$G=(\mathbb{Z},+)$

$n\in\mathbb{Z}^+$, $H=\{ng\mid g\in\mathbb{Z}\}$

$a\sim b\Leftrightarrow a\equiv b\pmod n$

$T=\{0,1,\cdots,n-1\}$

$a\circledast b=(a+b)\%n$

G $H\leq G$

$H\lhd G$

G, $H\lhd G$. 在G上定义等价关系$\sim$. $a\sim b\Leftrightarrow a^{-1}b\in H\Leftrightarrow \exists h\in H$, s.t. $b=ah$

取定$T\subseteq G$, 满足:

(i) $\forall g\in G$, $\exists a\in T$ s.t. $a\sim g$

(ii) $\forall a,b\in T$, $a\sim b\Rightarrow a=b$.

在T上定义二元运算$\circledast$. $\forall a,b\in T$, $a\circledast b\in T$, 且$a\circledast b\sim ab$ (由(i)(ii)知这样的$a\circledast b$存在且唯一)

$(T,\circledast)$是群

$f:G\to T$

$\forall g\in G$: $f(g)\in T$, 且$f(g)\sim g$

f是G到T的同态, 并且$\ker(f)=H$

G, $H\lhd G$, $A,B\subseteq G$, $AB=\{ab\mid a\in A, b\in B\}\subseteq G$ // 子集继承运算

对$a\in G$, $\{a\}B=aB=\{ab\mid b\in B\}$ $a=1_G$, $1_GB=B=B1_G$

$aH=\{ah\mid h\in H\}$ $G/H=\{aH\mid a\in G\}$ //左陪集的集合

命题. 设G是群, $H\lhd G$, 则$(G/H,\cdot)$也成群, 其中二元运算"$\cdot$"是G的子集之间的乘法, 并且:

(1) $\forall a,b\in G$, $(aH)(bH)=(ab)H$

(2) H是幺元, 即$\forall a\in H$, $H(aH)=(aH)H=aH$

(3) $\forall a\in G$, $a^{-1}H$和aH互为逆元, 即$(aH)(a^{-1}H)=(a^{-1}H)(aH)=H$.

(4) 定义$\pi_H: G\to G/H$ $\forall a\in G$, $\pi_H(a)=aH$

则π_H是G到G/H的同态, $\ker(\pi_H)=H$, $\mathrm{ran}(\pi_H)=G/H$.

range 满射 由def, 左陪集集合

G $H \leq G$

$H \lhd G$ $(\forall g \in G, a \in H: gag^{-1} \in H)$

事实 1. $H \leq G$, 则 $HH = H$

2. $H \lhd G$, 则 $\forall a \in G$, 有 $aH = Ha$ (充要条件: 有性质 $\Rightarrow H \lhd G$)

$\forall A \subseteq G$, 有 $AH = HA$

1. $HH = \{ab \mid a \in H, b \in H\} \subseteq H$

$1_e \in H$, $H = \{1_e h \mid h \in H\} \subseteq HH$

2. aH $\forall h \in H$, $ah = (aha^{-1})a$ $H \lhd G$. $h \in H$

$aha^{-1} \in H$ $\therefore (aha^{-1})a \in Ha$, 即 $ah \in Ha$.

Ha $\forall h \in H$. $ha = a(a^{-1}ha)$ $\because H \lhd G$, $h \in H$

$\therefore a^{-1}ha \in H$ $\therefore a(a^{-1}ha) \in aH$, 即 $ha \in aH$.

$\therefore aH \subseteq Ha$. $Ha \subseteq aH$

$\therefore aH = Ha$

$(AB)C = A(BC)$ 推冲结合律

左 $= \{(ab)c \mid a \in A, b \in B, c \in C\}$

右 $= \{a(bc) \mid a \in A, b \in B, c \in C\}$

命题的证明

(1) $(aH)(bH) = a(Hb)H = a(bH)H = (ab)(HH) = (ab)H$

(2) $HaH = aHH = aH$

(3) $(aH)(a^{-1}H) = (aa^{-1})H = 1_e H = H$

$(a^{-1}H)(aH) = (a^{-1}a)H = 1_e H = H$.

(4) $\forall a, b \in G$, 要证 $\pi_H(ab) = \pi_H(a)\pi_H(b)$

$\pi_H(ab) = (ab)H = (aH)(bH) = \pi_H(a)\pi_H(b)$.

