GroupAction4

2023年2月25日 星期六 下午12:33

transposition

alternating group

subgroup

cyclic group

permutation matrix.

Definition: An $n \times n$ matrix is a permutation matrix if each row and each column contain a single 1 and all other entries are 0.

$n=3$. $P_{(12)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ $(1\,2)$

$P_{(132)} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ $P_{(123)} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ inverse.

$(13)(12) = (132) \Leftrightarrow (12)(13)$

we can associate with $\sigma \in S_n$ a permutation matrix $P_\sigma$ s.t. the 1 entry in row $i$ of $P_\sigma$ is in column $i\sigma$

Proposition: (a) For $\sigma \in S_n$, $P_\sigma$ is indeed a permutation matrix.

(b) $\sigma, \tau \in S_n$. $P_{\sigma\tau} = P_\sigma P_\tau$.

proof: (a) $\sigma$ bijection.

(b). $(P_\sigma P_\tau)_{ij} = \sum_{k=1}^{n} (P_\sigma)_{ik} (P_\tau)_{kj} = \sum_{k=1}^{n} r_{i\sigma k}\, r_{k\tau j} = r_{i\sigma\tau j}$

$= (P_{\sigma\tau})_{ij}$. □

Definition: (i) A transposition is another term for a 2-cycle

(ii) A permutation is said to be odd. if it can be written as a product of an odd number of transpositions. (even)

product of an odd number of transpositions.
even

Lemma: If $\sigma$ is a transposition, then $\det P_\sigma = -1$.

proof: $\sigma = (ij)$

$\det P_\sigma = \det(I_n$ swaps rows $i$ and $j) = -1$

$= -\det(I_n)$ □

Theorem: Every permutation can be written as a product of transpositions.

No permutation is both even and odd.

proof: Theorem: disjoint cycles can be written as a product of transpositions.

$\alpha_1\ \alpha_2 \cdots \alpha_k$

2-cycle → odd permutation.

$(a_1 \cdots a_k) = (a_1 a_2)(a_1 a_3) \cdots (a_1 a_k)$

$\alpha_2\ \alpha_1 \cdots \alpha_k$

$\alpha_3\ \alpha_1\ \alpha_2 \cdots \alpha_k$

$\alpha_4\ \alpha_1\ \alpha_2\ \alpha_3 \cdots \alpha_k \rightarrow \alpha_k\ \alpha_1\ \alpha_2 \cdots \alpha_{k-1}$

$(a_k\ a_1\ a_2 \cdots a_{k-1}) = (a_1 \cdots a_k)$

lemma

$\det P_\sigma = (-1)^k$.

No permutation is both even and odd. □.

a permutation is even if.f. its cycle length has even number of even length cycles.

$S_7$.

7. even (0, even length cycles).

5. (0, even length cycles)

$4+2$ (2 )

$3+3$ (2 )

$3+2+2$ (2 )

3 (0 )

$2+2$ (2 )

e (0 ).

Proposition: (a). The even permutations in $S_n$ form a subgroup $A_n$.

(b) $n \geq 2$, the order of $A_n$ is $\frac{1}{2}n!$ ✓ alternating group

(c). $n \geq 4$. $A_n$ is non-abelian. $(\sigma\tau)\gamma = \sigma(\tau\gamma)$

proof: (a). $\sigma = \rho_1 \rho_2 \cdots \rho_{2k}$

$\tau = \psi_1 \psi_2 \cdots \psi_{2n}$. transposition.

$\sigma\tau = \rho_1 \cdots \rho_{2k} \psi_1 \cdots \psi_{2n} \in A_n$

$2k + 2n = 2(k+n)$

$\sigma^{-1} = \rho_{2k} \cdot \rho_{2k-1} \cdots \rho_1$ ✓ identity: $e \in A_n$.

(b) permutation (12) is odd.

$A_n \to A_n^c$ even → odd $\quad \sigma \to (12)\sigma$ $\qquad A_n^c \to A_n \quad \sigma \mapsto (12)\sigma$

$|A_n| = |A_n^c| = \frac{1}{2}n! \quad |A_n| + |A_n^c| = |S_n| = n!$

(c) $n \geq 4$. (123) (124) non-abelian

1234 (12)(13)(12)(14) ≠ (12)(14)(12)(13) □.

