$O_n=\{A\in M_n(R)\mid AA^T=I_n\}$ 正交群

$GL_n(R)=\{A\in M_n(R)\mid |A|\neq 0\}$ 一般线性群

$SL_n(R)=\{A\in GL_n(R)\mid |A|=1\}$ 特殊线性群

$\mathcal{M}_n$ 为变换

$m: R\to R,\ m\in \mathcal{M}_n$.

TFAE:
(等价)

1. m 为刚体. 且 $m(0)=0$.
2. $\forall x,y\in R^n$. $(m(x),m(y))=(x,y)$
3. $m=Ax$. A 为正交阵.

Proof: $1\to 2$. $|m(x)-m(y)|^2=|x-y|^2$

$\Rightarrow (m(x)-m(y),\ m(x)-m(y))=(x-y,\ x-y)$

$\Rightarrow$ (又 $(m(x),m(x))=(x,x)$, $(m(y),m(y))=(y,y)$

$\therefore (m(x),m(y))=(x,y)$ （$\because m(0)=0$. $\therefore |m(x)-m(0)|=|x-0|$）

$2\to 3$. $m(x)=Ax,\ m(y)=Ay$

$\therefore (m(x),m(y))=y^TA^TAx=(x,y)=y^Tx$

取 $x,y=e_1,e_2\cdots e_n\Rightarrow A^TA=I\Rightarrow A$ 为正交阵

$3\to 1$. $m(0)=0$ 显然

下证 m 为刚体.

此时 $|m(x)-m(y)|^2=|m(x)|^2+|m(y)|^2-2(m(x),m(y))$

$=x^TA^TAx+y^TA^TAy-2x^TA^TAy$

$=x^Tx+y^Ty-2x^Ty=|x-y|^2$

$\therefore$ TFAE ∎

引理: 若2成立. 且 $m(e_i)=e_i$. 则 $m=I$.

Proof: $m(e_i)=e_i$. 设 m 对应 $A=\begin{pmatrix}a_{11}&&\times\\&\ddots&\\\times&&a_{nn}\end{pmatrix}$

此时 $\forall x\in R^n\Rightarrow m(x)=x$ 即 $m=I$

刚体:

Def 1: $m: R^n\to R^n$ 变换

$\forall x,y\in R^n$ $|m(x)-m(y)|=|x-y|$

称 m 为刚体运动

Def 2: $(f\circ g)(\alpha)=f[g(\alpha)]$ 则 "$\circ$" 为复合.

$\circ: \mathcal{M}_n\times\mathcal{M}_n\longrightarrow\mathcal{M}_n$

$(f,g)\longmapsto fg$

则 f,g 是刚体下, $f\circ g$ 也为刚体: $|f\circ g(\alpha)-f\circ g(\beta)|$

$=|g(\alpha)-g(\beta)|=|\alpha-\beta|\Rightarrow$ 刚体.

即:

$\Rightarrow$ 刚体运动的复合为刚体运动.

性质 不动: 记为 I. 则 $I\circ f=f=f\circ I$.

逆 仍为刚体运动. $|f^{-1}(\alpha)-f^{-1}(\beta)|=|f(f^{-1}(\alpha))-f(f^{-1}(\beta))|=|\alpha-\beta|$

$(f\circ g)\circ h=f\circ(g\circ h)$

Def 3: $(\mathcal{M}_n,\circ)$ 为运动群

Def 4.

平移: $b=(b_1,\cdots,b_n)^T\in R^n$. $t_b(x)=(x_1+b_1,\cdots,x_n+b_n)$. 则 t_b 为平移

(显然平移为刚体)

Proof: $\forall$ 刚体 m, $m=Ax+b$. A 为正交阵. (记 $m(0)=b$)

$\therefore t_{-b}\circ m(0)=t_{-b}(b)=0$.

$\therefore t_{-b}\circ m(x)=Ax$. A 为正交阵

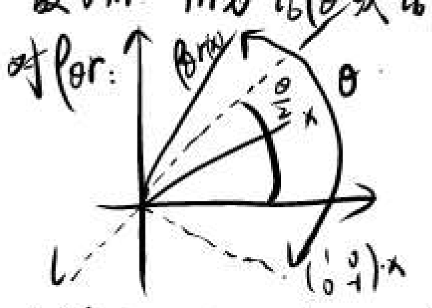
$\therefore m(x)-b=Ax$ $\therefore m(x)=Ax+b$

对正交阵 A: $|A|=1$ $A\to\begin{pmatrix}\cos\theta&-\sin\theta\\\sin\theta&\cos\theta\end{pmatrix}$ 旋转. $\rho_\theta(x)=Ax$

$|A|=-1$ $A\to\begin{pmatrix}\cos\theta&-\sin\theta\\\sin\theta&\cos\theta\end{pmatrix}\begin{pmatrix}1&0\\0&-1\end{pmatrix}$ 镜射 $\to$ 先以x轴反射再 ρ_θ. 称为 $\rho_\theta r$.

故 $\forall m$. m 为 $t_b\rho_\theta$ 或 $t_b\rho_\theta r$. m 为刚体.

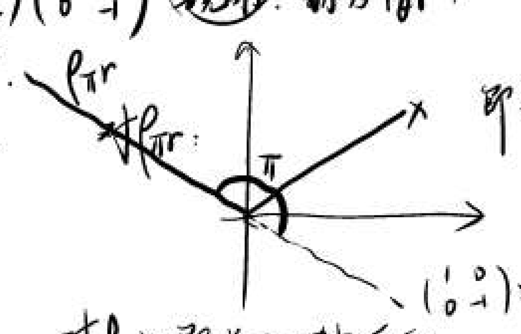
对 $\rho_\theta r$:



即关于 l 反射.
$\tan\frac{\theta}{2}$

$\rho_\pi r$

对 $\rho_\pi r$:



即关于y轴反射

对 $\rho_0 r$ 即关于x轴反射.

性质: $t_a+t_b=t_{a+b}$ $\rho_\theta\rho_\eta=\rho_{\theta+\eta}$

$\rho_\theta t_a=t_{a'}\rho_\theta$ $(a'=\rho_\theta(a))$

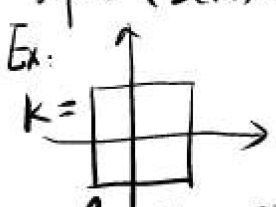
Def5:

对称群. K 为图形 $\subseteq R^2$

$S(K)=\{m\in\mathcal{M}_n\mid m(K)=K\}$

则称 $(S(K),\circ)$ 为 K 的对称群.

Ex:

$K=$ 

$m(x)=t_a\rho_\theta(x)$ or $t_a\rho_\theta r(x)$

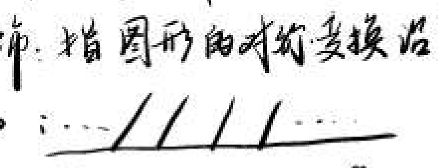
此时 $a=0$.

$\therefore m(x)=\rho_\theta(x)$ or $\rho_\theta r(x)$

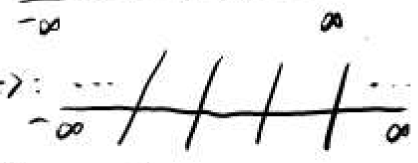
$\therefore S(K)$ $\begin{cases}\rho_\theta=\pi/2,\ \pi,\ 3\pi/2,\ 2\pi,\cdots\cdots\ (旋转)\\ \text{or}\\ \rho_{\pi/2}r,\ \rho_\pi r,\ \rho_{3\pi/2}r,\ \rho_{2\pi}r\ \ (镜射).\end{cases}$

Def6: 带饰: 指图形的对称变换沿着固定直线进行.

$\Rightarrow$ ① $\langle t_a\rangle$:

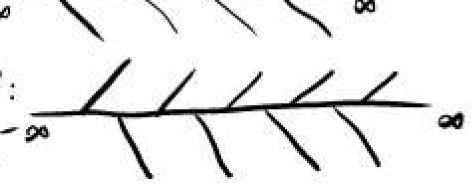


② $\langle t_a,\rho_\pi\rangle$:

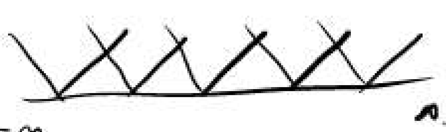


③ $\langle t_a, r\rangle$:

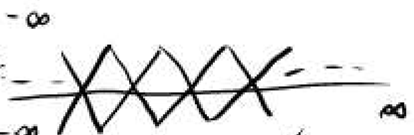
④ $\langle t_a, t_{\frac{a}{2}}r\rangle$:
滑动反射



⑤. $\langle t_a,\rho_\pi r\rangle$:



⑥. $\langle t_a,\rho_\pi, r\rangle$:



⑦ $\langle t_a,\rho_\pi r, t_{\frac{a}{2}}r\rangle$:

§2.

数域的对称

def 1: 若 $F\neq\phi$. F 为一数集. 则称 F 为数域.

当: F 关于和、差、积、商封闭 $\Rightarrow$ 必包含 "0与1".

Ex: R、Q、C. $Q(\sqrt2)=\{a+b\sqrt2\mid a,b\in Q\}$, $Q(\sqrt2,\sqrt3)$

def 2: F 为数域. $\phi: F\longrightarrow F$ 为双射.

当: $\phi(x+y)=\phi(x)+\phi(y)$, $\phi(xy)=\phi(x)\cdot\phi(y)$.

则 ϕ 称为 F 的一个自同构.

注: $\phi(0)=0$. $\phi(e)=e$. $\phi(-y)=-\phi(y)$.

且 $x,y\in F$. $\phi(x-y)=\phi(x)-\phi(y)$.

def 3: $Aut(F)=\{F$ 的全体自同构$\}$

注: $\forall\sigma,\tau\in Aut(F)$. 有 σ^{-1}、$\sigma\circ\tau\in Aut(F)$

proof: ① σ^{-1} 为双射显然

$\therefore$ 只需证 $\sigma^{-1}(x+y)=\sigma^{-1}(x)+\sigma^{-1}(y)$, $\sigma^{-1}(xy)=\sigma^{-1}(x)\sigma^{-1}(y)$

② $(\tau^{-1}\circ\sigma^{-1})\circ(\sigma\circ\tau)=\varepsilon$. $\therefore\sigma\circ\tau$ 有逆 $\Rightarrow$ 双射.

同 ①: $\sigma\tau(x+y)=\sigma[\tau(x)+\tau(y)]=\sigma\tau(x)+\sigma\tau(y)$.

