb{Z}_n$ are cyclic groups. And $\mathbb{Z} = \langle 1 \rangle$, $\mathbb{Z}_n = \langle \overline{1} \rangle$. Moreover, $\mathbb{Z} = \langle -1 \rangle$, $\mathbb{Z}_n = \langle \overline{-1} \rangle$. Notice that a cyclic group can have more than a single generator.

-

Example

$\mathbb{Z}_6$ is a cyclic group generated by $\overline{1}$ or $\overline{5}$. Not every element in a cyclic group is necessarily a generator of the group. $\overline{2} \in \mathbb{Z}_6$, the cyclic subgroup generated by $\overline{2}$ is $\{\overline{0}, \overline{2}, \overline{4}\}$.

-

Cyclic group

Example

$U(9) = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\} = \langle \overline{2} \rangle.$

-

Cyclic group

Example

$U(9) = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\} = \langle \overline{2} \rangle.$

-
- Show that $(U(9), \cdot) = \langle 2 \rangle$.

Cyclic group

Example

$U(16) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{15}\}$ is not a cyclic group, we can not find a generator in it. Every element of $U(16)$ generate $\mathbb{Z}(16)$, that is $\mathbb{Z}_{16}$.

- Give the generate relation of $(\mathbb{Z}_{16}, +) = \langle \overline{3} \rangle$.

Cyclic group

Theorem

Every cyclic group is abelian.

Proof.

Suppose $G = \langle a \rangle, g_1, g_2 \in G$, then $g_1 = a^m, g_2 = a^k$. Since

$$g_1 g_2 = a^m a^k = a^{m+k} = a^{k+m} = a^k a^m = g_2 g_1,$$

G is abelian. $\square$

-

Cyclic group

Theorem

Every subgroup of a cyclic group is cyclic.

- Proof: Let $G = \langle a \rangle$, H be a subgroup of G. If $H = \{e\}$, then H is cycle. If $H \neq \{e\}$, then H contains $a^m \neq e$. Since H must contains $(a^m)^{-1}$, we may assume that $m > 0$.

Cyclic group

Theorem

Every subgroup of a cyclic group is cyclic.

- Proof: Let $G = \langle a \rangle$, H be a subgroup of G. If $H = \{e\}$, then H is cycle. If $H \neq \{e\}$, then H contains $a^m \neq e$. Since H must contains $(a^m)^{-1}$, we may assume that $m > 0$.
- Let m be the smallest positive integer such that $h = a^m \in H$.

Cyclic group

- Assume that $h' = a^k \in H, k \in \mathbb{Z}$. By the division Algorithm, there exist integers q, r such that $k = mq + r, 0 \leq r < m$, then
$$h' = a^k = a^{mq+r} = a^{mq}a^r = h^q a^r.$$
So $a^r = a^k a^{-mq} \in G$.

Cyclic group

- Assume that $h' = a^k \in H, k \in \mathbb{Z}$. By the division Algorithm, there exist integers q, r such that $k = mq + r, 0 \leq r < m$, then
$$h' = a^k = a^{mq+r} = a^{mq}a^r = h^q a^r.$$
So $a^r = a^k a^{-mq} \in G$.
- Since $a^k, a^{mq} \in H$, $a^r \in H$. However, m was the smallest positive number such that a^m was in H. Consequently, $r = 0$ and so $k = mq$. Therefore $h' = a^k = a^{mq} = h^q$, and H is generated by h.

Cyclic group

- The group $(\mathbb{Z}, +)$ is generated by 1 or -1. For any $m \in \mathbb{Z}$, $m = m \cdot 1$, where $m \in \mathbb{Z}$.

Cyclic group

- The group $(\mathbb{Z}, +)$ is generated by 1 or -1. For any $m \in \mathbb{Z}$, $m = m \cdot 1$, where $m \in \mathbb{Z}$.
- $2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, \dots\}$ is a subgroup of $\mathbb{Z}$.

