L4 def: G.H 为group, $X=G\times H$ i.e. $X=\{(g,h): g\in G, h\in H\}$

运算 $(g,h)(g',h')=(gg',hh')$, then: $G\times H$ is group

$X=G\times H$: direct product / direct sum

def: cyclic group: $G=\langle g\rangle=\{g^{\pm i}: i\in\mathbb{N}\}$ 可以由其中某元素生成 "generator"

例: ① $(\mathbb{Z},+)=\{(\pm i)\cdot 1 \mid i\in\mathbb{N}\}=\{\pm i \mid i\in\mathbb{N}\}$

② $(\mathbb{Z}_p,\oplus)=\{(\pm i)\cdot 1 \mid i\in\mathbb{N}\}=\{\bar{0},\bar{1},\dots,\overline{p-1}\}$ "$\bar{\ }$"指$\oplus$下等价类

$(\pm i)\cdot 1$: "$\pm i$"对1操作$\pm i$次群运算."

def: dihedral group: $G=\{1, a, \dots a^{n-1}, b, ab, \dots a^{n-1}b : |a|=n, |b|=2\}$; $bab^{-1}=a^{-1}$.

⇒group: ① closed: $a^ib^j\in G$, $a^kb^l\in G$, $j,l\in\{1,0\}$, $a^ib^ja^kb^l=b^j\underline{b^{-j}a^ib^j}a^kb^l$ t

$=b^ja^ta^kb^l=b^ja^{t+k}b^l$

$=b^ja^{t}b^{-j}b^jb^l=a^{t}b^{j+l}\in G$

by: $|a|=n$, $|b|=2$ $bab^{-1}=a^{-1}$

②: $a^ib^j=b^jb^{-j}a^ib^j=\underline{b}^ja^{-i}=\underline{b}^{-j}a^{-i}$

$\therefore (a^ib^j)^{-1}=a^ib^j$

③ Identity: 1, asociation ✓

这个群 $G=D_{2n}$ 定义的运算就是一般乘法

def: symmetric group: $\Omega=\{1,2,\dots n\}$ (可以set), 1-1 map from Ω to Ω is permutation

$Sym(\Omega)=\{\forall$ permutations on $\Omega\}$, $|Sym(\Omega)|=n!$

定义运算"·" composition: $g\circ f$", $(Sym(\Omega),\cdot)$ is a group, 记为 S_n

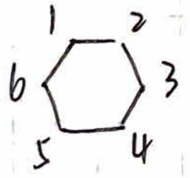
例①中: 1→2 denoted $(124)(3)=(124)$, 一个括号代表一个算子, 首尾闭合

2→4

3→3

4→1

②: 几何意义 D_{2n} & S_n



$a=(1,2\,3\,4\,5\,6)$

$b=(12)(36)(45)$; find ab, bab^{-1}

initial: 1 2 3 4 5 6 ⟩a

2 3 4 5 6 1 ⟩b

1 6 5 4 3 2 ⟩b: exchange 1,2, 3,6, 4,5

ab: 1→1 2→6, 3→5 4→4 5→3 6→2 ⇔ (26)(35)

bab^{-1}: 1→6, 2→1, 3→2, 4→3, 5→4, 6→5 ⇔ (1,6,5,4,3,2)

$b^{-1}=b$

Th CAA P99: the pair of cycles $\alpha=(a_1,a_2,\cdots a_m)$, $\beta=(b_1,b_2,\cdots b_n)$ have no entry in commom, then $\alpha\beta=\beta\alpha$

disjoint + even permutate $\Rightarrow A^2=e$

$\Rightarrow$ disjoint cycles commute.