2134 3124 1324 (4321) 2134 4132 1432 (3412)

(123) (132) are not conjugate in $A_4$. $\sigma^{-1}(123)\sigma = (132)$

$(1\sigma\ 2\sigma\ 3\sigma) = (132)$

$1\sigma=1\ 2\sigma=3\ 3\sigma=2\ 4\sigma=4$ $\sigma = (23)$

$1\sigma=2\ 2\sigma=1\ 3\sigma=3\ 4\sigma=4$ $\sigma = (21)$ odd.

$1\sigma=3\ 2\sigma=2\ 3\sigma=1\ 4\sigma=4$ $\sigma = (31)$

(213)

(321)

$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \times \begin{pmatrix}2&3&1\\1&2&3\end{pmatrix}$

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

$A_4$: 6 conjugacy classes.

$\{e\}$. $e \cdot e \cdot e = e$.

$\{(12)(34), (13)(24), (14)(23)\}$.

$\{(123), (134), (214), (324)\}$.

$\{(132), (143), (124), (234)\}$.

$\sigma^{-1}(134)\sigma = (214)$

$(123)^{-1}(134)(123) = (214)$

1234

4132

~~(123)~~

(13)(12)

$123\ (231) = (123) = (312)(13)(14)$

Subgroup: $H \leq G$. $G \leq G$

Subgroup: $H \leq G$. $G \leq G$

A subset $H$ of a group $G$ is a subgroup of $G$ if $H$ is a group in its own elements under the restriction of $G$'s group operation.

proposition: Let $G$ be a group. Then $H \subseteq G$ is a subgroup iff.

subgroup test. $H$ is non-empty and whenever $x.y \in H$, then $x^{-1}y \in H$. △

proof: $\Rightarrow$ $H \leq G$. $e \in H$. $H$ is non-empty.

$x^{-1}y \in H$. $H$ is closed under products and inverses.

$\Leftarrow$ $H \neq \emptyset$. $h \in H$. $x=y=h$. $h^{-1}\cdot h = e \in H$

$x=x$, $y=e$. $x^{-1}\cdot e = x^{-1} \in H$.

$xy = (x^{-1})^{-1} y \in H$

associativity. $xy.z \in G$. $x.y.z. \in H$.

$(xy)\cdot z = x(yz)$. $\frac{1}{2}n! = \frac{6}{2} = 3$ □.

$\begin{matrix}1&2&3\\1&2&3\end{matrix}$ ↓ 1 2 2 2 3 6.

$S_3$: $\{e\}$. $\{e,(12)\}$. $\{e,(13)\}$. $\{e,(23)\}$ $A_3$. $S_3$.

$3!=6$. $(23)(23)=e$

1 2 2 2 2 2

$D_8$. $\{e\}$. $\{e, r^2\}$. $\{e, s\}$. $\{e, rs\}$. $\{e, r^2s\}$. $\{e, r^3s\}$

8 4 4 4 4 8

$\{e, r, r^2, r^3\}$ $\{e, r^2, s, r^2s\}$. $\{e, r^2, rs, r^3s\}$ $D_8$.

$\{e, g^5, g^4, g^3, g^2, g\}$.

$C_6 = \{e, g, g^2, g^3, g^4, g^5\}$. $\{e\}$. $\{e, g^3\}$. $\{e, g^2, g^4\}$. $C_6$.

6 cyclic. $g$. $g^5$. 1 2 3 6

$|H|$ divides $|G|$. Lagrange's Theorem.

Proposition. Let $G$ be a group and $H, K$ be a subgroup of $G$.

$H \cap K$ is a subgroup. $\bigcap_{i \in I} H_i \leq G$.

proof. $e \in H$. $e \in K$. $x.y \in H \cap K$.