Cyclic group

- The group $(\mathbb{Z}, +)$ is generated by 1 or -1. For any $m \in \mathbb{Z}$, $m = m \cdot 1$, where $m \in \mathbb{Z}$.
- $2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ is a subgroup of $\mathbb{Z}$.
- All subgroups of $\mathbb{Z}$ are $n\mathbb{Z}, n \in \mathbb{N}$.

Cyclic group

Proposition

Let G be a cyclic group of order n and $G = \{a | a^n = e\}$. Then $a^k = e$ if and only if $n \mid k$.

- Suppose that $a^k = e$. By the division Algorithm, $k = nq + r$, where $0 \leq r < n$, hence

$$e = a^k = a^{nq+r} = a^{nq}a^r = ea^r = a^r.$$

  Since the smallest positive integer m such that $a^m = e$ is n, $r = 0$.

Cyclic group

Proposition

Let G be a cyclic group of order n and $G = \{a | a^n = e\}$. Then $a^k = e$ if and only if $n \mid k$.

- Suppose that $a^k = e$. By the division Algorithm, $k = nq + r$, where $0 \leq r < n$, hence

$$e = a^k = a^{nq+r} = a^{nq}a^r = ea^r = a^r.$$

  Since the smallest positive integer m such that $a^m = e$ is n, $r = 0$.

- Conversely, if n divides k, then $k = ns$ for some integer s. Consequently,

$$a^k = a^{ns} = (a^n)^s = e^s = e.$$

Cyclic group

Theorem

Let G be a cyclic group of order n and suppose that $a \in G$ is a generator of the group. If $b = a^k$, then the order of b is $\frac{n}{d}$, where $d = gcd(k, n)$.

-

Cyclic group

Theorem

Let G be a cyclic group of order n and suppose that $a \in G$ is a generator of the group. If $b = a^k$, then the order of b is $\frac{n}{d}$, where $d = gcd(k, n)$.

-
- Let m be the order of $b = a^k$, then $e = b^m = (a^k)^m = a^{km}$. Since n is the order of G, $n \mid km$. Thus $\frac{n}{d}$ prime to $\frac{k}{d}$. Hence, if $\frac{n}{d}$ divides $\frac{km}{d}$, we must have $\frac{n}{d} \mid m$. Thus, this kind smallest m is $\frac{n}{d}$.

Cyclic group

Theorem

Let G be a cyclic group of order n and suppose that $a \in G$ is a generator of the group. If $b = a^k$, then the order of b is $\frac{n}{d}$, where $d = gcd(k, n)$.

-
- Let m be the order of $b = a^k$, then $e = b^m = (a^k)^m = a^{km}$. Since n is the order of G, $n \mid km$. Thus $\frac{n}{d}$ prime to $\frac{k}{d}$. Hence, if $\frac{n}{d}$ divides $\frac{km}{d}$, we must have $\frac{n}{d} \mid m$. Thus, this kind smallest m is $\frac{n}{d}$.

Corollary

The generator of $\mathbb{Z}_n$ are the integers r so that $gcd(r, n) = 1$.

-

Cyclic group

Proposition

Let $G = \langle a \rangle$ be a cyclic group.
(1) If G is infinite, then each subgroup of G has the form $G_m = \langle a^m \rangle$, where $m \geq 0$. Furthermore, the G_m are all distinct and G_m has infinite order if $m > 0$.
(2) If G has finite order n, then it has exactly one subgroup of order d for each positive divisor d of n, namely $\langle a^{\frac{n}{d}} \rangle$.

- If G is infinite, $G_2 = \{\cdots, g^{-2}, e, g^2, g^4, \cdots, \}$.

Cyclic group

Proposition

Let $G = \langle a \rangle$ be a cyclic group.
(1) If G is infinite, then each subgroup of G has the form $G_m = \langle a^m \rangle$, where $m \geq 0$. Furthermore, the G_m are all distinct and G_m has infinite order if $m > 0$.
(2) If G has finite order n, then it has exactly one subgroup of order d for each positive divisor d of n, namely $\langle a^{\frac{n}{d}} \rangle$.

- If G is infinite, $G_2 = \{\cdots, g^{-2}, e, g^2, g^4, \cdots, \}$.
- $G_3 = \{\cdots, g^{-3}, e, g^3, g^6, \cdots, \}$.

