第3讲 正规子群，商群，群同态．核

关于陪集的两种看法：$H \leq G$ 子群

对 $a\in G$，记子集 $aH := \{ah \mid h\in H\}$

① $G/H = \{aH ; a\in G\}$ 是等价类的集合，即 $a \overset{R}{\sim} b$，若 $a^{-1}b\in H$.

② $G/H = \{aH ; a\in G\}$ 直接作为一些 G 的子集构成的集合.

$aH = bH$ 如果它们作为子集相等.

自由转换观点

<u>引理</u>：G 可以被化分为形如 aH $(a\in G)$ 这样的左陪集的无交并

只要证明：要么 $aH = bH$，要么 $aH\cap bH = \phi$.　（练习）.

如何指定一个陪集？

①可以指出其中一个元素 a，谈论它的等价类 aH.

若 $a \overset{R}{\sim} a'$，则 $aH = a'H$

自由转换观点.

②也可以直接看集合 aH，当然这个集合可能有不同写法.

· <u>记号</u>：若 $A,B\subseteq G$ 是群 G 的两个子集，记 $AB = \{ab \mid a\in A, b\in B\}$.

特别地，对子群 $H\leq G$　$H\cdot H = H$.

<u>定义</u> 称 G 的子群 H 为正规的，如果 $\forall a\in G$，$aH = Ha$ 作为子集相等

（这等价于 $\forall a\in G$，$aHa^{-1} = H$）←"更好"的定义

故一个 G 的子群 H 是<u>正规的</u> 当且仅当 H 所有的共轭都是它自己.

· <u>商群</u>：若 $H \trianglelefteq G$ 是一个正规子群．可以在陪集上定义乘法：

$$aH\cdot bH = a\cdot H b\cdot H \underset{\uparrow}{=} a\cdot bH\cdot H = abH.$$

正规性

显然，集合的乘法具有结合性．这给出了 G/H 上的一个群结构.

我们藏了什么？（如果用等价类操作）

希望定义 $G/H \times G/H \longrightarrow G/H$ 的乘法.

$$aH \times bH := abH.$$

但我们要验证这个定义是"良好定义"的！

即：若 $a \overset{R}{\sim} a'$，$b \overset{R}{\sim} b'$，则 $ab \overset{R}{\sim} a'b'$

$$\Downarrow$$

$$a' = a \cdot h_1,\ b' = b \cdot h_2$$

$$\Downarrow$$

$$a'b' = ah_1bh_2 = ab \cdot \underbrace{b^{-1}h_1b}_{\in H} \cdot \underbrace{h_2}_{\in H} \overset{R}{\sim} ab. \qquad \square$$

例子：$n \in \mathbb{N}$，$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} C_n = \{e, x, \dots, x^{n-1}\}$ ← $x^n = e$

$$i + n\mathbb{Z} \longleftrightarrow x^i$$

- 如何把 $\mathbb{Z}/n\mathbb{Z}$ "并在一起"？

考虑 $G := \mathbb{Q}/\mathbb{Z} = \{a + \mathbb{Z} \mid a \in \mathbb{Q}\}$ "$\approx \mathbb{Q} \cap [0,1)$" ← but not a good model.

- $\mathbb{Z}/n\mathbb{Z}$ 同构于 G 的一个子群！

$$\mathbb{Z}/n\mathbb{Z} \simeq \tfrac{1}{n}\mathbb{Z}/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}$$

$$i + n\mathbb{Z} \longleftrightarrow \tfrac{i}{n} + \mathbb{Z}$$

事实上，$\mathbb{Q}/\mathbb{Z} = \bigcup_n \frac{1}{n}\mathbb{Z}/\mathbb{Z}$

- 变种：p 为素数. $\mathbb{Z}[\frac{1}{p}] := \{\frac{a}{b} \mid a \in \mathbb{Z},\ b$ 是 p 的幂$\}$

$\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ 包含 $\frac{1}{p^r}\mathbb{Z}/\mathbb{Z} \simeq \mathbb{Z}/p^r\mathbb{Z}$.

