def: group H.G isomorphic (同构) 若 $\exists$ bijective $\phi: G\to H$ L3

$\phi(g_1 g_2)=\phi(g_1)*\phi(g_2)$ "·, *" 为G.H的对应群运算

ϕ is homomorphism if $\phi(ab)=\phi(a)\phi(b)$. preserve the group operation, 运算符省略了

若 ϕ is surj & inj. $\Rightarrow$ isomorphism

例: $G=\{\begin{pmatrix}1&c\\0&1\end{pmatrix}: c\in\mathbb{F}_p\}$ with dot product (默认), $H=(\mathbb{F}_p,+)$

$\phi: G\to H$, $\phi:\begin{pmatrix}1&c\\0&1\end{pmatrix}\to c$

$\phi[\begin{pmatrix}1&c_1\\0&1\end{pmatrix}\begin{pmatrix}1&c_2\\0&1\end{pmatrix}]=c_1+c_2=\phi\begin{pmatrix}1&c_1\\0&1\end{pmatrix}+\phi\begin{pmatrix}1&c_2\\0&1\end{pmatrix}$; ϕ is isomorphism

对于一般的homomorphism $\phi: G\to H$; G is homomorphic to H ;

pro: ①: $\phi: e\in G\to e\in H$;

let $b=e\in G$. $\phi(ab)=\phi(a)=\phi(a)*\phi(e)$ $\forall a\in G$

$\phi(a)\in H$ ∴ $\exists$ 逆元 $\phi(a^{-1})=\phi(a)^{-1}$ $\Rightarrow e=\phi(e)$

② 若 $|\langle g\rangle|$ finite, $|\langle\phi(g)\rangle| \,\big|\, |\langle g\rangle|$

$|\langle g\rangle|$ finite, 则 $\exists n: g^n=e$

∴ $e=\phi(g^n)=(\phi(g))^n$; $\phi(g)$ 也为循环子群生成元

$|\langle\phi(g)\rangle|$ 可能是n, 也可能 $\frac{n}{m}$ for $m\in\mathbb{Z}$. ∴ $|\langle\phi(g)\rangle| \,\big|\, |\langle g\rangle|$

def: 将 $\phi(G)$ 记为 $\mathrm{im}\,\phi$;

将 e 的原像记为 $\ker\phi$, (ϕ的核) $=\{g\in G: \phi(g)=e\in H\}$; $\ker\phi\le G$ 易知

③: $\phi(a)=\phi(b)\Leftrightarrow a\ker\phi=b\ker\phi\Leftrightarrow ab^{-1}\in\ker\phi$

LHS $\Rightarrow$ $\begin{cases}\text{则 } \phi(a\cdot b^{-1})=\phi(e)=e=\phi(a)*\phi(b)\\ \phi(a\cdot a^{-1})=\phi(a)*\phi(a^{-1}),\ \text{即 } \phi(a^{-1})=\phi^{-1}(a)\end{cases}$

def: homo $\phi(g)=g'$, 则 $\phi^{-1}(g')=\{x\in G: \phi(x)=g'\}=g\ker\phi$

th: $\varphi: G\to H$ homo, then $\mathrm{im}\,\varphi\le H$, $\ker\varphi\trianglelefteq G$.

(1): $\varphi(g_1g_2)=\varphi(g_1)*\varphi(g_2)$; $\mathrm{im}\,\varphi=\{\varphi(g): g\in G\}$ "close" 由 φ 的定义易知

$\varphi(e)=\varphi(g_1)*\varphi(g_1^{-1})$ ∴ for $\varphi(g_1)\in\mathrm{im}\,\varphi$, 逆元存在, 且也封闭 $\Rightarrow$ subgroup

(2): $\ker\varphi=\{g\in G: \varphi(g)=e\in H\}$

$\varphi(g^{-1}kg)=\varphi(g^{-1})*\varphi(k)*\varphi(g)=\varphi(g^{-1})*\varphi(g)=\varphi(g^{-1}\cdot g)=e$ $\forall g\in G, k\in\ker\varphi$