$\forall a \in G$. $a \in \ker(\pi_H) \Leftrightarrow \pi_H(a) = H$

$\Leftrightarrow aH = H \Leftrightarrow a \in H$.

G, L 群. $f: G \to L$ 同态

若 f 还是双射，则称 f 是群同构，

记作 $G \xrightarrow{f} L$.

eg. $\mathbb{R}^4 \to M_{2\times 2}(\mathbb{R})$

$(a,b,c,d) \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

G, L 是群

$f: G \to L$ 是同态，若 $\forall a,b \in G.\ f(ab) = f(a)f(b)$

$\ker(f) = \{a \mid a \in G,\ f(a) = |_L\}$ $\ker(f) \lhd G$ //证过的

同态定理. 设 G, L 是群，$f: G \to L$ 同态，$H = \ker(f)$，则：

(1) $\forall a,b \in G.\ aH = bH \Leftrightarrow f(a) = f(b)$

(2) 如下定义 $\varphi: G/H \to L$.

$\forall a \in G.\ \varphi(aH) = f(a)$

则 φ 是同态，φ 是单射，$\mathrm{ran}(\varphi) = \mathrm{ran}(f)$

因此 φ 是 G/H 到 $\mathrm{ran}(f)$ 的群同构，即 $G/H \overset{\varphi}{\cong} \mathrm{ran}(f)$

$G \cong L$ 是指 $\exists f: G \to L$ 是群同构

$f: G \to L$ 的群同态，则

(1) 设 $A \leq G$，则 $f[A] = \{f(a) \mid a \in A\} \leq L$

(2) 设 $B \leq L$，则 $f^{-1}[B] = \{a \mid a \in G,\ f(a) \in B\} \leq G$

Ⓚ 思考：像集是群？

证：(1) $\Rightarrow$ $\because aH = bH$ $\exists h \in H$ s.t. $b = ah$

注意到 $h \in \ker(f)$ $\therefore f(h) = |_L$.

$f(b) = f(ah) = f(a)f(h) = f(a)|_L = f(a)$

$\Leftarrow$ $\because f(a) = f(b)$

$\therefore |_L = f(a)^{-1}f(a) = f(a)^{-1}f(b) = f(a^{-1})f(b) = f(a^{-1}b)$

$\therefore f(a^{-1}b) = |_L$, $a^{-1}b \in H$ //3.18 课证明：$a^{-1}b \in H \Leftrightarrow b \in aH \Leftrightarrow b = ah$ $\exists h \in H$.

$\therefore aH = bH$ ($b = a(a^{-1}b) \in aH$) (下节) $\Leftrightarrow aH = bH$.

(2) φ 映射合理，同态，单射，像集

先说明 φ 是合理定义的，即若 $a,b \in G$，并且 $aH = bH$，则 $f(a) = f(b)$，由(1)保证 ✓

φ 是同态 $\forall a,b \in G$，要说 $\varphi((aH)(bH)) = \varphi(aH)\varphi(bH)$

$b = b|_H$

$b \in bH$ $b \in aH$.

$\exists h,\ b = ah$

左 $= \varphi((ab)H) = f(ab)$

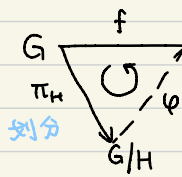
右 $= f(a)f(b) = f(ab) =$ 左

φ 是单射，$\forall a,b \in G$. $\varphi(aH) = \varphi(bH)$，要说 $aH = bH$，

$\because \varphi(aH) = f(a)$，$\varphi(bH) = f(b)$，$f(a) = f(b)$ $aH = bH$ (由(1))。

$\mathrm{ran}(\varphi) = \mathrm{ran}(f)$ (显然) #

$\pi_H(a) = aH$



$\varphi \circ \pi_H = f$

$(\mathbb{Z}, +)$ $n \in \mathbb{Z}^+$

$f: \mathbb{Z} \to \{0,1,\cdots,n-1\}$ $\forall a \in \mathbb{Z}$, $f(a) = a\%n$

f 是 $(\mathbb{Z},+)$ 到 $(\{0,1,\cdots,n-1\}, \oplus)$ 的同态。 模 n 加

$\mathrm{ran}(f) = \{0,1,\cdots,n-1\}$ 满射 待验

$H = \ker(f) = \{a \mid a \in \mathbb{Z},\ f(a) = \bar{0}\} = \{a \mid a \in \mathbb{Z},\ a\%n = 0\} = \{qn \mid q \in \mathbb{Z}\}$

$G/H \cong \{0,1,\cdots,n-1\}$. $\varphi(a+H) = a\%n$

G 是有限循环群，$|G| = n$.