且 $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z} = \bigcup_r \frac{1}{p^r}\mathbb{Z}/\mathbb{Z}$

- $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ 是"可除的"，即 $\forall g \in G$，$\forall n \in \mathbb{N}$，存在 $h \in G$ 使得 $g = n \cdot h$.

证：$g = \frac{a}{p^r} \overset{?}{=} n \cdot h$，若 $n = p^s$，则取 $h = \frac{a}{p^{r+s}}$

若 $(n,p)=1$. 则存在 $a' \equiv a \mod p^r$ 使得 a' 是 n 的倍数.

取 $h = \dfrac{a'/n}{p^r}$. $\square$

数学的发展需要借鉴:

线性空间	直和	子空间	线性同构	仿射空间 $v+W$	商空间	线性映射	像核
群	直积	子群	同构	陪集	商群	同态	像核

定义. 设 $(G,*)$ 和 $(H,\circ)$ 为两个群, 称映射 $\varphi: G\to H$ 为一个同态 (homomorphism)

如果 $\forall x,y\in G$, $\varphi(x*y)=\varphi(x)\circ\varphi(y)$

$\ker\varphi := \varphi^{-1}(e_H)$ 称为同态的核.

引理: (1) 同态的像 $\varphi(G)\leq H$ 是 H 的子群

(2) 同态的核 $\ker\varphi$ 是 G 的正规子群

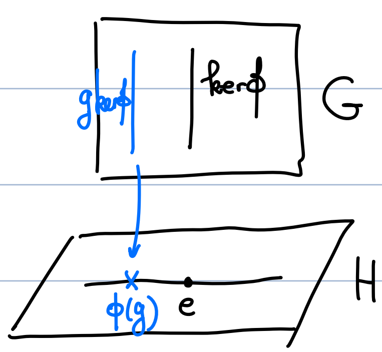
(3) 同态是单射当且仅当 $\ker\varphi=\{e_G\}$.

} 线性空间的类比.

更多的类比: 线性空间中. $f: V\to W$ 线性映射 $\Rightarrow V/\ker f \cong f(V)$

群的第一同构定理 如果 $\varphi: G\to H$ 是群同态, 则 $\ker\varphi \trianglelefteq G$ 且 $G/\ker\varphi \cong \varphi(G)$

示意图:



证明: 已证 $\ker\varphi \trianglelefteq G$ 是正规子群

定义映射 $\psi: G/\ker\varphi \longrightarrow \varphi(G)$

$$g\ker\varphi \longmapsto \varphi(g)$$

(1) 验证 ψ 是良好定义的

若 $g_1\ker\varphi = g_2\ker\varphi \overset{?}{\Longrightarrow} \varphi(g_1)=\varphi(g_2)$

$$\Downarrow$$

$g_1 = g_2 h$ 对某个 $h\in\ker\varphi$

$$\Downarrow$$

$\varphi(g_1)=\varphi(g_2)\varphi(h)=\varphi(g_2)$ ✓

(2) ψ是同态：$\psi(g_1\ker\phi \cdot g_2\ker\phi) \overset{?}{=} \psi(g_1\ker\phi)\cdot\psi(g_2\ker\phi)$

$$\psi(g_1\ker\phi \cdot g_2\ker\phi) = \psi(g_1g_2\ker\phi) = \phi(g_1g_2)$$

$$\psi(g_1\ker\phi)\cdot\psi(g_2\ker\phi) = \phi(g_1)\cdot\phi(g_2)$$

$$\phi(g_1g_2) = \phi(g_1)\cdot\phi(g_2) \quad ✓$$

(3) ψ是满射：显然，因为$\varphi(G)$中任何一个元素都形如$\varphi(g)=\psi(g\ker\phi)$

(4) ψ是单射．因ψ是同态，只需计算$\ker\psi$

$$\ker\psi = \{g\ker\phi \in G/\ker\phi \mid \underbrace{\phi(g)=e_H}_{\Downarrow\ g\in\ker\phi}\} = \{\ker\phi\} \Rightarrow \psi\text{是单射} \quad \square$$