$\sigma\tau(xy)=\sigma(\tau(x)\cdot\tau(y))=\sigma\tau(x)\cdot\sigma\tau(y)$

$\therefore\sigma\tau\in Aut(F)$. ∎

注: 此时 $\forall\sigma,\tau\in Aut(F)$ 有 $\sigma\tau\in Aut(F)$

$id\in Aut(F)$ 且 $id\circ\sigma=\sigma=\sigma\circ id$.

$\forall\sigma\in Aut(F)$ 有 $\sigma^{-1}\in Aut(F)$

$(\sigma\circ\tau)\circ\gamma=\sigma\circ(\tau\circ\gamma)$

则称 $Aut(F)$ 为 F 的自同构群

对: $Aut(Q)$ 下证 $=\{id\}$

$\forall f\in Aut(Q)$ 有:

$f(1)=1\Rightarrow\forall m\in Z^+$. $f(m)=f(\overbrace{1+1+\cdots+1}^{m个})=mf(1)$.

$\forall m\in Z^-$. $f(-m)=-f(m)=-mf(1)$.

$\therefore\forall m,n\in Z$. $n\neq0\Rightarrow m=mf(1)=f(m)=f(n\cdot\frac{m}{n})=n\cdot f(\frac{m}{n})$

$\therefore f(\frac{m}{n})=\frac{m}{n}\Rightarrow f=id$

故 $Aut(Q)=\{id\}$

对: $Q(\sqrt2)$. $Aut[Q(\sqrt2)]$

$\because Aut(Q)=\{id\}$. $f: Q(\sqrt2)\longrightarrow Q(\sqrt2)$. (也是 $Q\to Q$)

$\therefore\forall a\in Q$. $f\in Aut[Q(\sqrt2)]\Rightarrow f(a)=a$.

$\therefore f(a+b\sqrt2)=f(a)+f(b\sqrt2)=a+bf(\sqrt2)$

$\because 2=f(2)=f(\sqrt2^2)=[f(\sqrt2)]^2\Rightarrow f(\sqrt2)=\pm\sqrt2$.

$\therefore f(a+b\sqrt2)=a\pm b\sqrt2$.

令 $\phi_1\begin{cases}Q\mapsto Q\\\sqrt2\mapsto\sqrt2\end{cases}$. $\phi_2\begin{cases}Q\to Q\\\sqrt2\mapsto-\sqrt2\end{cases}$.

故 $\phi_1(a+b\sqrt2)=a+b\sqrt2$. $\phi_2(a+b\sqrt2)=a-b\sqrt2$

$(\phi_1,\phi_2\in Aut[Q(\sqrt2)])$

对: $Q(\sqrt2,\sqrt3)=\{a+b\sqrt2+c\sqrt3+d\sqrt2\sqrt3\mid a,b,c,d\in Q\}$

$Aut(Q(\sqrt2,\sqrt3))$: $f(a+b\sqrt2+c\sqrt3+d\sqrt2\sqrt3)=a+bf(\sqrt2)+cf(\sqrt3)+df(\sqrt2)\cdot f(\sqrt3)$.

而 $f(\sqrt2)=\pm\sqrt2$, $f(\sqrt3)=\pm\sqrt3\Rightarrow f(a+b\sqrt2+c\sqrt3+d\sqrt2\sqrt3)=$ 四种.

def4: E. F 为数域. $F\subset E$. 称 F 为 E 的子域 (E 为扩域).

对限主映射: $f: E\to E\Rightarrow f|_F: F\to E$.

$Aut(E/F)=\{\phi\in Aut(E)\mid\phi|_F=id\}$ 称 E 在 F 上的自同构群

Ex: $Aut[Q(\sqrt2,\sqrt3)/Q(\sqrt2)]$

§. 对称群 S_n.

def1: M 为非空集合. $S(M)=\{f: M\to M$ 的双射$\}\neq\phi$

则 $(S(M),\circ)$ 为 M 的变换群

若 $M=\{1,2,3,\cdots,n\}$. 则 $S(M)$ 为 n 元对称群. 记为 S_n.

$\forall\sigma\in S_n$. $\sigma=\begin{pmatrix}1&2&\cdots&n\\a_1&a_2&\cdots&a_n\end{pmatrix}$ 故 $a_1\sim a_n$ 为 $1\sim n$ 的排列

S_n 中有 $n!$ 个元素.

对 $\sigma=\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}$ $\tau=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$

则 $\sigma\tau=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}$

τ: 1 2 3 4 / 1 2 3 4 σ: 1 2 3 4 / 1 2 3 4

def2: 取 $\sigma\in S_n$. 若 $\sigma(\alpha_1)=\alpha_2$, $\sigma(\alpha_2)=\alpha_3$, $\cdots\cdots$, $\sigma(\alpha_n)=\alpha_1$ 且 σ 不在其余数作用。

则 σ 是一个轮换. 记为 $\sigma\triangleq(\alpha_1\alpha_2\cdots\alpha_m)$. 也记为 m 轮换. $m=2$ 称为对换.

$\therefore\sigma=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}=(3\ 4)$ 为对换.

$\sigma=\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}=(1\ 2\ 4\ 3)$ 为4轮换.

若 $\sigma=(\alpha_1\alpha_2\cdots\alpha_m)$. $\tau=(\beta_1\beta_2\cdots\beta_n)$ 称 σ. τ 不相交, 当: $\alpha_i\neq\beta_j$ $(i,j=1\sim n,m)$

或当: $\{\alpha_1,\alpha_2,\cdots,\alpha_m\}\cap\{\beta_1,\beta_2,\cdots,\beta_n\}=\phi$

Ex: $\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}=(3\ 4)$ 与 $\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}=(1\ 2)$ 不相交

注: $\alpha=(a_1a_2\cdots a_m)$, $\beta=(b_1b_2\cdots b_l)$ 不相交. 则 $\alpha\beta=\beta\alpha$.

proof: $\beta\alpha(i)=\beta[\alpha(i)]$

① $i\notin\{a_1,\cdots,a_m\}$ 故 $\alpha(i)=i\to\beta\alpha(i)=\beta(i)$

② $i\in\{a_1,\cdots,a_m\}$ 故 $\alpha(i)=a_j$. $j\in1\sim m\to\beta\alpha(i)=a_j=\alpha(i)$

对 $\alpha\beta(i)=\alpha[\beta(i)]$

① $i\notin\{b_1,\cdots,b_l\}$ 故 $\beta(i)=i\to\alpha[\beta(i)]=\alpha(i)$.

② $i\in\{b_1,\cdots,b_l\}$ 故 $\beta(i)=b_j$. $j\in1\sim l\to\alpha\beta(i)=b_j=\beta(i)$.

而 $i\notin\{b_1\cdots b_l\}\Leftrightarrow i\in\{a_1,\cdots,a_m\}$

故可知: $\alpha\beta=\beta\alpha$. ∎

注: 任意一个 n 元置换 σ, 可以写成"不相交"的轮换的积.

(表示唯一)

proof 唯一: 设 $\sigma=\sigma_1\sigma_2\cdots\sigma_t=\tau_1\cdots\tau_t$.

(其中 σ_i 与 τ_i 均不相交)

设 $\sigma(a_1)=\sigma_1(a_1)=\tau_1(a_1)$. $a_2=\sigma(a_1)$. $\cdots\cdots$. $a_j=\sigma(a_{j-1})$, $a_1=\sigma(a_j)$.

下证: $\sigma_1=(a_1a_2\cdots a_j)$

$\because\sigma(a_2)=\sigma(\sigma(a_1))=\sigma(\sigma_1(a_1))=\sigma_1^2(a_1)$.

故 $\sigma^2=\sigma_1^2$ 类似: $\sigma^i=\sigma_1^i\Rightarrow\sigma_1=(a_1a_2\cdots a_j)$.

同理 $\tau_1=(a_1a_2\cdots a_j)$.

故 $\sigma_2\cdots\sigma_t=\tau_2\tau_3\cdots\tau_t\Rightarrow$ 由归纳: $\sigma_i=\tau_i$.

$\therefore\sigma$ 分解唯一. ∎

§2

数域的对称

def 1: 若 $F\neq\phi$. F为一数集. 则称F为数域.
当: F关于和、差、积、商封闭 ⇒ 必包含"0"与"1".

Ex: R、Q、C. $Q(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in Q\}$. $Q(\sqrt{2},\sqrt{3})$

def 2: F为数域. $\phi: F\longrightarrow F$ 为双射.
当: $\phi(x+y)=\phi(x)+\phi(y)$, $\phi(xy)=\phi(x)\cdot\phi(y)$.
则ϕ称为F的一个自同构.
注: $\phi(0)=0$. $\phi(e)=e$. $\phi(-y)=-\phi(y)$.
且$x,y\in F$. $\phi(x-y)=\phi(x)-\phi(y)$.

def 3: $Aut(F)=\{F$的全体自同构$\}$
注: $\forall\sigma,\tau\in Aut(F)$. 有$\sigma^{-1}$、$\sigma\circ\tau\in Aut(F)$.
proof: ① σ^{-1}为双射显然
∴只需证 $\sigma^{-1}(x+y)=\sigma^{-1}(x)+\sigma^{-1}(y)$, $\sigma^{-1}(xy)=\sigma^{-1}(x)\sigma^{-1}(y)$
② $(\tau^{-1}\circ\sigma^{-1})\cdot(\sigma\circ\tau)=\varepsilon$. ∴ $\sigma\circ\tau$ 有逆 ⇒ 双射.
同①: $\sigma\tau(x+y)=\sigma[\tau(x)+\tau(y)]=\sigma\tau(x)+\sigma\tau(y)$.
$\sigma\tau(xy)=\sigma(\tau(x)\cdot\tau(y))=\sigma\tau(x)\cdot\sigma\tau(y)$
∴ $\sigma\tau\in Aut(F)$. ∎

注: 此时 $\forall\sigma,\tau\in Aut(F)$ 有 $\sigma\tau\in Aut(F)$

$$\begin{cases} id\in Aut(F)\text{ 且 } id\circ\sigma=\sigma=\sigma\circ id \\ \forall\sigma\in Aut(F)\text{ 有 }\sigma^{-1}\in Aut(F) \\ (\sigma\circ\tau)\circ\gamma=\sigma\circ(\tau\circ\gamma) \end{cases}$$

则称$Aut(F)$为F的自同构群.