∴ $\forall g.k$ $g^{-1}kg\in\ker\varphi\Rightarrow$ normal th: ① $\varphi: G \to H$ is homo; $G/\ker\varphi \cong \mathrm{im}\varphi$ ($H=\mathrm{Im}\varphi \Leftrightarrow \varphi$ is surj)

(类比: 线性映射基本定理, range.null → whole space)

def: $\Phi: G/\ker\varphi \to \mathrm{im}\varphi$, $\Phi(a\ker\varphi) \to \varphi(a)$

for $b \in \ker\varphi$ $\Phi(a\ker\varphi) = \Phi(ab\ker\varphi) = \varphi(ab) = \varphi(a) * \varphi(b) = \varphi(a)$

(输出与自变量的表示形式无关 1值"对应值) $\Rightarrow$ well-defined ⋯①

$\Phi(a_1\ker\varphi \cdot a_2\ker\varphi) = \Phi(a_1a_2\ker\varphi) = \varphi(a_1 \cdot a_2) = \varphi(a_1) * \varphi(a_2) = \Phi(a_1\ker\varphi) * \Phi(a_2\ker\varphi)$

$\Rightarrow \Phi$ is homo ⋯②

$a_1\ker\varphi \cdot a_2\ker\varphi = \{a_1h_1 \cdot a_2h_2 : h_1, h_2 \in \ker\varphi\}$

$= \{a_1h_1a_1^{-1} \cdot a_1a_2h_2 : h_1, h_2 \in \ker\varphi\}$ since $a_1h_1a_1^{-1} \in \ker\varphi$ by "normal"

$= \{h_1'a_1a_2h_2 : h_1', h_2 \in \ker\varphi\}$

$\forall \varphi(a) \in \mathrm{im}\varphi$, $\exists a\ker\varphi$ as preimage of Φ $\Rightarrow$ surj ⋯③

if $\Phi(a_1\ker\varphi) = \Phi(a_2\ker\varphi)$; $\varphi(a_1) = \varphi(a_2)$

$\therefore \varphi(a_1) = \varphi(a_2) * \varphi(h) = \varphi(a_2h)$ for $h \in \ker\varphi$

$a_1 = a_2h$ for some $h \in \ker\varphi$ (反证很明显)

$\therefore a_1\ker\varphi = a_2\ker\varphi \Rightarrow$ inj ④

①+②+③+④: Φ iso; $G/\ker\varphi \cong \mathrm{Im}\varphi$

th: $G = AB = \{ab : a \in A, b \in B\}$, A, B 为 group, 且运算符可以不同?

why∃ $A \triangleleft G$, 则: $A \cap B \triangleleft B$, $AB \le G$; $G/A \cong B/A\cap B$?

(1): $x \in A \cap B$, $g \in B$; let $a = e$ $g \in G$

$g^{-1}xg \in A$ since $A \triangleleft G$; $g^{-1}, x, g \in B$ $\therefore g^{-1}xg \in B$ since B group

$\Rightarrow g^{-1}xg \in A \cap B$; $A \cap B \triangleleft B$

(2): def: $\Phi: B \to G/A$, $\Phi(b) = bA$

B运算未知道的部分, 但我们知道G/A运算定义

$\Phi(b_1b_2) = b_1b_2A$

$\Phi(b_1) * \Phi(b_2) = b_1A * b_2A = b_1b_2A$, 由为 G/A 群运算

$\Rightarrow \Phi$ homo

th: $B/\ker\varphi \cong \mathrm{im}\varphi$) φ 即 Φ

关注所在群 & 运算性质! $\Rightarrow$ $\mathrm{im}\varphi = \{bA : b \in B\} = \{A * bA : b \in B\} = \{aA * bA : b \in B, a \in A\}$ $= \{abA : b \in B, a \in A\} = G/A$

$\ker\varphi = \{b \in B : \Phi(b) = e \in G/A\} = \{b \in B : \Phi(b) = bA = A\} = A \cap B$

$\therefore B/A\cap B \cong G/A$

th: G is group, $H \triangleleft G$, $K \le G$ 则 $H \triangleleft HK$ (2) 以有(3)

(1): $HK \le G$, $H\cap K \triangleleft K$ (2): $(HK)/H \cong K/(H\cap K)$; 事实仅有 $H, K \le G$, 也有 $|HK| = \frac{|H|\cdot|K|}{|H\cap K|}$

1.1, identity 存在, Associate 存在显然.