设 $\alpha\beta$ are permutations of set $S=\{a_1,a_2,\cdots a_m, b_1,\cdots b_n; c_1,\cdots c_k\}$

$(\alpha\beta)(a_i)=\alpha(\beta(a_i))=\alpha(a_i)=a_{i+1}$

$(\beta\alpha)(a_i)=\beta(\alpha(a_i))=\beta(a_{i+1})=a_{i+1}$

similarly $(\beta\alpha)(b_i)=(\alpha\beta)(b_i)$, $\forall b_i$ $(\beta\alpha)(c_i)=(\alpha\beta)(c_i)$ $\forall c_i$

$\Rightarrow$ PKU版 P99 $\therefore (\alpha\beta)(x)=(\beta\alpha)(x)$ $\forall x\in S$

Th CAA P100: the order of a permutation of a finite set (written in disjoint cycle form) is the least common multiple of the lengths of the cycles

例: $|(1432)(56)|=4$

$|(123)(456)(78)|=6$

$|(123)(145)|=|(14532)|=5$ since $(123)(145)$ $\overset{\text{cycle}}{}$ $(123\overset{\text{set}}{}45)$

$=(145123)(12345)$

易知 cycle length $=N$, 这个 cycle 阶为 N

suppose α length m, β length n, $\alpha\beta$ disjoint cycles; $k=\mathrm{lcm}(m,n)$

$\alpha^k=(\alpha^m)^{k/m}=e^{k/m}=e$; $\beta^k=e$ $\quad$ t: 阶定义为 $=e$ 的最小…

since $\alpha\beta$ commute, $(\alpha\beta)^k=\alpha^k\beta^k=e \Rightarrow |\alpha\beta|\,|\,k \cdots ①$

$(\alpha\beta)^t=\alpha^t\beta^t=e$ $\therefore \alpha^t=\beta^{-t}$ ~~$=\beta^t$~~ $()^{-1}$仅适用于2-cycle

α,β disjoint $\therefore \alpha^t,\beta^t$ disjoint $\}$ equal & disjoint $\Rightarrow$ identi…

$\therefore \alpha^t=\beta^t=e$; $m|t$ and $n|t \Rightarrow k|t \cdots ②$

①+② $k=t$, $|\alpha\beta|=\mathrm{lcm}(m,n)$

(2) Th CAA P102, $\forall$ permutation in S_n $n>1$, is a product of 2-cycles

(1) Th CAA P98 ……… finite set Ω, can be written as a cycle or a product of disjoint cycles

let $\Omega=\{1,2,\cdots n\}$

to write α in disjoint cycle form, start by choosing any $a_1\in\Omega$

$a_2=\alpha(a_1)$, $a_3=\alpha(a_2)=\alpha^2(a_1)$ …… $a_1=\alpha^m(a_1)$

m exists since S_n finite

then $\alpha=(a_1,a_2,\cdots a_{m-1})\cdots$ $\quad$ $(a_1,a_{m-1})(a_1,a_{m-2})\cdots(a_1,a_3)(a_1,a_2)$

choose any $b_1\in\Omega$, 重复上述过程 $\alpha=(a_1,a_2,\cdots a_{m-1})(b_1,b_2,\cdots b_{m-1})\cdots$

$b_1\neq a_i$ $\quad$ $\alpha(b_i)\neq a_j$ since α invertible, $b_i\neq\alpha^{-1}(a_j)=a_{j-1}$

th: A&C 10.3 identity permutation $e = \beta_1\beta_2\cdots\beta_r$, β_i are 2-cycles; r is even

$r \neq 1$, since $e \neq (a,b)$ for any a,b

if $r=2$, e can be $(a,b)(b,a)$, r can be 2

for $r>2$: $\beta_{r-1}\beta_r$ may have the form
$$\begin{cases} (ab)(ab) = e \\ (ab)(bc) = (ac)(ab) = (bc)(ac) \\ (ac)(cb) = (bc)(ab) \\ (ab)(cd) = (cd)(ab) \end{cases}$$

若为第一种, $e = \beta_1\beta_2\cdots\beta_{r-2}$

or: $\beta_{r-1}\beta_r$ 为"="右侧的情况 fix a, 将其变化为"="左侧情况 $\beta_{r-1}'\beta_r'$

Still focus on "a", consider $\beta_{r-2}\beta_{r-1}'$; if $\beta_{r-2}\beta_{r-1}' \neq e$ then $\beta_{r-3}\beta_{r-2}'\cdots$

若 $\beta_i\beta_{i+1}' \neq e$ $\forall i=1,2,\ldots$, finally obtain "$\beta_1'\beta_2'\cdots\beta_r$", a只在$\beta_1'$中出现

⇒矛盾, ∴必有 $\beta_i\beta_{i+1}' = e$, some i

"可能动过也可能没

即由 $e = \beta_1\beta_2\cdots\beta_r$ 可以得到 $e = \beta_1\beta_2'\beta_3'\cdots\beta_{r-2}'$

induction: e = product of r cycles = product of (r-2) another 2-cycles...