对: $Aut(Q)$ 下证 $=\{id\}$
$\forall f\in Aut(Q)$有:
$f(1)=1\Rightarrow\forall m\in Z^{+}$. $f(m)=f(\overbrace{1+1+\cdots+1}^{(m个)})=mf(1)$.
$\forall m\in Z^{-}$. $f(-m)=-f(m)=-mf(1)$
∴ $\forall m,n\in Z$. $n\neq0\Rightarrow m=mf(1)=f(m)=f(n\cdot\frac{m}{n})=n\cdot f(\frac{m}{n})$
∴ $f(\frac{m}{n})=\frac{m}{n}\Rightarrow f=id$.
故$Aut(Q)=\{id\}$

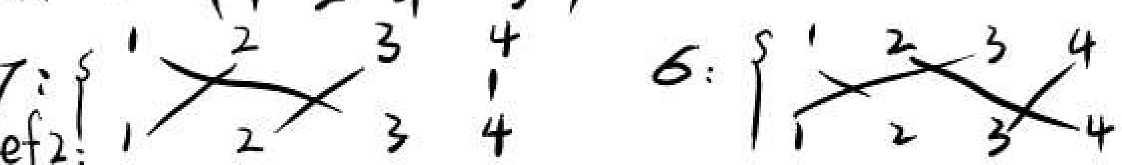
对: $Q(\sqrt{2})$. $Aut[Q(\sqrt{2})]$
∵ $Aut(Q)=\{id\}$. $f: Q(\sqrt{2})\longrightarrow Q(\sqrt{2})$ (也是$Q\to Q$)
∴ $\forall a\in Q$. $f\in Aut[Q(\sqrt{2})]\Rightarrow f(a)=a$.
∴ $f(a+b\sqrt{2})=f(a)+f(b\sqrt{2})=a+bf(\sqrt{2})$
∵ $2=f(2)=f(\sqrt{2}^2)=[f(\sqrt{2})]^2\Rightarrow f(\sqrt{2})=\pm\sqrt{2}$.
∴ $f(a+b\sqrt{2})=a\pm b\sqrt{2}$.
令 $\phi_1\begin{cases}Q\mapsto Q\\ \sqrt{2}\mapsto\sqrt{2}\end{cases}$. $\phi_2\begin{cases}Q\to Q\\ \sqrt{2}\mapsto-\sqrt{2}\end{cases}$.
故 $\phi_1(a+b\sqrt{2})=a+b\sqrt{2}$. $\phi_2(a+b\sqrt{2})=a-b\sqrt{2}$
($\phi_1,\phi_2\in Aut[Q(\sqrt{2})]$)

对: $Q(\sqrt{2},\sqrt{3})=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}\mid a.b.c.d\in Q\}$
$Aut[Q(\sqrt{2},\sqrt{3})]$: $f(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3})=a+bf(\sqrt{2})+cf(\sqrt{3})+df(\sqrt{2})\cdot f(\sqrt{3})$.
而 $f(\sqrt{2})=\pm\sqrt{2}$, $f(\sqrt{3})=\pm\sqrt{3}\Rightarrow f(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\cdot\sqrt{3})=$四种.

def4: E、F为数域. $F\subset E$. 称F为E的子域 (E为扩域).
对限定映射: $f: E\to E\Rightarrow f|_F: F\to E$.
$Aut(E/F)=\{\phi\in Aut(E)\mid\phi|_F=id\}$ 称E在F上的自同构群
Ex: $Aut[Q(\sqrt{2},\sqrt{3})/Q(\sqrt{2})]$

§. 对称群S_n.

def1: M为非空集合. $S(M)=\{f: M\to M$的双射$\}\neq\phi$
则$(S(M),\circ)$为M的变换群
若$M=\{1,2,3,\cdots,n\}$. 则$S(M)$为n元对称群. 记为S_n.
$\forall\sigma\in S_n$. $\sigma=\begin{pmatrix}1&2&\cdots&n\\a_1&a_2&\cdots&a_n\end{pmatrix}$ 故 $a_1\sim a_n$为$1\sim n$的排列
S_n中有$n!$个元素.
对 $\sigma=\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}$ $\tau=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$
则 $\sigma\circ\tau=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}$

τ:  σ:

def2:
取 $\sigma\in S_n$. 若 $\sigma(\alpha_1)=\alpha_2$, $\sigma(\alpha_2)=\alpha_3$, ……, $\sigma(\alpha_n)=\alpha_1$ 且σ不在其余数作用
则σ是一个轮换, 记为$\sigma\triangleq(\alpha_1\alpha_2\cdots\alpha_m)$. 也记为$m$轮换. $m=2$称为对换.
∴ $\sigma=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}=(3\ 4)$ 为对换
$\sigma=\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}=(1\ 2\ 4\ 3)$ 为4轮换.
若 $\sigma=(\alpha_1\alpha_2\cdots\alpha_m)$. $\tau=(\beta_1\beta_2\cdots\beta_n)$ 称σ、τ不相交, 当: $\alpha_i\neq\beta_j$ ($i,j=1\sim n,m$
或当: $\{\alpha_1,\alpha_2,\cdots,\alpha_m\}\cap\{\beta_1,\beta_2,\cdots,\beta_n\}=\phi$
Ex: $\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}=(3\ 4)$ 与 $\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}=(1\ 2)$ 不相交
注: $\alpha=(a_1a_2\cdots a_m)$, $\beta=(b_1b_2\cdots b_l)$ 不相交, 则$\alpha\beta=\beta\alpha$.
proof: $\beta\alpha(i)=\beta[\alpha(i)]$
① $i\notin\{a_1,\cdots,a_m\}$ 故$\alpha(i)=i\to\beta\alpha(i)=\beta(i)$
② $i\in\{a_1,\cdots,a_m\}$ 故$\alpha(i)=a_j$. $j\in1\sim m$. $\to\beta\alpha(i)=a_j=\alpha(i)$
对 $\alpha\beta(i)=\alpha[\beta(i)]$
① $i\notin\{b_1,\cdots,b_l\}$ 故$\beta(i)=i\to\alpha[\beta(i)]=\alpha(i)$.
② $i\in\{b_1,\cdots,b_l\}$ 故$\beta(i)=b_j$. $j\in1\sim l$ $\to\alpha\beta(i)=b_j=\beta(i)$.
而 $i\notin\{b_1\cdots b_l\}\Leftrightarrow i\in\{a_1,\cdots,a_m\}$.
故可知: $\alpha\beta=\beta\alpha$. ∎

注: 任意一个n元置换σ, 可以写成"不相交"的轮换的积.
(表示唯一)
proof唯一: 计 $\sigma=\sigma_1\sigma_2\cdots\sigma_l=\tau_1\cdots\tau_t$.
(其中σ_i与τ_j均不相交)
设$\sigma(a_1)=\sigma_1(a_1)=\tau_1(a_1)$. $a_2=\sigma(a_1)$. ……. $a_j=\sigma(a_{j-1})$, $a_1=\sigma(a_j)$.
下证: $\sigma_1=(a_1a_2\cdots a_j)$
∵ $\sigma(a_2)=\sigma(\sigma(a_1))=\sigma(\sigma_1(a_1))=\sigma_1^2(a_1)$.
故$\sigma^2=\sigma_1^2$ 类似: $\sigma^i=\sigma_1^i\Rightarrow\sigma_1=(a_1a_2\cdots a_j)$.
同理 $\tau_1=(a_1a_2\cdots a_j)$.
故 $\sigma_2\cdots\sigma_l=\tau_2\tau_3\cdots\tau_t$. ⇒ 由归纳: $\sigma_i=\tau_i$.
∴ σ分解唯一. ∎

§2

数域的对称

def 1：若$F\neq\phi$，F为一数集，则称F为数域。
当：F关于和、差、积、商封闭⇒必包含"0与1"。
Ex：R、Q、C、$Q(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in Q\}$、$Q(\sqrt{2},\sqrt{3})$

def 2：F为数域，$\phi: F\longrightarrow F$为双射。
当：$\phi(x+y)=\phi(x)+\phi(y)$，$\phi(xy)=\phi(x)\cdot\phi(y)$。
则ϕ称为F的一个自同构。
注：$\phi(0)=0$，$\phi(e)=e$，$\phi(-y)=-\phi(y)$。
且$x,y\in F$，$\phi(x-y)=\phi(x)-\phi(y)$。

def 3：$Aut(F)=\{F$的全体自同构$\}$
注：$\forall\sigma,\tau\in Aut(F)$，有$\sigma^{-1}$、$\sigma\circ\tau\in Aut(F)$
proof：① σ^{-1}为双射显然
∴只需证$\sigma^{-1}(x+y)=\sigma^{-1}(x)+\sigma^{-1}(y)$，$\sigma^{-1}(xy)=\sigma^{-1}(x)\sigma^{-1}(y)$
② $(\tau^{-1}\circ\sigma^{-1})\cdot(\sigma\circ\tau)=\varepsilon$。∴$\sigma\circ\tau$有逆⇒双射。
同①：$\sigma\tau(x+y)=\sigma[\tau(x)+\tau(y)]=\sigma\tau(x)+\sigma\tau(y)$。
$\sigma\tau(xy)=\sigma(\tau(x)\cdot\tau(y))=\sigma\tau(x)\cdot\sigma\tau(y)$
∴$\sigma\tau\in Aut(F)$。 ▨

注：此时$\forall\sigma,\tau\in Aut(F)$ 有$\sigma\tau\in Aut(F)$
$$\begin{cases} id\in Aut(F)\text{ 且 } id\circ\sigma=\sigma=\sigma\circ id \\ \forall\sigma\in Aut(F)\text{ 有 }\sigma^{-1}\in Aut(F) \\ (\sigma\circ\tau)\circ\gamma=\sigma\circ(\tau\circ\gamma) \end{cases}$$
则称$Aut(F)$为F的自同构群。

对：$Aut(Q)$ 下证$=\{id\}$
$\forall f\in Aut(Q)$有：
$f(1)=1\Rightarrow\forall m\in Z^+$，$f(m)=f(\overbrace{1+1+\cdots+1}^{(m\text{个})})=mf(1)$。
$\forall m\in Z^-$，$f(-m)=-f(m)=-mf(1)$
∴$\forall m,n\in Z$，$n\neq0\Rightarrow m=mf(1)=f(m)=f(n\cdot\frac{m}{n})=n\cdot f(\frac{m}{n})$
∴$f(\frac{m}{n})=\frac{m}{n}\Rightarrow f=id$
故$Aut(Q)=\{id\}$