Cyclic group

Proposition

Let $G = \langle a \rangle$ be a cyclic group.
(1) If G is infinite, then each subgroup of G has the form $G_m = \langle a^m \rangle$, where $m \geq 0$. Furthermore, the G_m are all distinct and G_m has infinite order if $m > 0$.
(2) If G has finite order n, then it has exactly one subgroup of order d for each positive divisor d of n, namely $\langle a^{\frac{n}{d}} \rangle$.

- If G is infinite, $G_2 = \{\cdots, g^{-2}, e, g^2, g^4, \cdots, \}$.
- $G_3 = \{\cdots, g^{-3}, e, g^3, g^6, \cdots, \}$.
- If G is finite with order $2m$, then $G_2 = \{e, g^2, g^4, \cdots, g^{2m-2}\}$.

Cyclic group

- Proof: Assume first that G is infinite and let H be a subgroup of G, then H is cyclic, say $H = \langle a^m \rangle$ where $m \geq 0$. Thus $H = G_m$.

Cyclic group

- Proof: Assume first that G is infinite and let H be a subgroup of G, then H is cyclic, say $H = \langle a^m \rangle$ where $m \geq 0$. Thus $H = G_m$.
- If a^m had finite order s, then $a^{ms} = e$, since a has infinite order. This can only mean that $m = 0$ and $H = \{e\}$. Thus H is certainly infinite cyclic if $m > 0$.

Cyclic group

- Proof: Assume first that G is infinite and let H be a subgroup of G, then H is cyclic, say $H = \langle a^m \rangle$ where $m \geq 0$. Thus $H = G_m$.
- If a^m had finite order s, then $a^{ms} = e$, since a has infinite order. This can only mean that $m = 0$ and $H = \{e\}$. Thus H is certainly infinite cyclic if $m > 0$.
- Next $G_m = G_s$ implies that $a^m \in \langle a^s \rangle$ and $a^s \in \langle a^m \rangle$, that is, $m|s$ and $s|m$, so that $m = s$. Thus all the G_m's are different.

Definition

- Next let G have finite order n and suppose d is a positive divisor of n. Now $(a^{\frac{n}{d}})^d = a^n = e$, so the order l of $a^{\frac{n}{d}}$ must divide d. But also $a^{\frac{nl}{d}} = e$, and hence n divides $\frac{nl}{d}$, i.e., d divides l. It follows that $l = d$ and thus $\langle a^{\frac{n}{d}} \rangle$ has order exactly d.

Definition

- Next let G have finite order n and suppose d is a positive divisor of n. Now $(a^{\frac{n}{d}})^d = a^n = e$, so the order l of $a^{\frac{n}{d}}$ must divide d. But also $a^{\frac{nl}{d}} = e$, and hence n divides $\frac{nl}{d}$, i.e., d divides l. It follows that $l = d$ and thus $\langle a^{\frac{n}{d}} \rangle$ has order exactly d.
- To complete the proof, suppose that $H = \langle a^r \rangle$ is another subgroup with order d. Then $a^{rd} = e$, so n divides rd and $\frac{n}{d}$ divides r. This shows that $H = \langle a^r \rangle \subseteq \langle a^{\frac{n}{d}} \rangle$. But $|H| = |\langle a^{\frac{n}{d}} \rangle| = d$, from which it follows that $H = \langle a^{\frac{n}{d}} \rangle$. Consequently there is exactly one subgroup of order d.

2.4 Permutation groups

Permutation

A permutation of a set X is a bijection from X to X.

- Assume that $X = \{x_1, x_2, \cdots, x_n\}$, σ be a permutation of X. Since σ is injective, then $\sigma(x_1), \sigma(x_2), \cdots, \sigma(x_n)$ are all different and therefore constitute all n elements of the set X, but in some different order from $x_1, \cdots, x_n$.

Permutation

A permutation of a set X is a bijection from X to X.