$h_1k_1\cdot h_2k_2 = h_1\underline{k_1\cdot h_2k_1^{-1}}\cdot \underline{k_1k_2} = h_2h_3\cdot k_3 = h_4\cdot k_3$ for some $h_4 \in H$, $k_3 \in K$, since $H\triangleleft G$, $H, K \le G$

for $\forall h_1k_1 \in HK$ $k_1^{-1}h_1^{-1} = \underline{k_1^{-1}h_1^{-1}k_1}\cdot k_1^{-1} = h_2\cdot k_1^{-1}$ for some $h_2 \in H$ $\Rightarrow$ HK closed

$\therefore (h_1k_1)^{-1} \in HK$ $\forall h_1k_1 \in HK$ $\Rightarrow$ inverse

$\therefore HK \le G$ ($H\le G$, $K\le G$ 时 $HK=KH \Leftrightarrow HK \le G$; 此处 $H\triangleleft G$ 非充要条件强于 $H \le G$)

1.2, $\forall x \in H\cap K$, $k \in K$

$k^{-1}xk \in H$ since $H \triangleleft G$, $x\in H$, $k \in G$; $k^{-1}xk \in K$ since $x \in K$, K is closed

(2): 基本同态定理: $\varphi: D \to$ some set   从 $K \to (HK)/H$ 更清楚, $H\cap K$ 为 ker

$D/\ker\varphi \cong \operatorname{im}\varphi$ if φ is homo; 在此处 $D = HK$ $\ker\varphi = H$

$\therefore$ define $\varphi: HK \to K/(H\cap K)$, $\varphi(hk) = k(H\cap K)$

$\varphi(hk) = H\cap K \Leftrightarrow hk \in H$ 推出 φ $\Leftrightarrow k \in H$

$\varphi(h_1\underbrace{k_1h_2}k_2) = \varphi(h_3k_3) = k_3(H\cap K)$

$\varphi(h_1k_1)\cdot\varphi(h_2k_2) = k_1(H\cap K)\cdot k_2(H\cap K) = k_1k_2(H\cap K)$

...

if $h_1k_1 = h_2k_2$, $k_1k_2^{-1} = h_1^{-1}h_2$,

$k_1k_2^{-1} \in K$, $h_1^{-1}h_2 \in H$ $\therefore k_1k_2^{-1} = h_1^{-1}h_2 \in (K\cap H)$

$\therefore \varphi(h_1k_1) = k_1(H\cap K) = k_1k_2^{-1}\cdot k_2(H\cap K) = k_1k_2^{-1}(H\cap K)\cdot k_2(H\cap K) = k_2(H\cap K) = \varphi(h_2k_2)$

$\Rightarrow$ well-defined …①

$K/H\cap K$ 的商群运算建立在"$H\cap K \triangleleft K$"条件上

证明 $k_3(H\cap K) = k_1k_2(H\cap K) \Leftrightarrow k_3 = k_1k_2\cdot x$ for some $x \in H\cap K$

$\Leftrightarrow k_3^{-1}k_1k_2 \in H\cap K$

$h_1k_1h_2k_2 = h_3k_3$

$\therefore h_1^{-1}h_3 = k_1h_2k_2k_3^{-1} = (k_1h_2k_1^{-1})k_1k_2k_3^{-1} = h_4k_1k_2k_3^{-1}$

$h_4^{-1}h_1^{-1}h_3 = k_1k_2k_3^{-1}$ $\therefore k_1k_2k_3^{-1} \in H\cap K$ …② homo