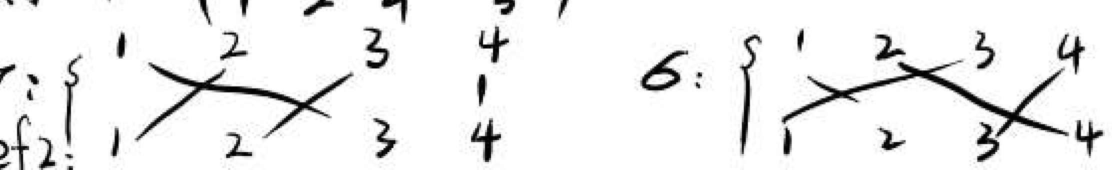
对：$Q(\sqrt{2})$，$Aut[Q(\sqrt{2})]$
∵$Aut(Q)=\{id\}$，$f: Q(\sqrt{2})\longrightarrow Q(\sqrt{2})$（也是$Q\to Q$）
∴$\forall a\in Q$，$f\in Aut[Q(\sqrt{2})]\Rightarrow f(a)=a$。
∴$f(a+b\sqrt{2})=f(a)+f(b\sqrt{2})=a+bf(\sqrt{2})$
∵$2=f(2)=f(\sqrt{2}^2)=[f(\sqrt{2})]^2\Rightarrow f(\sqrt{2})=\pm\sqrt{2}$。
∴$f(a+b\sqrt{2})=a\pm b\sqrt{2}$。
令 $\phi_1\begin{cases}Q\mapsto Q\\ \sqrt{2}\mapsto\sqrt{2}\end{cases}$，$\phi_2\begin{cases}Q\to Q\\ \sqrt{2}\mapsto-\sqrt{2}\end{cases}$。
故$\phi_1(a+b\sqrt{2})=a+b\sqrt{2}$，$\phi_2(a+b\sqrt{2})=a-b\sqrt{2}$
$(\phi_1,\phi_2\in Aut[Q(\sqrt{2})])$

对：$Q(\sqrt{2},\sqrt{3})=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}\mid a,b,c,d\in Q\}$
$Aut[Q(\sqrt{2},\sqrt{3})]$：$f(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3})=a+bf(\sqrt{2})+cf(\sqrt{3})+df(\sqrt{2})\cdot f(\sqrt{3})$。
而$f(\sqrt{2})=\pm\sqrt{2}$，$f(\sqrt{3})=\pm\sqrt{3}\Rightarrow f(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3})=$四种。

def4：E、F为数域，$F\subset E$，称F为E的子域（E为扩域）。
对限定映射：$f: E\to E\Rightarrow f|_F: F\to E$。
$Aut(E/F)=\{\phi\in Aut(E)\mid\phi|_F=id\}$ 称E在F上的自同构群
Ex：$Aut[Q(\sqrt{2},\sqrt{3})/Q(\sqrt{2})]$

§ 对称群S_n。

def1：M为非空集合，$S(M)=\{f: M\to M$的双射$\}\neq\phi$
则$(S(M),\circ)$为M的变换群
若$M=\{1,2,3,\cdots,n\}$，则$S(M)$为n元对称群，记为S_n。
$\forall\sigma\in S_n$，$\sigma=\begin{pmatrix}1&2&\cdots&n\\a_1&a_2&\cdots&a_n\end{pmatrix}$ 故$a_1\sim a_n$为$1\sim n$的排列
S_n中有$n!$个元素。
对 $\sigma=\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}$，$\tau=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$
则$\sigma\circ\tau=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}$

τ： σ：


def2：
取$\sigma\in S_n$，若$\sigma(\alpha_1)=\alpha_2$，$\sigma(\alpha_2)=\alpha_3$，……，$\sigma(\alpha_n)=\alpha_1$且σ不在其余数作用
则σ是一个轮换，记为$\sigma\triangleq(\alpha_1\alpha_2\cdots\alpha_m)$，也记为m轮换。m=2称为对换。
∴$\sigma=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}=(3\ 4)$为对换
$\sigma=\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}=(1\ 2\ 4\ 3)$为4轮换。
若$\sigma=(\alpha_1\alpha_2\cdots\alpha_m)$，$\tau=(\beta_1\beta_2\cdots\beta_n)$ 称σ、τ不相交，当：$\alpha_i\neq\beta_j$（$i,j=1\sim n,m$
或当：$\{\alpha_1,\alpha_2,\cdots,\alpha_m\}\cap\{\beta_1,\beta_2,\cdots,\beta_n\}=\phi$
Ex：$\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}=(3\ 4)$与$\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}=(1\ 2)$不相交
注：$\alpha=(a_1a_2\cdots a_m)$，$\beta=(b_1b_2\cdots b_l)$不相交，则$\alpha\beta=\beta\alpha$。
proof：$\beta\alpha(i)=\beta[\alpha(i)]$
① $i\notin\{a_1,\cdots,a_m\}$ 故$\alpha(i)=i\to\beta\alpha(i)=\beta(i)$
② $i\in\{a_1,\cdots,a_m\}$ 故$\alpha(i)=a_j$，$j\in1\sim m\to\beta\alpha(i)=a_j=\alpha(i)$
对$\alpha\beta(i)=\alpha[\beta(i)]$
① $i\notin\{b_1,\cdots,b_l\}$ 故$\beta(i)=i\to\alpha[\beta(i)]=\alpha(i)$。
② $i\in\{b_1,\cdots,b_l\}$ 故$\beta(i)=b_j$，$j\in1\sim l\to\alpha\beta(i)=b_j=\beta(i)$。
而$i\notin\{b_1\cdots b_l\}\Leftrightarrow i\in\{a_1,\cdots,a_m\}$
故可知：$\alpha\beta=\beta\alpha$。 ▨

注：任意一个n元置换σ，可以写成"不相交"的轮换的积。
（表示唯一）
proof唯一：设$\sigma=\sigma_1\sigma_2\cdots\sigma_l=\tau_1\cdots\tau_t$。
（其中σ_i与τ_i均为不相交）
设$\sigma(a_1)=\sigma_1(a_1)=\tau_1(a_1)$，$a_2=\sigma(a_1)$，……，$a_j=\sigma(a_{j-1})$，$a_1=\sigma(a_j)$。
下证：$\sigma_1=(a_1a_2\cdots a_j)$
∵$\sigma(a_2)=\sigma(\sigma(a_1))=\sigma(\sigma_1(a_1))=\sigma_1^2(a_1)$。
故$\sigma^2=\sigma_1^2$ 类似：$\sigma^i=\sigma_1^i\Rightarrow\sigma_1=(a_1a_2\cdots a_j)$。
同理$\tau_1=(a_1a_2\cdots a_j)$。
故$\sigma_2\cdots\sigma_l=\tau_2\tau_3\cdots\tau_t$。⇒由归纳：$\sigma_i=\tau_i$。
∴σ分解唯一。 ▨

§. 子群

规定：$(G,\cdot)$ 为一群，H_i 为群，$i\in I$.

记："$\underbrace{a\cdot a\cdots a}_{n个}=a^n$" $\begin{cases}\bigcap H_i=\wedge H_i \\ \bigcup H_i=\vee H_i\end{cases}$

if G 为 Abel 群，$\forall a,b\in G$，$a\cdot b=b\cdot a\rightarrow$ 记为 $(G,+)$

$\forall t\in(G,+)\Rightarrow \underbrace{t+t+\cdots+t}_{n个}=nt$.

def 1. 元素的阶：
若 $a\in G$，$\exists$ 一个 n s.t. $a^n=e$ 且 $\forall m<n$，$a^m\neq e$. 则 n 为 a 的阶
记作：$|a|$. Ex: $|e|=1$
若 $\forall n\in\mathbb{Z}^+$ $a^n\neq e$. 则 a 的阶为 ∞.

def 2：群的中心元：对 $a\in G$，若 $\forall x\in G$，有 $ax=xa$. 则 a 为中心元
G 的中心元集合为 $C(G)$ 记为 G 的中心.
注：e 必 $\in C(G)$.
若 $a\in C(G)$ 则 $a^{-1}\in C(G)$.

def 3. $H,K\subset G$. 记：$HK=\{h\cdot k\mid h\in H,k\in K\}$，$H^{-1}=\{h^{-1}\mid h\in H\}$
若 $H\subset G$，$HH\subset H$，$H^{-1}\subset H$. 则 H 为 G 的一个子群. 记：$H<G$.
即：$\forall a,b\in H$，$ab\in H$，$a^{-1}\in H$.
平凡子群：G 与 $\{e\}$. 其余为非平凡子群（真子群）.
注. 若 H 为 G 子群. 则 H 关于 G 中运算构成一个群，且 $e_H=e_G$.
Proof：H 为群只需证：H 有单位元 e_H. 逆元. 下证：
$\because HH\subset H\Rightarrow$ 取 $a\in H$ $\because HH^{-1}\subset H\cdot H\subset H$.
$\therefore a\cdot a^{-1}\subset H\Rightarrow e_G\in H$.
又 $\forall h\in H\subset G$ 则 $h\cdot e_G=e_G\cdot h=h$.
$\therefore e_G=e_H$
$\because H\subset G$. $\therefore\forall a\in H$ 有逆元 a^{-1} 又 $H^{-1}\subset H\Rightarrow a^{-1}\in H$
$\therefore H$ 中有单位元 $e_H=e_G$，逆元 $a^{-1}\in H$. ∎
注：H_i，$i\in I$ 均为 G 的子群. 则 H_i 任意交均为 G 子群
Proof：显然 H_i 中有 G 的单位元 e
$\therefore\wedge H_i\neq\phi$ $\forall a,b\in\wedge H_i$.
$\therefore a,b\in H_i$ $(\forall i\in I)$
故 $a\cdot b\in H_i\Rightarrow a\cdot b\in\wedge H_i$. $\Rightarrow\wedge H_i\wedge H_i\subset\wedge H_i$.
同理 $a^{-1}\in\wedge H_i\Rightarrow\wedge H_i$ 为 G 子群 ∎
注：设 M 为 G 的一个集合. 记 H_i 为 G 子群，$M\subset H_i$，$\forall i\in I$
则记 G 中包含 M 的所有子群交：$\wedge H_i$ 为包含 M 的最小子群
Proof. 由上注. $\wedge H_i$ 也为包含 M 的 G 的子群
只需证：$\forall K$ 子群 $\supset M$，有 $K\supset\wedge H_i$ 即可，这是显然的 ∎
Ex：$M=\phi\Rightarrow\wedge H_i=\{e\}$
$\begin{cases}M 为一个群\Rightarrow\wedge H_i=M. \\ M\neq\phi 且不为一个群：即\exists a,b\in M,\ s.t.\ ab\notin M\ or\ a^{-1}\notin M.\end{cases}$
下求 $M\neq\phi$ 且不为群的 $\wedge H_i$：
令 $\wedge H_i=\{x_1\cdots x_n\mid x_i\in M\cup M^{-1}\}$ 即可
下证 $\wedge H_i$ 满足是包含 M 的最小子群：
① $\forall a,b\in\wedge H_i$. $\therefore a\cdot b=x_1\cdots x_n y_1\cdots y_n\in\wedge H_i$.
$\therefore\wedge H_i\wedge H_i\subset\wedge H_i$
② $\forall a\in\wedge H_i$. $\therefore a=x_1^{-1}\cdots x_n^{-1}\in\wedge H_i$
$\therefore\wedge H_i^{-1}\subset\wedge H_i$
③. 显然 $M\subset\wedge H_i$. 若 $\forall K\supset M$
$\because\forall a\in M$. $a\in K$，又 $K^{-1}\subset K\Rightarrow a^{-1}\in K$
又 $K\cdot K\cdots K\subset K\cdot K\subset K\Rightarrow\underbrace{M\cup M^{-1}\cdot M\cup M^{-1}\cdots}_{n个积}=\wedge H_i\subset K$
$\therefore\wedge H_i$ 找到. 记为 $\langle M\rangle$