- Assume that $X = \{x_1, x_2, \cdots, x_n\}$, σ be a permutation of X. Since σ is injective, then $\sigma(x_1), \sigma(x_2), \cdots, \sigma(x_n)$ are all different and therefore constitute all n elements of the set X, but in some different order from $x_1, \cdots, x_n$.
- $$\sigma = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ \sigma(x_1) & \sigma(x_2) & \cdots & \sigma(x_n) \end{pmatrix}$$

Permutation

A permutation of a set X is a bijection from X to X.

- Assume that $X = \{x_1, x_2, \cdots, x_n\}$, σ be a permutation of X. Since σ is injective, then $\sigma(x_1), \sigma(x_2), \cdots, \sigma(x_n)$ are all different and therefore constitute all n elements of the set X, but in some different order from $x_1, \cdots, x_n$.
- $$\sigma = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ \sigma(x_1) & \sigma(x_2) & \cdots & \sigma(x_n) \end{pmatrix}$$
- Let $|X| = n$, denote the set of all permutations of X as S_n.

Permutation

- $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$

Permutation

- $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$
- $\delta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}.$

Permutation

Theorem

S_n is a group with $n!$ elements. The operation of S_n is the composition of bijections.

- Proof: Let X be a set. It is obvious that $S_n \times S_n \to S_n$ is a binary operation of S_n since the composition of bijections is still a bijection of X.

Permutation

Theorem

S_n is a group with $n!$ elements. The operation of S_n is the composition of bijections.

- Proof: Let X be a set. It is obvious that $S_n \times S_n \to S_n$ is a binary operation of S_n since the composition of bijections is still a bijection of X.
- And the composition of bijections is associative. The identity of S_n is identity map. If $f \in S_n$, then $f^{-1} \in S_n$ since f is a bijection.

Permutation

- Consider the number of ways of constructing the second row of a permutation

$$\sigma = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ \sigma(x_1) & \sigma(x_2) & \cdots & \sigma(x_n) \end{pmatrix}$$

  There are n choices for σx_1, but only $n-1$ choices for $\sigma(x_2)$. Next we cannot choose σx_1 or $\sigma(x_2)$, so there are $n-2$ choices for $\sigma(x_3)$, and so on.

Permutation

- Consider the number of ways of constructing the second row of a permutation

$$\sigma = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ \sigma(x_1) & \sigma(x_2) & \cdots & \sigma(x_n) \end{pmatrix}$$

  There are n choices for σx_1, but only $n-1$ choices for $\sigma(x_2)$. Next we cannot choose σx_1 or $\sigma(x_2)$, so there are $n-2$ choices for $\sigma(x_3)$, and so on.
- Finally, there is just one choice for $\sigma(x_n)$. Each choice of $\sigma(x_i)$ can occur with each choice of $\sigma(x_j)$. Therefore the number of different permutations of X is

$$n(n-1)(n-2)\cdots 1 = n!.$$

Permutation

- S_3:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Permutation

Definition

S_n is called a symmetric group. A subgroup of S_n is called a permutation group.

Definition

Let $x_1, x_2, \cdots, x_t$ be distinct elements of the set $\{x_1, x_2, \cdots, x_n\}$. A *cycle* of length t is a permutation σ if

$$\sigma = \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_t \\ x_2 & x_3 & x_4 & \cdots & x_1 \end{pmatrix},$$

while leaving all the remaining elements of $\{x_1, x_2, \cdots, x_n\}$ fixed.

- Write $\sigma = (x_1 x_2 \cdots x_t)$.

Permutation

Definition

S_n is called a symmetric group. A subgroup of S_n is called a permutation group.

Definition

Let $x_1, x_2, \cdots, x_t$ be distinct elements of the set $\{x_1, x_2, \cdots, x_n\}$. A *cycle* of length t is a permutation σ if

$$\sigma = \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_t \\ x_2 & x_3 & x_4 & \cdots & x_1 \end{pmatrix},$$

while leaving all the remaining elements of $\{x_1, x_2, \cdots, x_n\}$ fixed.

- Write $\sigma = (x_1 x_2 \cdots x_t)$.
- Two cycles $\sigma = (x_1 \cdots x_s), \tau = (y_1 \cdots y_t)$ in S_n are disjoint if $x_i \neq y_j$ for all i and j.