$\exists g \in G$, s.t. $G = \langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}$

$\therefore g$ 的阶为 n ($o(g) = n$)，即：$g^n = |_G$ 且 $\forall i \in \{1,\cdots,n-1\}$, $g^i \neq |_G$.

$G = \{g^i \mid i \in \{0,1,\cdots,n-1\}\}$

(1) 设 $d \in \mathbb{Z}^+$, $d \mid n$. $H = \langle g^d \rangle$. 则 $H \leq G$. $|H| = \frac{n}{d}$. 并且 $H = \{y \mid y \in G,\ y^{\frac{n}{d}} = |_G\}$

(2) 设 $H \leq G$. 则 $\exists d \in \mathbb{Z}^+$, $d \mid n$. s.t. $H = \langle g^d \rangle$.

(2) 记 $I = \{i \mid i \in \mathbb{Z},\ g^i \in H\}$ 则 I 是 $(\mathbb{Z},+)$ 的子群，并且 $n \in I$.

于是 $\exists d \in \mathbb{Z}^+$, s.t. $I = \{qd \mid q \in \mathbb{Z}\}$，则由 $n \in I$ 知 $d \mid n$，并且 $H = \langle g^d \rangle$.

G, $H \leq G$

定义 G 上等价关系 $\sim$ $\forall a,b \in G$, $a \sim b \Leftrightarrow a^{-1}b \in H \Leftrightarrow \exists h \in H$, s.t. $b = ah$

(1) $(G, \sim)$ 是等价关系

(2) 对 $a \in G$, $\{b \mid b \in G, a \sim b\} = \{ah \mid h \in H\} = aH$

(3) $a \sim b \Rightarrow (\forall g \in G, ga \sim gb)$

或: $\forall a \in G$, $aH = \{ah \mid h \in H\}$ ($\because 1_G \in H$, $\therefore a = a1_G \in aH$)

(不考) 对 $a,b \in G$, 下面几个说法等价 (def)

(1) $a^{-1}b \in H$

(2) $b \in aH$

(3) $\exists h \in H$, s.t. $b = ah$

$b \in aH \Leftrightarrow \exists h \in H$, s.t. $b = ah$

由def $\Leftrightarrow \exists h \in H$, s.t. $a^{-1}b = h \Leftrightarrow a^{-1}b \in H$

(1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3)

(4) $aH \cap bH \neq \phi$

(5) $aH = bH$ (最强)

(2) $\Rightarrow$ (4) 由(2), $b \in aH$, $b \in bH$. ($\because 1_G \in H$, $b = b1_G \in bH$) $\therefore aH \cap bH \neq \phi$

(4) $\Rightarrow$ (2) 取 $x \in aH \cap bH$ $\because x \in aH$ $\therefore \exists h_1 \in H$, s.t. $x = ah_1$

$\because x \in bH$ $\therefore \exists h_2 \in H$, s.t. $x = bh_2$

$ah_1 = bh_2$ $ah_1h_2^{-1} = b$ // (4) $\Rightarrow$ (3)

$\because H \leq G$, $h_1, h_2 \in H$ $\therefore h_1h_2^{-1} \in H$. $\therefore b \in aH$

(5) $\Rightarrow$ (4) 显然

(3) $\Rightarrow$ (5) 设 $b = ah$, $h \in H$

$bH \subseteq aH$. $\forall x \in H$, $bx = ahx = a(hx)$ $\because H \leq G$, $h, x \in H$ $\therefore hx \in H$.

$\therefore bx = a(hx) \in aH$. $\therefore bH \subseteq aH$.

$aH \subseteq bH$. $b = ah \Rightarrow a = bh^{-1}$ $h \in H \Rightarrow h^{-1} \in H$

$\forall x \in H$ $ax = bh^{-1}x$. $h^{-1}x \in H$ $ax = b(h^{-1}x) \in bH$. $\therefore aH \subseteq bH$.