def 4：$\langle M\rangle$ 记为 M 的生成元群. 基本元素"为生成元".

def 5：对 $\forall a\in G$. 作 T_a：$\begin{matrix}G\rightarrow G\\ x\rightarrow axa^{-1}\end{matrix}$ 的映射.
则 T_a 显然双射 $\Rightarrow T_a$ 为 G 的一个自同构 $\in Aut(G)$
记为 G 的内自同构. 记 $Inn(G)=\{T_a\mid a\in G\}$
Ex：$Inn(G)$ 为 $Aut(G)$ 的子群
Proof：$\because T_a\cdot T_b=T_{ab}\in Inn(G)$
且 $T_aT_{a^{-1}}=I_n\Rightarrow T_a^{-1}=T_{a^{-1}}\in Inn(G)$
故记 $Inn(G)$ 为 G 的内自同构群

$xT_{ab}=abx(ab)^{-1}=abxb^{-1}a^{-1}$
而 $xT_aT_b=abxb^{-1}a^{-1}$
$\therefore T_{ab}=T_aT_b$ （同构）

def 6. $H<G$. $\forall a\in G$，$T_a(H)\subset H$. 则记 H 为 G 的"正规子群"
记作 $H\lhd G$.
注：$H\lhd G\Leftrightarrow\forall a\in G$. $aH=Ha\Leftrightarrow aHa^{-1}=H$.
Proof：$T_a(H)\subset H\Rightarrow\forall H$. $aHa^{-1}\subset H$
$\therefore aH\subset Ha$. 同：$a^{-1}Ha\subset H\Rightarrow Ha\subset aH$
$\therefore aH=Ha$. ∎
Ex：m 为平面的刚体：$m=t_a\rho_\theta r$ or $t_a\rho_\theta$.
则 $\{t_a,\rho_\theta,r\}$ 为运动群 T 的生成元集
Ex：对 $\langle\rho_\theta,r\rangle$. 记作"二面体群" $(\theta=\frac{2\pi}{n})$.
则 $\rho_\theta^n=r^2=id$. $\because r\rho_\theta=\rho_{-\theta}r\Rightarrow r\rho_\theta r^{-1}=\rho_{-\theta}$.
Ex：求 S_n 生成元集
$\because S_n$ 为不相交轮换之并
$S_n=(i_1i_2\cdots i_t)(j_1\cdots j_k)\cdots(\delta_1\cdots\delta_m)$. 用轮换生成 S_n
$\forall(i_1i_2\cdots i_t)=(i_1i_2)(i_1i_3)\cdots(i_1i_t)$ 对换生成轮换证.
$\Rightarrow S_n$ 由对换的生成元集："$\langle(12)(23)\cdots(n-1\,n)\rangle$"
或 $\langle(i,j)\rangle$（有 $\frac{n\cdot(n-1)}{2}$ 个） 因为 $(i,j)=(j,i)$ （有 $n-1$ 个）
$=(j,j-1)(j\ j-2)\Rightarrow(j-2\ j)$
公式："$(j-2\ j-1)(j-1\ j)=(j-1\ j\ j-2)$" 右往左时". $=(j\ j-1)(j-2\ j-1)(j-1\ j)$.

def 7. $t(x_1,\cdots,x_n)=\begin{vmatrix}1&\cdots&1\\ x_1&\cdots&x_n\\ \vdots&&\vdots\\ x_1^{n-1}&\cdots&x_n^{n-1}\end{vmatrix}$
当 $\forall\sigma\in S_n$
记 $\sigma(t(x_1,\cdots,x_n))=t(x_{\sigma(1)},\cdots,x_{\sigma(n)})=\begin{cases}t(x_1,\cdots,x_n)\Rightarrow\sigma 为偶置换\\ -t(x_1,\cdots,x_n)\Rightarrow\sigma 为奇置换.\end{cases}$
（σ 可写成对换之积，又对换即：
行列式交换两行，多了一个负号）.
等价：偶置换即可写成偶数个对换的积.
记 A_n 为 $\{S_n$ 中所有偶置换$\}\Rightarrow A_n\lhd S_n$.
称 A_n 为 n 元交错群（$\frac{n!}{2}$ 个元素）
注：求 A_n 生成元集：
$\because(i\,j)(i\,k)=(i\,k\,j)$ $(j\,k\,i)(k\,l\,j)$.
故 $(i\,j)(k\,l)=(i\,j)(j\,k)(j\,k)(k\,l)$
故偶数个对换 $\Rightarrow$ 三轮换的积.
又三轮换为偶置换
$\Rightarrow A_n$ 由三轮换生成

def 8. 若 $G=\langle a\rangle$. 记为循环群
若 $G=\langle a_1,\cdots,a_n\rangle$ 记为有限生成群
注：若 $G=\langle a\rangle$ 则 G 必为以下之一.
① $G=\langle\cdots a^{-2},a^{-1},e,a,a^2,\cdots\rangle\Rightarrow$ 无限
② $G=\langle e,a,a^2,\cdots,a^n\rangle\Rightarrow$ 有限
且①中若 $a^m=a^n\Rightarrow m=n$，②中 $a^n=e$，$a^i=a^j\Rightarrow n\mid j-i$.
Proof：① $|a|=\infty$. 故 $\forall m\neq n$ 有 $a^m\neq a^n$.
又 $\langle a\rangle=\{x_1x_2\cdots\mid x_i\in a\vee a^{-1}\}$
$\therefore G=\{\cdots,a^{-2},a^{-1},e,a,\cdots\}$
② 若 $|a|=n$. $\forall m\in\mathbb{Z}\Rightarrow m=nq+r$. $0\le r\le n-1$.（q 可为负数）
$\therefore a^m=a^{nq+r}=a^{nq}\cdot a^r=e\cdot a^r=a^r$
而若 $1\le i,j<n$ 时 $a^i\neq a^j$（若 $a^i=a^j\Rightarrow a^{i-j}=e\Rightarrow|a|<n$ 矛盾!）
$\Rightarrow G=\{e,a,a^2,\cdots,a^{n-1}\}$ ∎
Ex：①"$(\mathbb{Z},+)$：生成元 1" ② $G=\langle\rho_\theta\rangle$.（$\theta=\frac{2\pi}{n}$）
$\Rightarrow$ 在同构意义下. 循环群只有两个：$(\mathbb{Z},+)$，$\langle\rho_\theta\rangle$.
Proof：Ⅰ 若 $G=\{a^n\mid n\in\mathbb{Z}\}$. 则令 θ_1：$\begin{matrix}\mathbb{Z}\longrightarrow G\\ n\longmapsto a^n\end{matrix}$
可证 θ_1 为双射. 又 $\theta_1(x+y)=a^{x+y}=\theta_1(x)\theta_1(y)$
$\therefore\theta_1$ 同构对应 $\Rightarrow(\mathbb{Z},+)\cong G$.
Ⅱ. 若 $G=\{e,a,a^2,\cdots,a^{n-1}\}$ $(a^n=e)$ 则令 θ_2：$C_n\rightarrow G$.
则对 θ_2：① $a^i=a^j\Rightarrow n\mid i-j$. $i-j=kn$. $(\rho_\theta\rightarrow\frac{2\pi}{n})$ $\rho_\theta^i\mapsto a^i$
故 $\rho_\theta^i=\rho_\theta^j\cdot\rho_\theta^{kn}=\rho_\theta^j$. $\therefore\theta_2$ 为单射. 又 θ_2 显然为满射 $\Rightarrow$"双射"
② $\theta_2(\rho_\theta^i\cdot\rho_\theta^j)=\theta_2(\rho_\theta^{i+j})=a^{i+j}=a^i\cdot a^j=\theta_2(\rho_\theta^i)\theta_2(\rho_\theta^j)\Rightarrow$ 同构对应.
则 $C_n\cong G$ ∎

5、子群（续）.

1. G 为平面运动群的有限子群. 则平面上 $\exists P$. s.t $\forall g\in G$. s.t $g(P)=P$.

$\cdot g_n(p_0)$ $\cdot g_1(p_0)$ $\cdot p_0$ $\cdot g_2(p_0)$ $g_{n-1}(p_0)$ $\cdots$ $\cdot g_3(p_0)$

$G=\{g_1, g_2, \cdots, g_n\}$

令 $P=\dfrac{\sum\limits_{i=1}^{n} g_i(p_0)}{n}$ $\Rightarrow$ 因为 h 不一定是线性

$\therefore \forall h$. $h(P)=h\left(\sum\limits_{i=1}^{n} g_i(p_0)/n\right)$ 不能直接 $\dfrac{\sum h g_i(p)}{n}$ $\Big|$ $\dfrac{1}{n}\sum\limits_{i=1}^{n} h g_i(p_0)$.