Permutation

Proposition

Let σ and τ be two disjoint cycles in S_X. Then $\sigma\tau = \tau\sigma$.

- Proof: Let $\sigma = (x_1 \ x_2 \ \cdots x_s), \tau = (y_1 \ y_2 \cdots y_t)$, we want to show $\sigma\tau(x) = \tau\sigma(x)$ for any $x \in X$. If x is neither $x_1 \cdots x_s$ nor $y_1 \cdots y_t$, then both σ and τ fix x. That is $\sigma(x) = x$ and $tau(x) = x$. Hence,

  $$\sigma\tau(x) = \sigma(\tau(x)) = \sigma(x) = x = \tau(x) = x = \tau(\sigma(x)) = \tau\sigma(x).$$

Permutation

Proposition

Let σ and τ be two disjoint cycles in S_X. Then $\sigma\tau = \tau\sigma$.

- Proof: Let $\sigma = (x_1\ x_2\ \cdots x_s), \tau = (y_1\ y_2 \cdots y_t)$, we want to show $\sigma\tau(x) = \tau\sigma(x)$ for any $x \in X$. If x is neither $x_1 \cdots x_s$ nor $y_1 \cdots y_t$, then both σ and τ fix x. That is $\sigma(x) = x$ and $tau(x) = x$. Hence,

  $$\sigma\tau(x) = \sigma(\tau(x)) = \sigma(x) = x = \tau(x) = x = \tau(\sigma(x)) = \tau\sigma(x).$$

- Suppose that $x \in \{x_1, \cdots, x_s\}$, then $\sigma(x_i) = x_{i \mod s+1}$. However, $\tau(x_i) = x_i$ since σ and τ are disjoint. Therefore

  $$\begin{aligned} \sigma\tau(x_i) &= \sigma(\tau(x_i)) = \sigma(x_i) \\ &= x_{i \mod s+1} = \tau(x_{i \mod s+1}) \\ &= \tau\sigma(x_i). \end{aligned}$$

  Similarly, if $x \in \{y_1, y_2, \cdots, y_t\}$, then σ and τ also commute.

Permutation

Theorem

Every permutation in S_n is expressible as a product of disjoint cycles and the cycles appearing in the product are unique.

- Assume that $X = \{1, 2, \cdots, n\}$. If σ is the identity (1), then obviously $\sigma = (1)(2)\cdots(n)$.

Permutation

Theorem

Every permutation in S_n is expressible as a product of disjoint cycles and the cycles appearing in the product are unique.

- Assume that $X = \{1, 2, \cdots, n\}$. If σ is the identity (1), then obviously $\sigma = (1)(2)\cdots(n)$.
- Assume that $\sigma \in S_n$ and $\sigma \neq (1)$, define $X_1 = \{\sigma(1), \sigma^2(1), \cdots\}$ and $|X_1| < \infty$ since $|X| = n < \infty$.

Permutation

Theorem

Every permutation in S_n is expressible as a product of disjoint cycles and the cycles appearing in the product are unique.

- Assume that $X = \{1, 2, \cdots, n\}$. If σ is the identity (1), then obviously $\sigma = (1)(2)\cdots(n)$.
- Assume that $\sigma \in S_n$ and $\sigma \neq (1)$, define $X_1 = \{\sigma(1), \sigma^2(1), \cdots\}$ and $|X_1| < \infty$ since $|X| = n < \infty$.
- Now let i be the first integer in X that is not in X_1 and define X_2 by $\{\sigma(i), \sigma^2(i), \cdots\}$ and $|X_2| < \infty$. Continuing in this manner, we can define finite disjoint sets $X_3, X_4, \cdots$. Since X is a finite set, we are guaranteed that this process will end, and there will be only a finite number of these sets r.

Permutation

- If σ_i is the cycle defined by

$$\sigma_i(x) = \begin{cases} \sigma(x), & x \in X_i \\ x, & x \notin X_i, \end{cases}$$

then $\sigma = \sigma_1 \sigma_2 \cdots \sigma_r$. Since the sets $X_1, X_2, \cdots, X_r$ are disjoint, the cycles $\sigma_1, \sigma_2, \cdots, \sigma_r$ must also be disjoint.