$x \in H$ $x^{-1} \in H$ $x^{-1} \in H \cap K$. $\frac{x \in H \quad x \in K}{y \in H \quad y \in K}$ $\frac{xy \in H, K}{xy \in H \cap K}$

proof: $x \in H$ $x^{-1} \in H$ $x^{-1} \in H \cap K$.
$x \in K$ $x^{-1} \in K$

$x \in H$ $x \in K$ $xy \in H, K$
$y \in H$ $y \in K$ $xy \in H \cap K$. □

**Definition:** Let $G$ be a group and $S$ a subset of $G$

i). The subgroup generated by $S$. $\langle S \rangle$ is a smallest subgroup of $G$ which contains $S$. well defined. $H_i$ generated by $S$. $\bigcap_{i \in I} H_i = \langle S \rangle$.

ii) If $g \in G$. then we write $\langle g \rangle$. rather then $\langle \{g\} \rangle$.

iii) If $\langle S \rangle = G$. the elements of $S$ are said to be generators of $G$.

$G = \mathbb{Z}$. $S = \{12, 42\}$ $42 - 3 \times 12 = 6$ $\langle S \rangle = 6\mathbb{Z}$.
$12 - 2 \times 6 = 0$ $\{6, 12, 18 \cdots\}$.

$G = S_4$. $S = \{\underbrace{(123)}_{\sigma \in A_4}, \underbrace{(12)(34)}_{\tau \in A_4}\}$. $\langle S \rangle \subseteq A_4$.

$e$, $\sigma$, $\tau$. $\tau\sigma\tau = (214)$ $(\tau\sigma\tau)^2 = (124)$ $\cdots$ $\langle S \rangle = A_4$.

If. $G$ is abelian, $g, h \in G$. then $\langle g, h \rangle = \{g^r h^s ; r, s \in \mathbb{Z}\}$.

proof: $\{g^r h^s ; h, s \in \mathbb{Z}\} \subseteq \langle g, h \rangle$. $hg = gh$.
subgroup $H$

(i) $g^0 h^0 = e \in H$ identity. Associativity.

(ii) $(g^k h^l)(g^k h^l) = g^{k+k} h^{l+l} \in H$ closed.

(iii) $(g^k h^l)^{-1} = h^{-l} g^{-k} = g^{-k} \cdot g^{-l} \in H$. inverse □

**division algorithm:**

Let $a, b$ be integers. $b > 0$. $\exists$ unique $q, r$. s.t. $a = bq + r$. $0 \le r < b$.

**Proposition:** Let $G$ be a group and $g \in G$. Then.

(a) $\langle g \rangle = \{g^k, k \in \mathbb{Z}\}$.

(b). If order of $g$ ($o(g)$) is finite. then $\langle g \rangle = \{e, g, g^2 \cdots g^{o(g)-1}\}$.

proof: $g^k \in \langle g \rangle$ $H = \{g^k ; k \in \mathbb{Z}\}$. is a subgroup

proof: $g^k \in \langle g \rangle$ $H = \{g^k : k \in \mathbb{Z}\}$ is a subgroup.

$g^0 = e \in H$. $g^k \cdot g^l = g^{k+l}$. $(g^k)^{-1} \cdot g^l = g^{-k} g^l = g^{l-k} \in H$.

$\{e, g, g^2, \dots g^{o(g)-1}\} \subseteq \langle g \rangle$. $k = q\,o(g) + r$. $q, r, k \in \mathbb{Z}$. $0 \le r < o(g)$.

$g^k = g^{q\,o(g)+r} = (g^{o(g)})^q g^r = e^q g^r = g^r \in \{e, g, g^2, \dots g^{o(g)-1}\}$. □

A group $G$ is cyclic if there exists $g \in G$, s.t. $G = \langle g \rangle$. ⇔ $o(g) = |G|$ (A finite group)

abelian. $a = g^k$, $b = g^l$. $g^k \cdot g^l = g^{k+l} = g^l \cdot g^k$. $ab = ba$.

$C_5 = \{e, g, g^2, g^3, g^4\}$. $g, g^2, g^3, g^4$.

$C_2 \times C_3$. $\{e, g\}$. $\{e, h, h^2\}$.

$\{(e,e), (e,h), (e,h^2)$
$(g,e), (g,h), (g,h^2)\}$

$(g,h)$. $(e,h^2)$. $(g,e)$, $(e,h)$, $(g,h^2)$ $(e,e)$.

$(g,h^2)$ $(e,h)$, $(g,e)$ $(e,h^2)$ $(g,h)$ $(e,e)$.

$C_2 \times C_2$. $\{e, g\}$. $\{e, h\}$ is not cyclic.

11. Mar. 2023.
4pm (+8).