① $h=t_a\rho_\theta \Rightarrow h(P)=\rho_\theta\left(\sum\limits_{i=1}^{n} g_i(p_0)/n\right)+\vec{a}$

② $h=t_a\rho_\theta r$ 同上

ρ_θ 为线性 $\Rightarrow =\dfrac{\sum\limits_{i=1}^{n}\rho_\theta g_i(p_0)}{n}+\vec{a}=\dfrac{1}{n}\sum\limits_{i=1}^{n}\left(\rho_\theta g_i(p_0)+\vec{a}\right)$ $=\dfrac{1}{n}\sum\limits_{i=1}^{n} h g_i(p_0)$.

$\Rightarrow h=\dfrac{1}{n}\sum\limits_{i=1}^{n} h g_i(p_0)$ 又 $hg_i\in G$.

假设 $hg_1=g_i$, $hg_2=g_j$ $\Rightarrow$ 若 $g_i=g_j \Rightarrow hg_1=hg_2 \Rightarrow g_1=g_2$.

故 hg_i 跑遍 G $\Rightarrow$ $h(P)=P$ （即 $\{hg_i\}=\{g_i\}$） ▨

应用：适当选系. 令 P 为原点"O".

则 G 为 $\begin{cases} \langle\rho_\theta\rangle & C_n \quad \theta=\frac{2\pi}{n} \\ \langle\rho_\theta, r\rangle & D_n \text{（二面体群）} \end{cases}$ $\Rightarrow$ 即为平面运动群的子群

Proof：① G 只为旋转群

令 θ 为旋转角的"最小角". 则 $\forall\alpha$. $\Rightarrow \alpha=m\theta+\psi$ $(0\le\psi<\theta)$.

则 $\rho_\psi=\rho_{\alpha-m\theta}=\rho_\alpha\rho_\theta^{-m}\in G$ $\because \psi<\theta \Rightarrow \psi=0$. $\therefore \forall\alpha \Rightarrow \theta\mid\alpha$

$\therefore G$ 中旋转为 $\rho_\theta^k \Rightarrow \therefore G=\langle\rho_\theta\rangle$. ▨

② G 有镜射 适当选系 令其为 r（关于 x 轴反射）. $(r^2=e)$

设 $G\neq\{e, r\}$ 则存在 $\rho_\theta\in G$

设 H 为 G 中所有旋转 $\Rightarrow H=\langle\rho_\theta\rangle$.

故 G 中必有 $\{\rho_\theta^k, \rho_\theta^k r\}=H'$

现 $\forall G$ 中的 g. 若 g 为旋转，则 $g\in H'$. 若 g 为反射：

设 g 与 x 轴夹角为 α $\Rightarrow$ 则 $\rho_{2\alpha}r=g\in H'$, 由①. $\rho_{2\alpha}=\rho_\theta^k$.

故 $G=H'=\langle\rho_\theta, r\rangle$. ▨

Q：若 $t_a\in G$. 则"G 无限".（一直作 $t_a, t_{2a}, \cdots, t_{\infty a}$）

但 $t_a\rho_\theta\in G$ 呢？

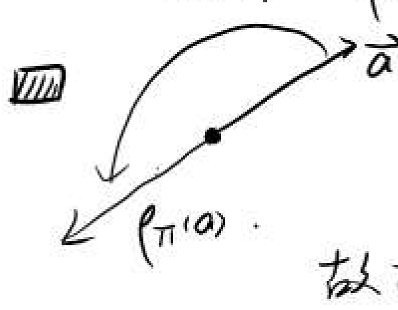
$\Downarrow$

不妨设 $\langle t_a\rho_\pi\rangle\in G$.

又 $\rho_\theta t_a=t_{\rho_\theta(a)}\rho_\theta \Rightarrow t_a\rho_\theta t_a\rho_\theta=t_a t_{\rho_\theta(a)}\rho_{2\theta}$.

$\because \theta=\pi$ $\therefore \rho_{2\theta}=id$ $\therefore t_a\rho_\theta t_a\rho_\theta=t_{a+\rho_\pi(a)}$.

▨



故 $a+\rho_\pi(a)=0$

$\therefore (t_a\rho_\theta)^2=id$

故 $t_a\rho_\theta$ 可以 $\in G$ 不违反 G 有限

Cayley Thm：群 G 的 $|G|=n$. 则 $G\cong S_n$ 子群

Proof：令 $T_a: G\to G$ （左平移）
$x\to ax$

则 T_a 为双射 同构. 设 $T=\{T_a. \forall a\in G\}$ 则 $T\le S_n$ $\begin{cases} T_aT_b=T_a(bx)=abx=T_{ab}\in T. \\ \text{单位元：} T_e\in T \\ \text{逆元：} (T_a)^{-1}=T_{a^{-1}}\in T \end{cases}$

则作 $\sigma: a\mapsto T_a$ 则 σ 为双射、同构
$G\to T$ $\quad \hookrightarrow \sigma(ab)=T_{ab}=T_aT_b=\sigma(a)\sigma(b)$

$\therefore G\cong T$ 即 S_n 一个子群. 记 T 为左正则表示群 ▨

"如何确定 S_n 的一个正规子群？".

Ⅰ. $a. b\in G$. 若 $\exists g\in G$ s.t. $b=gag^{-1}$ 则 $a. b$ 相似（共轭） 记作"$a\sim b$" 不相似记"$a\nsim b$".

Ⅱ. 左陪集：$H\le G$ 作 $aH=\{ah, \forall h\in H\}$ $(a\in G)$ $\to$ 若 $aH\cap bH\neq\phi \Rightarrow$ 必有 $aH=bH$"

右陪集：$H\le G$ 作 $Ha=\{ha. \forall h\in H\}$. $(a\in G)$.

$\Downarrow$

取"$ah_1=bh_2$".

$\Rightarrow a=bh_2h_1^{-1} \Rightarrow b^{-1}a=h_2h_1^{-1}\in H$.

$\forall h$. $ah=bh_2h_1^{-1}h\in bH$

$\therefore aH\subset bH$

同理 $bH\subset aH$ $\Big\}$ $aH=bH$

$\therefore \{H, a_1H, a_2H, \cdots\}$ 为 H 的左陪集群

$\Rightarrow G=\bigcup\limits_{a\in G} aH=a_1H\cup a_2H\cup\cdots\cup a_nH$. 记 n 为 H 在 G 下指数.
$\hookrightarrow$ 不交并 $\quad\hookrightarrow [G:H]$

$\Rightarrow$ Lagrange：$|H|\,\big|\,|G|$. $(|aH|=|H|)$

$(|G|=[G:H]\,|H|)$

$\forall x\in G$. $O_x=\{g^{-1}xg \mid g\in G\}$. 为 x 的"一个轨道" 也称 x 的"共轭类"

注：$x\sim y \Leftrightarrow O_x=O_y$ 且 $O_x\cap O_y=\underset{\hookrightarrow x\nsim y}{\phi}$ or $\underset{\hookrightarrow x\sim y}{O_x}$

注 ① $O_e=\{e\}$
② x 为中心元 $\Rightarrow O_x=\{x\}$.
③ $g^{-1}O_xg=O_x$.

∵. $N\lhd G$. 则 $\forall g\in G$. $g^{-1}ng=N$

$\Rightarrow$ "$N=\bigcup\limits_{g\in G} g^{-1}ng=\bigcup\limits_{x\in N} O_x$." （正规子群 $N\lhd G \Leftrightarrow \forall g\in G^{+}$. $g^{-1}Ng=N$）

$\Rightarrow$ 正规子群即为 G 中一些轨道的并 $\left(N=\bigcup\limits_{g\in G}\bigcup\limits_{n\in N} g^{-1}ng=\bigcup\limits_{n\in N}\left(\bigcup\limits_{g\in G} g^{-1}ng\right)=\bigcup\limits_{n\in N} O_n\right)$

Ex：
∵任一置换可由轮换生成（引）

$\Rightarrow \alpha=(a_{11}\cdots a_{1j})(a_{21}\cdots a_{2l})\cdots(a_{k1}\cdots a_{km})$. （不交积）.

则去括号后为 $1\sim n$ 的一个排列

$\Rightarrow (264)(13)(5) \Rightarrow 264135$

$\forall r\in S_n$. 则 $r\alpha r^{-1}=(r(a_{11})\cdots r(a_{1j}))\cdots\cdots(r(a_{k1})\cdots r(a_{km}))$. —— $(*)$

Def：n 元置换的循环分解中 长度为 l 的轮换个数记为 $\lambda_l(\alpha)\in N$.

称为 α 的第 l 个型函数. 其中 $(\lambda_1, \lambda_2, \cdots, \lambda_n)$ 称为型 $(\lambda_1+2\lambda_2+\cdots+n\lambda_n=n)$.

$\Rightarrow S_n$ 中. $r\alpha r^{-1}=\beta \Leftrightarrow \lambda_l(\alpha)=\lambda_l(\beta)$. $\forall l\in N$.

Proof："$\Rightarrow$" 由 $(*)$ 即知.

"$\Leftarrow$" $r=\begin{pmatrix} a_{11}\cdots a_{1j}, a_{21}\cdots a_{2l}, \cdots, a_{k1}\cdots a_{km} \\ b_{11}\cdots b_{1j}, b_{21}\cdots b_{2l}, \cdots, b_{k1}\cdots b_{km} \end{pmatrix} \Rightarrow r\alpha r^{-1}(b_{11})=r\alpha(b_{1j})=b_{1j}=\beta(b_{11})$

同理：$r\alpha r^{-1}=\beta$. ▨

Def：整数 n 的一个划分指"序列"$(a_1\cdots a_l)$

满足：$\begin{cases} a_1\ge a_2\ge\cdots\ge a_l \\ a_1+a_2+\cdots+a_l=n. \end{cases}$ $(a_i\in N)$

Ex：5 的划分

Ex：求 S_3 的正规子群

注：型为 $(\lambda_1, \cdots, \lambda_l)$ 的置换个数为 $\dfrac{n!}{\lambda_1!\cdots\lambda_l!\cdot 1^{\lambda_1}2^{\lambda_2}\cdots l^{\lambda_l}}$.

Ex：求 S_4 的正规子群：

$|S_4|=24$. 则 $|N|=2.3.4.6.8.12$.

对 4 分划：

① (1). $O_{(1)}=(1)$. 型为 $(4,0,0,0)$ 1个

② $(12)(34)$ 型：$(0,2,0,0)$ $O_{(12)(34)}$ 3个

③ $(12)(3)(4)$ 型：$(2,1,0,0)$ $O_{(12)(3)(4)}$ 6个

④ $(123)(4)$ 型 $(1,0,1,0)$ $O_{(123)(4)}$ 8个

⑤ (1234) 型 $(0,0,0,1)$ $O_{(1234)}$ 6个

$\therefore N=(①\cup②)$ or $(①\cup④\cup②=A_4)$

$\hookrightarrow A_n\lhd S_n$（由 $[S_n:A_n]=2$）.