Permutation

- Uniqueness: Assume that there are two expressions for σ as a product of disjoint cycles, say

$$(x_1 x_2 \cdots)(y_1 y_2 \cdots)\cdots$$

and

$$(a_1 a_2 \cdots)(b_1 b_2 \cdots)\cdots .$$

Permutation

- Uniqueness: Assume that there are two expressions for σ as a product of disjoint cycles, say

$$(x_1 x_2 \cdots)(y_1 y_2 \cdots) \cdots$$

and

$$(a_1 a_2 \cdots)(b_1 b_2 \cdots) \cdots .$$

- By disjoint cycles commute. Thus without loss of generality we can assume that x_1 occurs in the cycle $(a_1 a_2 \cdots)$. Since any element of a cycle can be moved up to the initial position, it can also be assumed that $x_1 = a_1$. Then $x_2 = \sigma(x_1) = \sigma(a_1) = a_2$; similarly $x_3 = a_3$, and so on. The other cycles are dealt with in the same way. Therefore the two expressions for σ are identical.

Permutation

- $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 1 & 5 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 6 & 4 \end{pmatrix},$

Permutation

- $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 1 & 5 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 6 & 4 \end{pmatrix},$
- $\sigma\tau = (1\ 3\ 6)(2\ 4\ 5), \tau\sigma = (1\ 4\ 3)(2\ 5\ 6).$

Permutation

Definition

A permutation with length 2 is called a transposition.

-

Permutation

Definition

A permutation with length 2 is called a transposition.

-

Corollary

Every element of S_n is expressible as a product of transpositions.

-

Permutation

Definition

A permutation with length 2 is called a transposition.

-

Corollary

Every element of S_n is expressible as a product of transpositions.

-
- This is true since

$$(x_1\ x_2\ \cdots x_r) = (x_1\ x_r)(x_1\ x_{r-1})\cdots(x_1\ x_3)(x_1\ x_2).$$

Permutation

Lemma

If the identity is written as the product of transposition, $id = \sigma_1\sigma_2\cdots\sigma_r$ *then* r *is an even number.*

- We will show the conclusion by induction on r. A transposition cannot be the identity (1). Hence, $r > 1$. If $r = 2$, then we have done.

Permutation

Lemma

If the identity is written as the product of transposition, $id = \sigma_1\sigma_2\cdots\sigma_r$ then r is an even number.

- We will show the conclusion by induction on r. A transposition cannot be the identity (1). Hence, $r > 1$. If $r = 2$, then we have done.
- Suppose that $r > 2$. Let $\sigma_{r-1}\sigma_r$ be the last two transpositions, then $\sigma_{r-1}\sigma_r$ must be one of the following cases:

$$\begin{aligned}
(x\ y)(x\ y) &= id,\\
(y\ z)(x\ y) &= (x\ z)(y\ z),\\
(z\ w)(x\ y) &= (x\ y)(z\ w),\\
(x\ z)(x\ y) &= (x\ y)(y\ z),
\end{aligned}$$

where x, y, z, w are distinct.

Permutation

- The first equation simply says that a transposition is its own inverse. If this case occurs, delete $\sigma_{r-1}\sigma_r$ from the product to obtain $id = \sigma_1\sigma_2 \cdots \sigma_{r-2}$. By induction $r - 2$ is even; hence, r must be even.

Permutation

- The first equation simply says that a transposition is its own inverse. If this case occurs, delete $\sigma_{r-1}\sigma_r$ from the product to obtain $id = \sigma_1\sigma_2 \cdots \sigma_{r-2}$. By induction $r - 2$ is even; hence, r must be even.
- In each of the other three cases, we can replace $\sigma_{r-1}\sigma_r$ with the righthand side of the corresponding equation to obtain a new product of r transpositions for the identity. In this new product the last occurrence of x will be in the next-to-the-last transposition.

Permutation

- We can continue this process with $\sigma_{r-2}\sigma_{r-1}$ to obtain either a product of $r-2$ transpositions or a new product of r transpositions where the last occurrence of x is in σ_{r-2}. If the identity is the product of $r-2$ transpositions, then again we are done. Otherwise, we will repeat the procedure with $\sigma_{r-3}\sigma_{r-2}$.