∴ r is even since r=2可行 r=1不可行

coro ⇒ 任意 permutation 可以写成多个 cycles 的积,

cycle的个数无数种, 但奇偶性 fixed

then: define even, odd permutation

even permutations form subgroup of S_n, odd ones not

⇓

记为 A_n, group of even permutations of n symbol, n阶交换群

右侧: $\pi: G \to G/H$

$$\begin{cases} H \le M_1,\ H \le M_2\quad M_1 \neq M_2 \Rightarrow M_1/H \neq M_2/H \quad \text{inj} \\ N \le G/H.\ \pi^{-1}(N) \text{是含H的子群} \quad \text{sur.} \end{cases}$$

如 A为B的max normal ← 如Abel group $\mathbb{Z}/6\mathbb{Z}$ $|\{0\}|=1$ 和 $|\{\mathbb{Z}/6\mathbb{Z}\}|=6$

B/A仅有2个normal

A和B/A，∴A和B/A均为B/A max normal ② max ⊲ 子群的order不一定相等

限制性单子的bij证明 π | G中含H的子群 ③

Th: P141书及P17，G is group，$H \lhd G$；则在典范同态 $\left\{\begin{array}{l}\pi: G \to G/H \\ a \to aH\end{array}\right.$ 下，有：

(1)：G中包含H的子群与G/H的子群一一对应

(2)：在π下：正规子群对应正规子群，即 $H \subseteq K \lhd G$，K对应G/H中的正规子群 K/H正规

(3)：设 $K \lhd G$，$K \supseteq H$，则：$G/K \cong (G/H)/(K/H)$

injective: $x_1 \neq x_2 \to y_1 \neq y_2$

(1)：设M_1, M_2为G含H的子群，$M_1 \neq M_2$；

即 $\exists a \in M_1, a \notin M_2$，∴ $aH \notin M_2/H$

（否则 $\exists b \in M_2$，$aH = bH$，$a = bh_2h_1^{-1} = bh \in M_2$）

∴ 若 $M_1 \neq M_2$，then $M_1/H \neq M_2/H$，π injective in subgroup containing H ①

$G/H = \{gH : g \in G\}$，对于任一G/H的子群N，$\pi^{-1}(N)$为G中含H的子群，

since: $H = \pi^{-1}(e \text{ in } G/H) \in \pi^{-1}(N)$

且 $\forall a, b \in \pi^{-1}(N)$，$ab^{-1} \in \pi^{-1}(N)$，$ba^{-1} \in \pi^{-1}(N)$

∴ $\pi^{-1}(N)$是一个含H的子群，$\forall N$，π surjective in subgroup containing H ②

①+② 在…，π bijective 要说明preimage在限制范围中

(2) 若 $H \subseteq K \lhd G$，$\forall gH \in G/H$，$kH \in K/H$：

$(gH)^{-1} kH (gH) = g^{-1}H \cdot kH \cdot gH = (g^{-1}kg)H = k'H \in K/H$ since $K \lhd G$

∴ $K \lhd G$，$\pi(K) \lhd \pi(G)$；

$gH \to gK$ $H \subseteq K \subseteq G$，∴ "一一对应"关系成立

(3)：$\varphi: G/H \to G/K$，$\ker\varphi = K/H$ $\operatorname{im}\varphi = G/K$

$(G/H)/\ker\varphi \cong \operatorname{im}\varphi \Rightarrow (G/H)/(K/H) \cong G/K$ im

构造bijective

（以上可以改写成：）$\varphi: G \to G_1$ 是群的满同态，则 （G_1: G/H）

(1)' G中包含kerφ的子群与G_1的子群一一对应

(2)' 此对应下，……，(3)' $K \lhd G$，$K \supseteq \ker\varphi$，$G/K \cong (G/\ker\varphi)/(K/\ker\varphi)$

$\cong G_1/\varphi(K)$

*: 并不是说 $G_1 = G/\ker$

~~$H \lhd G$ $K \lhd G$~~ $G/K \cong \frac{G/H}{K/H}$ $H \subseteq K$