3. 同态

Def: $\phi: (G,\cdot) \longrightarrow (H,\times)$

if $\phi(xy) = \phi(x)\times\phi(y) \Rightarrow \phi$ 为同态

$\begin{cases} Im\phi = \{\phi(g),\ \forall g\in G\} & \text{称为像} \\ ker\phi = \{g,\ \phi(g) = e_H\} & \text{称为核} \end{cases}$

1. $\begin{cases} \phi\text{单} \Leftrightarrow ker\phi = \{e_G\} \\ \phi\text{满} \Leftrightarrow Im\phi = H. \end{cases}$

2. $\phi(e_G) = e_H$. $\phi(a^{-1}) = \phi^{-1}(a)$

Proof: 先证2:

$\because \phi(e_G)e_H = \phi(e_G) = \phi(e_G\cdot e_G) = \phi(e_G)\cdot\phi(e_G)$.

$\Rightarrow \phi(e_G) = e_H$

又 $\begin{cases} \phi(a^{-1})\cdot\phi(a) = \phi(e_G) = e_H \\ \phi(a)\cdot\phi(a^{-1}) = \phi(e_G) = e_H \end{cases} \Rightarrow \phi(a^{-1}) = \phi^{-1}(a)$

再证1: I. "$\Rightarrow$" ϕ单时. $\forall a\in ker\phi$

$\therefore \phi(a) = \phi(e) = e_H$ 故 $a = e_G$ $\therefore ker\phi = \{e_G\}$

"$\Leftarrow$" $ker\phi = \{e_G\}$ 时.

$\forall \phi(g) = \phi(h) \Rightarrow \phi(gh^{-1}) = e_H \Rightarrow gh^{-1} = e_G \Rightarrow g = h$. 故$\phi$单.

II. "$\Rightarrow$" ϕ满时 $\forall k\in H$. 有 $k = \phi(\theta)$.

故 $H \subset Im\phi$. 又 $Im\phi \subset H \Rightarrow Im\phi = H$.

"$\Leftarrow$" 此时 $\forall k\in H$ $\because H = Im\phi$. $\therefore \exists\theta\in G$ s.t. $k = \phi(\theta)$ 故ϕ满 ■

Ex1. $\phi: GL_n(R) \longrightarrow (R^*,\cdot)$
$A \longrightarrow |A|$.

$\Rightarrow$ ① $ker\phi = SL_n(R)$

② $Im\phi = R^*$. ($\forall k\in R^*$. 令 $A = \begin{bmatrix} k & \\ & E_{n-1} \end{bmatrix}$ 即可).

③ $\phi(A\cdot B) = |AB| = |A||B| = \phi(A)\cdot\phi(B)$

$\therefore \phi$为满同态.

Ex2. $\phi: (R^*,\cdot) \longrightarrow GL_n(R)$.
$r \longrightarrow rI_n$.

$\Rightarrow$ ① $ker\phi = 1$. 注意 $e_{R^*} = 1$.

② $Im\phi = \{rI_n\}$

③ $\phi(k\cdot h) = (k\cdot h)I_n = kI_n\cdot hI_n = \phi(k)\cdot\phi(h)$.

故ϕ为单同态.

Ex3. 嵌入同态: $\phi: H \to G$ 为单同态
$(H\le G)$ $h \to h$.

Ex4. 典范同态: $\phi: G \to G/H$. 为满同态
$(H\trianglelefteq G)$ $a \to aH$

且 $ker\phi = H$.

Ex5. $\phi: (R,+) \to (R^*,\cdot)$. 为同构. $\begin{cases} e_{(R,+)} = 0 \\ e_{(R^*,\cdot)} = 1 \end{cases}$
$a \to e^a$

$\begin{cases} ker\phi = 0,\ \text{而 } e_{(R,+)} = 0. \\ Im\phi = R^*\ (\forall k\in R^*.\ \text{令 } a = \ln k). \\ \phi(a+b) = e^{a+b} = \phi(a)\cdot\phi(b) \end{cases}$

Ex6. $\phi: (R,+) \to (S^1,\cdot)$ $S^1 \triangleq \{z\in\mathbb{C} \mid |z| = 1\}$. $\begin{cases} e_{(R)} = 0 \\ e_{(S,\cdot)} = 1. \end{cases}$
$a \to e^{2\pi ai}$

$\begin{cases} Im\phi = S^1. \\ ker\phi = \mathbb{Z} \end{cases}$ $(e^{2\pi ai} = \cos 2\pi a + i\sin 2\pi a)$

Ex7. $sgn: S_n \to \{-1,1\}$.

$sgn(\sigma) = \begin{cases} 1 & \sigma\text{为偶} \\ -1 & \sigma\text{为奇} \end{cases}$

故 $\begin{cases} sgn(\sigma\cdot\tau) = sgn(\sigma)sgn(\tau) \\ ker\ sgn = A_n. \\ Im\ sgn = \{-1,1\}. \end{cases}$

3. ϕ为 $G \to H$ 的同态

则 $\begin{cases} Im\phi \le H \\ ker\phi \trianglelefteq G. \end{cases}$

Proof: ① $Im\phi \le H$: $\forall g,h\in Im\phi$ $\Rightarrow Im\phi \le H$.

$\because g = \phi(a), h = \phi(b) \Rightarrow gh^{-1} = \phi(ab^{-1}) \in Im\phi$.

② $ker\phi \trianglelefteq G$: $\forall g\in G \Rightarrow \phi(g\,ker\phi\,g^{-1}) = \phi(g)\phi(ker\phi)\phi(g^{-1})$

$= \phi(g)\cdot e\cdot\phi(g^{-1}) = e$ 故 $g\,ker\phi\,g^{-1} \subseteq ker\phi$

$\therefore ker\phi \trianglelefteq G$ ■

4. First. Thm: ① if $H\trianglelefteq G$ 则 $\phi: G \to G/H$ 为满同态
$g \to gH$

② 且 $G/ker\phi \cong Im\phi \triangleq \overline{G}$.

Proof: ①: $\begin{cases} \phi(g_1g_2) = g_1g_2H. \\ \phi(g_1)\phi(g_2) = g_1H\,g_2H. \end{cases}$

故 $g_1g_2H \subset g_1H\cdot g_2H$ (右边第一个H取e).

$g_1H\cdot g_2H = g_1g_2H\cdot H \subset g_1g_2H$ ($Hg_2 = g_2H$, $H\cdot H \subseteq H$)

故 $\phi(g_1g_2) = g_1g_2H = g_1H\cdot g_2H = \phi(g_1)\cdot\phi(g_2)$

故ϕ为同态. 显然为满.

②. 作 θ: $G/ker\phi \to Im\phi$.
$a\,ker\phi \to \phi(a)$.

则: $\begin{cases} ker\theta = ker\phi.\ (\text{注意 } e_{G/ker\phi} = ker\phi) \\ Im\theta = Im\phi \\ \theta(a\,ker\phi\cdot b\,ker\phi) = \theta(ab\,ker\phi) = \phi(ab) \end{cases}$

$\phi(a)\cdot\phi(b) = \theta(a\,ker\phi)\cdot\theta(b\,ker\phi)$.

故θ为同构. $\therefore G/ker\phi \cong Im\phi$ ■

5. $\phi: G \to G'$ 同态 则 $\forall a\in G$. $a' = \phi(a)$.

则: $\{\phi^{-1}(a')\} = a\,ker\phi$

Proof: $\forall c\in\phi^{-1}(a')$ 故 $\phi(c) = a' = \phi(a)$

$\therefore \phi(a^{-1}c) = e \Rightarrow a^{-1}c\in ker\phi \Rightarrow c\in a\,ker\phi$. 故 $\phi^{-1}(a') \subset a\,ker\phi$.

又 $\phi(a\,ker\phi) = \phi(a)\cdot\phi(ker\phi) = \phi(a) = a'$

$\therefore a\,ker\phi \subset \phi^{-1}(a')$ 故 $\phi^{-1}(a') = a\,ker\phi$ ■

6. $\varphi: G \to G'$ 同态.

则 ① $H\le G \Rightarrow \varphi(H) \le G'$

② $H' \le G' \Rightarrow \varphi^{-1}(H') \le G$

Proof: ①: $H\le G$时.

$\forall \varphi(h)、\varphi(g)$ 对: $\varphi(h)\varphi^{-1}(g) = \varphi(hg^{-1})$

$\because hg^{-1}\in H$ $\therefore hg^{-1} = k$

$\therefore \varphi(h)\cdot\varphi^{-1}(g) = \varphi(k) \subset \varphi(H)$

故 $\varphi(H) \le G'$

②. $\forall a.b\in\varphi^{-1}(H')$ 故 $\varphi(a).\varphi(b)\in H'$.

对: $\varphi(ab^{-1}) = \varphi(a)\varphi^{-1}(b) \in H'$

$\therefore ab^{-1}\in\varphi^{-1}(H') \Rightarrow \varphi^{-1}(H') \le G$. ■

7. Second Thm: 设ϕ为 $G \to \overline{G}$ 的满同态, $H = ker\phi$.

令 $\mathcal{L}(G,H) = \{G\text{中包含}H\text{的子群}\}$

$\mathcal{L}(\overline{G}) = \overline{G}$中所有子群

则: ① $\theta: \mathcal{L}(G,H) \to \mathcal{L}(\overline{G})$ 为双射.
$S \longmapsto \phi(S) = \overline{S}$

②. $S \supset T \Leftrightarrow \phi(S) \supset \phi(T)$

③. $S \trianglelefteq G \Leftrightarrow \phi(S) \trianglelefteq \overline{G}$

④ $S\trianglelefteq G$. 有 $G/S \cong \overline{G}/\overline{S} = \left(\dfrac{G/H}{S/H}\right)$

Proof: ①单. $\phi(S) = \phi(T)$时.

$\forall \phi(s)\in\phi(S)$. $\exists t$. $\phi(s) = \phi(t)$ 又ϕ满 $\Rightarrow s\in T\cdot ker\phi = TH = T$ $(H\subset T)$

$\therefore s\in T$ $\therefore S\subset T$ 同. $T\subset S \Rightarrow S = T$ $\therefore\theta$为单

满: $\because \phi(S) = \{\phi(s),\ s\in S\}$.