Permutation

- We can continue this process with $\sigma_{r-2}\sigma_{r-1}$ to obtain either a product of $r-2$ transpositions or a new product of r transpositions where the last occurrence of x is in σ_{r-2}. If the identity is the product of $r-2$ transpositions, then again we are done. Otherwise, we will repeat the procedure with $\sigma_{r-3}\sigma_{r-2}$.
- Either we will have two adjacent, identical transpositions canceling each other out or x will be shuffled so that it will appear only in the first transposition. However, the latter case cannot occur, because the identity would not fix x in this instance. Therefore, the identity permutation must be the product of $r-2$ transpositions and, again by our induction hypothesis, we are done.

Permutation

Theorem

If $\sigma = \tau_1\tau_2\cdots\tau_r = \mu_1\mu_2\cdots\mu_s$, where τ_i and μ_j are transpositions for $i = 1, \cdots, m, j = 1, \cdots, s$, then r and s have the same parity.

-

Permutation

Theorem

If $\sigma = \tau_1\tau_2\cdots\tau_r = \mu_1\mu_2\cdots\mu_s$, *where* τ_i *and* μ_j *are transpositions for* $i = 1, \cdots, m, j = 1, \cdots, s$, *then* r *and* s *have the same parity.*

-
- Proof: suppose that $\sigma = \tau_1\tau_2\cdots\tau_r = \mu_1\mu_2\cdots\mu_s$, where r is even. The inverse of $\tau_1\tau_2\cdots\tau_r$ is $\tau_r\tau_{r-1}\cdots\tau_1$. Since

$$id = \sigma\sigma^{-1} = \tau_1\tau_2\cdots\tau_r\tau_r\tau_{r-1}\cdots\tau_1 = \mu_1\mu_2\cdots\mu_s\tau_r\tau_{r-1}\cdots\tau_1.$$

Then $r + s$ is even, s is even.

Permutation

Definition

A permutation is called even permutation if the permutation can be written as even number of transpositions. Similarly, odd permutation is defined the same way.

-

Permutation

Definition

A permutation is called even permutation if the permutation can be written as even number of transpositions. Similarly, odd permutation is defined the same way.

-

Example

In S_3, the even permutations are $(1), (1\ 2\ 3), (1\ 3\ 2)$, while the odd permutations are $(1\ 2), (2\ 3), (1\ 3)$.

-

Permutation

Definition

The alternating group A_n is the set of all even permutations of S_n.

Theorem

The alternating group A_n is a subgroup of S_n. $|A_n| = n!/2$.

-

Permutation

Definition

The alternating group A_n is the set of all even permutations of S_n.

Theorem

The alternating group A_n is a subgroup of S_n. $|A_n| = n!/2$.

-

Permutation

Definition

The alternating group A_n is the set of all even permutations of S_n.

Theorem

The alternating group A_n is a subgroup of S_n. $|A_n| = n!/2$.

-
- Proof: Operation of $A_n \subseteq S_n$ is closed because the product of two even permutations must also be an even permutation. A_n is associative since S_n is associative. Secondly, the identity (1) is an even permutation. Let $\sigma = \sigma_1\sigma_2\cdots\sigma_s$ with s even. Then

$$\sigma^{-1} = (\sigma_1\sigma_2\cdots\sigma_s)^{-1} = \sigma_s^{-1}\sigma_{s-1}^{-1}\cdots\sigma_1^{-1}$$

is an even transpositions.

Dihedral group

Definition

The n-th *dihedral group* is a group of rigid motions of a regular n-gon. We will denote this group by D_n.