上次讲过 ←

子群：相象，用其他量对应子群

$\mathbb{R}^3$ 子空间：取一组基，矩阵刻画

设 G 是循环群，$|G|=n$. $G=\langle a\rangle$，则

(1) 设 $d\in\mathbb{Z}^+$，$d\mid n$，$H=\langle a^d\rangle$，则 $H\leq G$，$|H|=\frac{n}{d}$，并且 $H=\{y\mid y\in G, y^{\frac{n}{d}}=|_G\}$.

(2) 设 $H\leq G$，则 $\exists d\in\mathbb{Z}^+$，$d\mid n$. s.t. $H=\langle a^d\rangle$.

$\{H\mid H\leq G\}\leftrightarrow\{d\mid d\in\mathbb{Z}, d\mid n\}$

$\langle a^d\rangle\leftrightarrow d$　　循环群刻画：简单

eg. $n=6$. $\langle a\rangle$, $\langle a^2\rangle$, $\langle a^3\rangle$, $\langle a^6\rangle=\{|_G\}$

回忆：所. $a\in G$ $\begin{cases}\forall m\in\mathbb{Z}^+, a^m\neq|_G, o(a)=+\infty\\ \exists m_0\in\mathbb{Z}^+, \text{s.t. } a^{m_0}=|_G\end{cases}$

令 $n=\min\{m\mid m\in\mathbb{Z}^+, a^m=|_G\}$，记 $o(a)=n$.

$a^i=|_G\Leftrightarrow n\mid i$　　$a^i=a^j\Leftrightarrow i\equiv j\pmod n$

$\langle a\rangle=\{a^i\mid i\in\{0,1,\cdots,n-1\}\}$　　$|\langle a\rangle|=n=o(a)$

(1) $o(a)=n$. 断言 $o(a^d)=\frac{n}{d}$

$(a^d)^{\frac{n}{d}}=a^n=|_G$

$\forall i\in\mathbb{Z}$, $(a^d)^i=|_G\Leftrightarrow a^{di}=|_G\Leftrightarrow n\mid di\Leftrightarrow\frac{n}{d}\mid i$. //所以 $\frac{n}{d}$ 是最小的让 $(a^d)^i=|_G$ 的

$\therefore|\langle a^d\rangle|=o(a^d)=\frac{n}{d}$.

$\forall h\in H$, $h\in\langle a^d\rangle$. $\therefore\exists i\in\mathbb{Z}$, s.t. $h=(a^d)^i$　　$h=a^{di}$

$h^{\frac{n}{d}}=(a^{di})^{\frac{n}{d}}=a^{ni}=|_G$ ($\because a^n=|_G$)

$\forall y\in G$, s.t. $y^{\frac{n}{d}}=|_G$

$\because y\in\langle a\rangle$ $\therefore\exists j\in\mathbb{Z}$, s.t. $y=a^j$.　　$|_G=y^{\frac{n}{d}}=(a^j)^{\frac{n}{d}}=a^{\frac{jn}{d}}$.

$\because o(a)=n$　　$\therefore n\mid j\cdot\frac{n}{d}$　　$\therefore d\mid j$.　　$y=a^j$, $H=\langle a^d\rangle$, $y=(a^d)^{\frac{j}{d}}\in H$.

思考

设 $o(a)=n$. 若 $d\in\mathbb{Z}^+$, $d\mid n$，则 $o(a^d)=\frac{n}{d}$.

一般地，对 $k\in\mathbb{Z}^+$，$o(a^k)=\frac{n}{\gcd(k,n)}$

$\langle a^k\rangle=\langle a^{\gcd(k,n)}\rangle$

↳ n 的因子，回到 $d\mid n$ 的情况

$o(a)=6$. $a^6=|_G$.

$\langle a^4\rangle=\{a^4, a^2, |_G\}$　　$o(a^4)=\frac{6}{\gcd(4,6)}=\frac{6}{2}=3$.

双射也称为置换

设X是集合.