故 $\forall \phi(S)\in\mathcal{L}(\overline{G})$. 自变量组成 $\phi^{-1}(\phi(S)) \triangleq S'$

下证 $H\subset S'$. $S'\le G$. 由 $\phi(S) \le \overline{G}$ 及 6 中结论 $\Rightarrow S'\le G$.

只需证 $H\subset S'$! 由于 $e\in\phi(S)$. 故 $H\subset S'$. $\therefore\theta$为满.

θ为双射.

②. 略

③ "$\Rightarrow$" $S\trianglelefteq G$时. $\forall g\in\overline{G}$. $g = \phi(k)$.

$\therefore$ 对: $g\phi(S)g^{-1} = \phi(kSk^{-1})$.

又 $S\trianglelefteq G$. $\therefore kSk^{-1}\subset S$.

$\therefore \phi(kSk^{-1}) \subset \phi(S)$. 故 $\phi(S) \trianglelefteq \overline{G}$.

"$\Leftarrow$" $\phi(S) \trianglelefteq \overline{G}$时: $\forall g\in G$. $g' = \phi(g)\in\overline{G}$

对: $g'\phi(S)\cdot g'^{-1} = \phi(g\cdot Sg^{-1}) \subset \phi(S)$

故 $g\cdot S\cdot g^{-1}\subset S$. $\therefore S\trianglelefteq G$

④ 先说明: $\overline{G}/\overline{S} = \dfrac{G/H}{S/H}$. 与 G/S 对比.

$G \xrightarrow{\pi} \underset{=\overline{G}}{G/S} \xrightarrow{\psi} \overline{G}/\overline{S}$

$\therefore \pi、\psi$为满 $\Rightarrow \psi\circ\pi$为满

即 $Im\,\psi\circ\pi = \overline{G}/\overline{S}$.

$ker\,\psi\circ\pi = \pi^{-1}(ker\psi) = \pi^{-1}(\overline{S}) = S$.

故 $\underset{\displaystyle \overset{\parallel}{G/S}}{G/ker\,\psi\circ\pi} \cong Im\,\psi\circ\pi = \overline{G}/\overline{S}$ ■

8. Third Thm. 设 $N\trianglelefteq G$. $\forall H\le G$. 则: $H/H\cap N \cong HN/N$

Proof: $\pi: G \to G/N = \overline{G}$

则 $\overline{H} = \pi(H) \le \overline{G}$

$\pi^{-1}(\overline{H}) = H\,ker\pi = HN \Rightarrow \overline{H} \cong HN/N$.

又作限制 $\pi|_H: H \to \overline{H}$.

$ker(\pi|_H) = ker\pi \cap H = H\cap N$.

$Im(\pi|_H) = \overline{H}$ 故 $\overline{H} \cong H/H\cap N$.

故 $\overline{H} \cong HN/N \cong H/H\cap N$ ■

5. 有限群

Lagrange. $H\le G$. $|H|=m$. $|G|=n \Rightarrow m\mid n$

问 Lagrange 逆命题是否成立?

即: $\forall m\mid n$. $\exists$? H. $|H|=m$. $H\le G$. $(n=m\cdot t)$.

(不一定)

1. $G=\langle a\rangle$. $|a|=|G|=n$. 则令 $H=\langle a^t\rangle$. $b=a^t$.

P: 则 $(a^t)^m=a^n=e$. 且 $\forall l<m$. $(a^t)^l=a^{tl}\ne e$. $(tl<tm=n)$

故 $|a^t|=m$. 故 $|H|=m$. (或 $|a^t|=\frac{n}{(t,n)}=\frac{n}{t}=m$). $\blacksquare$

2. G 为有限交换? p 为素数

其中 $|G|=n=p\cdot m$. 则 G 中必存在阶为 p 的元素

P: 归纳: ① $m=1$. $|G|=p$. 则 G 为"循环群"

则 $G=\langle a\rangle$ ($\because |a|\mid |G|=p \Rightarrow |a|=1$ or p 故 $G=\langle a\rangle$).

② $m>1$. 设 $a\in G$. $a\ne e$. 令 $H=\langle a\rangle$.

I. $p\mid |H|$. 故由 1. H 中存在 b s.t. $|b|=p$.

$\therefore b\in H\le G \Rightarrow b\in G$.

II. $p\nmid |H|$. 由于交换群子群均为正规

故令 $\bar G=G/\langle a\rangle=G/H$.

$|\bar G|=|G|/|\langle a\rangle|=pm'$. $0<m'<m$.

由归纳. 在 $\bar G$ 中存在 $\bar b$. s.t. $|\bar b|=p \Rightarrow b^p\in\langle a\rangle=H$.

设 $|H|=s$. 对 $(b^s)^p=(b^p)^s=e$

故设 b 的阶为 r. $b^r=e$. 则 $|b^s|=\frac{r}{(r,s)}$

$\Rightarrow p\mid\frac{r}{(r,s)} \Rightarrow r=p(r,s)k$

又 $p(r,s)k<pm \Rightarrow$ 对于 $\langle b\rangle=H'$. 存在 c, s.t. $|c|=p$.

$\therefore c\in H'\in G$. $\blacksquare$

(或当证到 $(b^s)^p=e$ 时 故 $|b^s|\mid p$ 又 p 素数

$\Rightarrow |b^s|=1$ or p. 又 $|b^s|=1$ 时. 则 $b^s=e$

$\because p\nmid |H|$. 故 $(p,s)=1 \Rightarrow 1=pu+sv$.

故 $b=b^{pu}$ $\because b^p\in H$ 故 $b\in H$. 下证 $b\notin H$:

若 $b\in H$ 时. $bH\subset H$. 故 $|\bar b|\ne p$. 矛盾!

故 $|b^s|=p$ 且 $b^s\in G$.) $\blacksquare$

3. G 有限交换 $|G|=n$. 则 $\forall m\mid n$. $\exists H$. $H\le G$. s.t. $|H|=m$.

P: 对 m 归纳: ① $m=1$ 令 $H=\langle e\rangle$.

② $m>1$ 时. 取素数 $p\mid m$. 则由 2.

G 中存在阶为 p 的元素 a.

对 $\bar G=G/\langle a\rangle$ $|\bar G|=n/p$ 且 $m/p\mid n/p$.

故 $\bar G$ 中存在子群 $\bar H$. s.t. $|\bar H|=m/p$.

对 π: $G\longrightarrow\bar G$. $\pi(\pi^{-1}(\bar H))=\bar H$.

$b\longrightarrow b\langle a\rangle$.

对 $\pi^{-1}(\bar H)\le G$. 且 $\langle a\rangle\subseteq\pi^{-1}(\bar H)$.

记 $\pi^{-1}(\bar H)=H$. 作 π 限制 $\pi|_H$.

则 $\ker\pi|_H=H\cap\ker\pi=H\cap\langle a\rangle=\langle a\rangle$.

$\mathrm{Im}\,\pi|_H=\bar H \Rightarrow H/\langle a\rangle\cong\bar H$

故 $|H|=|\bar H|\cdot|\langle a\rangle|=m/p\cdot p=m$. $\blacksquare$

Now. 设 G 为普通的有限群?

Def. $S\subseteq G$. $N(S)=\{g\in G\mid gSg^{-1}=S\}$ 记为 S 的正规化子.

$\Rightarrow N(S)\le G$ $\{O_a=\{gag^{-1}\mid g\in G\}$ 为 a 轨道 or 共轭类

对 $a\in C(G)$ (中心) 有: $N(a)=G$. $O_a=\{a\}$.

且 $S\le G$ 有: $\boxed{S\lhd N(S)}$

4. G 为有限群. S 为 G 的一个共轭元素类, $|S|=t$. 则 $\exists H\le G$

s.t. $[G:H]=t$.

P: 作 φ: $G/N(S)\to S$.

$a\cdot N(S)\to aSa^{-1}$

故 $xSx^{-1}=ySy^{-1}\Leftrightarrow(x^{-1}y)S(x^{-1}y)^{-1}=S\Leftrightarrow x^{-1}y\in N(S)\Leftrightarrow x,y\in aN(S)$.

故 $xN(S)=yN(S)\Rightarrow\varphi$ 双射.

则 $|G|/|N(S)|=|S|\Rightarrow[G:N(S)]=|S|=t$. $\blacksquare$

5. 西罗定理: G 为有限群. $|G|=n=p^r m$. p 为素. 则 $\exists H\le G$.

s.t. $|H|=p^r$.

P: ① 设 $C(G)=G$. 即 G 为交换群.

由于 $p^r\mid n$. 故由 3. 知 $\exists H\le G$. $|H|=p^r$.

② 设 $C(G)\le G$

I. $p\mid |C(G)|$. 则由于 $C(G)$ 为交换群 $\Rightarrow$ 由 3. 知 $\exists$ 阶为 p 的元素 a.

作 $\langle a\rangle$. 则对 $\underbrace{\bar G=G/\langle a\rangle}_{(|G|=p^r m)}$. 由归纳 $\bar G$ 中 $\exists\bar H$. $|\bar H|=p^{r-1}$

故 $|H|=|\langle a\rangle||\bar H|\to p^r$.

II. $p\nmid |C(G)|$.

由于 $|G|=n=|C(G)|+\sum_i^t|O_i|$ $|O_i|$ 记为 n_i. (类方程).

故 $\exists j$. s.t. $p\nmid n_i$.

由 $|O_i|=n_i\Rightarrow\exists N\le G$. s.t. $[G:N]=|O_i|=n_i$.

$\therefore p^r m=|G|=|N|\cdot[G:N]\Rightarrow p^r\mid |N|$.

由归纳. $\exists H\le N\le G$. s.t. $|H|=p^r$. $\blacksquare$

Def: 有限 p-群: 每个元素的阶都是 "p 的幂次".

则 $\Leftrightarrow |G|$ 为 p 的幂. (p^n).

P: "$\Leftarrow$" $|G|=p^n$. 由 Lagrange: $\forall |a|$. $|a|\mid p^n\Rightarrow |a|=p^k$.

"$\Rightarrow$" $|G|=p_1^{r_1}p_2^{r_2}\cdots p_t^{r_t}$.

则 $\exists$ 阶为 p_i^r 的子群 H. 由于 $|H|=p^k$. 故 $\forall a\in H$. $|a|\mid p^k$

故 $|G|=p^n$. $\Rightarrow p=p_i\Rightarrow p_i\equiv p$. $\blacksquare$