Dihedral group

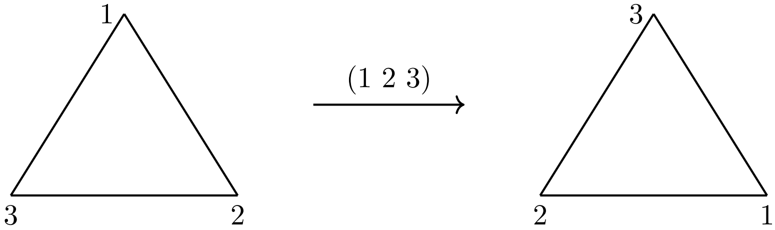
- $$D_3 = \{(1), (2\ 3), (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3)\} \subseteq S_3.$$

  $|S_3| = |D_3| = 6$, that means $D_3 = S_3$.

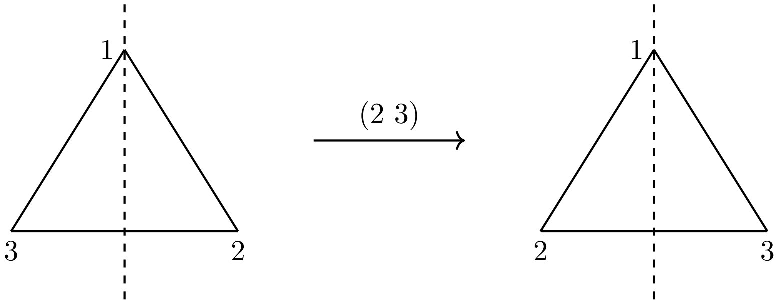
Dihedral group

- $$D_3 = \{(1), (2\ 3), (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3)\} \subseteq S_3.$$

  $|S_3| = |D_3| = 6$, that means $D_3 = S_3$.
- Let $r = (1\ 2\ 3)$, $s = (2\ 3)$,



Dihedral group



Dihedral group

- Let $r = (1\ 2\ 3),\ s = (2\ 3)$, then

$$
\begin{aligned}
r^2 &= (1\ 3\ 2), \\
r^3 &= (1), \\
rs &= (1\ 2\ 3)(2\ 3) = (1\ 2), \\
r^2 s &= (1\ 3\ 2)(2\ 3) = (1\ 3).
\end{aligned}
$$

Dihedral group

- Let $r = (1\ 2\ 3),\ s = (2\ 3)$, then

$$\begin{aligned} r^2 &= (1\ 3\ 2), \\ r^3 &= (1), \\ rs &= (1\ 2\ 3)(2\ 3) = (1\ 2), \\ r^2s &= (1\ 3\ 2)(2\ 3) = (1\ 3). \end{aligned}$$

-

$$\begin{aligned} D_3 &= &< r, s \mid s^2 = id = r^3,\ srs = r^{-1} > \\ & &= \{1, s, r, r^2, rs, r^2s\}. \end{aligned}$$

Dihedral group

- $$\begin{aligned} D_4 &= < r, s \mid s^2 = id = r^4,\ srs = r^{-1} > \\ &= \{1, s, r, r^2, r^3, rs, r^2s, r^3s\}. \end{aligned}$$

Dihedral group

- $$\begin{aligned} D_4 &= < r, s \mid s^2 = id = r^4,\ srs = r^{-1} > \\ &= \{1, s, r, r^2, r^3, rs, r^2s, r^3s\}. \end{aligned}$$

- Let $r = (1\ 2\ 3\ 4),\ s = (1\ 2)(3\ 4)$, then

$$\begin{aligned} r^2 &= (1\ 3)(2\ 4), \\ r^3 &= (1\ 4\ 3\ 2), \\ rs &= (1\ 2\ 3\ 4)(1\ 2)(3\ 4) = (1\ 3), \\ r^2s &= (1\ 3)(2\ 4)(1\ 2)(3\ 4) = (1\ 4)(2\ 3), \\ r^3s &= (1\ 4\ 3\ 2)(1\ 2)(3\ 4) = (2\ 4). \end{aligned}$$

  Thus

$$\begin{aligned} D_4 &= \{(1), (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), \\ &\quad (1\ 2)(3\ 4), (1\ 3), (1\ 4)(2\ 3), (2\ 4)\}. \end{aligned}$$

Definition

Theorem

The dihedral group D_n, is a subgroup of S_n of order $2n$. And

$$D_n = < s, r | s^2 = 1, r^n = 1, srs = r^{-1} > .$$