$Sym(X)=\{\sigma \mid \sigma: X\to X \text{ 是双射}\}$ $(Sym(X),\circ)$ 是群

映射的复合(关系复合的特殊情况) $(g\circ f)(x)=g(f(x))$

幺元: $|_X$ (X到自身的恒等映射, $|_X(a)=a, \forall a\in X$)

逆元: $\sigma\in Sym(X)$, σ^{-1} 是 σ 的逆映射, $\sigma^{-1}\in Sym(X)$

$\sigma\circ\sigma^{-1}=\sigma^{-1}\circ\sigma=|_X$ (=元关系的逆关系,特殊) $\sigma(a)=b \leftrightarrow \sigma^{-1}(b)=a$

↘ X上的对称群

$Sym(X)$的子群称为X上的置换群 // 可以 $\sigma(x)$ 在群元素上操作,比抽象群好

$H\le Sym(X)$ $(|_X\in H,\ \forall\sigma_1,\sigma_2\in H,\ \sigma_1\circ\sigma_2\in H,\ \sigma_1^{-1}\in H)$

G群, $Sym(G)$

$\forall a\in G$, 定义 $L_a\in Sym(G)$

$\forall b\in G, L_a(b)=ab$ (左乘) // 单射: $ab=ac$, 则 $b=c$. 群内元素有消去律

$f: G\to Sym(G)$ $L_a(a^{-1}b)=b$, $\forall b\in G$, 在L_a像集

$f(a)=L_a$ $(f(ab)=L_{ab}=L_a\circ L_b)$ f单同态(同态,且单射)

n=3 {1,2,3} 3!=6

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

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

$X=\{1,2,\cdots,n\}$, $n\in\mathbb{Z}^+$, $Sym(X)=S_n$.

$|S_n|=n!=n\times(n-1)\times\cdots\times 1$

$\begin{pmatrix}1&2&3&\cdots&n\\a_1&a_2&a_3&\cdots&a_n\end{pmatrix}$ $(\sigma(i)=a_i,\ \forall 1\le i\le n)$ $\begin{pmatrix}1&2&3&\cdots&n\\\sigma(1)&\sigma(2)&\cdots&&\sigma(n)\end{pmatrix}$

? 答辰 ?

$\left|\{\sigma \mid \sigma(i)\neq i,\ \forall 1\le i\le n\}\right|=C_n$

$\frac{C_n}{n!}=\sum_{i=0}^{n}\frac{(-1)^i}{i!}=\frac{1}{2!}-\frac{1}{3!}+\frac{1}{4!}-\cdots+\frac{(-1)^n}{n!}\approx\frac{1}{e}$ $(n\to+\infty)$

// 在 $Sym(G)$ 中 任选一个, 落在 的概率 $\approx\frac{1}{e}$

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

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

(1 2 3) (1 3 2) (1,3)

$Sym(X)$

对换$(i\ j)$ 对$i\in X, j\in X, i\neq j$

$\sigma(i)=j,\ \sigma(j)=i,\ \sigma(l)=l,\ \forall l\neq i,j$

三轮换$(i\ j\ k)$ 对$i,j,k\in X$ 两两不同. $\sigma(i)=j,\ \sigma(j)=k,\ \sigma(k)=i,\ \sigma(l)=l,\ \forall l\neq i,j,k$

一般的轮换 // 可通过对换乘积(复合)得到

$m\in\mathbb{Z}^+,\ a_1,a_2,\cdots,a_m$ 两两不同.

$(a_1\ a_2\ \cdots\ a_m)$

$\sigma(a_1)=a_2\quad \sigma(a_2)=a_3\ \cdots\ \sigma(a_{m-1})=a_m\quad \sigma(a_m)=a_1\quad \sigma(l)=l,\ \forall l\in\{a_1\cdots a_m\}$

Basic Algebra ←

1 Determine $\alpha\beta$, $\beta\alpha$ and α^{-1} in S_5 if

$$\alpha=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix},\qquad \beta=\begin{pmatrix}1&2&3&4&5\\1&3&4&5&2\end{pmatrix}$$

从右到左,从里到外

$\alpha\circ\beta=\begin{pmatrix}1&2&3&4&5\\2&1&5&4&3\end{pmatrix}$ $\beta\circ\alpha=\begin{pmatrix}1&2&3&4&5\\3&4&1&2&5\end{pmatrix}$ // 无交换律

$(\alpha\circ\beta(1)=\alpha(\beta(1))=\alpha(1)=2,\cdots)$

$\alpha^{-1}=\begin{pmatrix}1&2&3&4&5\\3&1&2&5&4\end{pmatrix}$