综上 $\psi: G/\ker\phi \simeq \varphi(G)$． $\square$

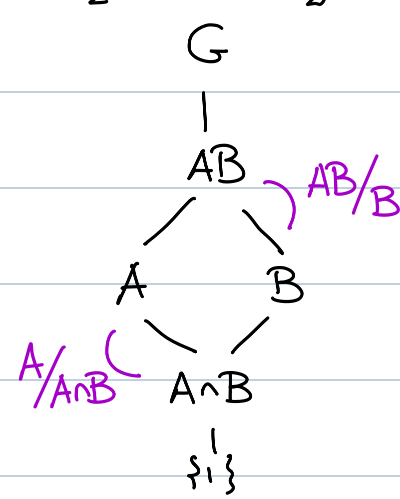
<u>群的第二同构定理</u>：类比线性空间 $W_1, W_2 \le V \Rightarrow \dfrac{W_1+W_2}{W_2} \simeq \dfrac{W_1}{W_1\cap W_2}$

在群G中，A，B是子群，B是正规子群

则 (1) AB是群G的子群

(2) $B \trianglelefteq AB$ 且 $A\cap B \trianglelefteq A$

(3) 我们有同构 $\dfrac{A}{A\cap B} \xrightarrow{\sim} \dfrac{AB}{B}$



证明：(1) 前面已证．

(2) 因为 $B \trianglelefteq G \Rightarrow \forall g\in G$，$gBg^{-1}=B$，而$AB\le G$，故$\forall g\in AB$，$gBg^{-1}$

我们可以如第一同构定理一样构造同构+验证良好定义……

但更好的方法是利用第一同构定理．

先构造<u>同态</u>：$\varphi: A \longrightarrow AB \longrightarrow AB/B$

$$a \longmapsto a \longmapsto aB$$

* φ是满射．AB/B中的陪集形如 $abB = aB = \varphi(a)$ ✓

* $\ker\varphi = \{a\in A, \underset{\Updownarrow\atop a\in B}{aB=B}\} = A\cap B$ （特别地，这说明 $A\cap B$ 在 A 中正规.）

应用第一同构定理得 $A/A\cap B \xrightarrow{\sim} AB/B$ □

注1：此题是一个标准使用第一同构定理的证明的例子：

即：要证 $G/H \xrightarrow{\sim} G'/H'$

* 首先构造同态 $\varphi: G\to G'/H'$（或有时通过 $G\to G'\to G'/H'$）
* 再证明 φ 是满射 + $\ker\varphi = H$.

用第一同构定理完成证明.

注2：此定理的条件 $B\trianglelefteq G$ 可弱化为 $\forall a\in A$, $aBa^{-1}=B$.

<u>群的第三同构定理</u>：类比线性空间 $U\subseteq W\subseteq V \Rightarrow W/U \subseteq V/U$ 是子空间，且 $\dfrac{V/U}{W/U}\cong V/W$.

设 G 是一个群 $H\trianglelefteq G$, $K\trianglelefteq G$ 且 $H\leq K$.

则 $K/H \trianglelefteq G/H$ 且 $\dfrac{G/H}{K/H}\simeq G/K$

证：考虑 $\phi: G/H \longrightarrow G/K$

$$gH \longmapsto gH\cdot K = gK \quad \text{直接良好定义}$$

* ϕ 是同态：$\phi(g_1H\cdot g_2H) \overset{?}{=} \phi(g_1H)\cdot\phi(g_2H)$

$$\begin{array}{ccc} \phi(g_1H\cdot g_2H) & \overset{?}{=} & \phi(g_1H)\cdot\phi(g_2H) \\ \| & & \| \\ \phi(g_1g_2H) & & g_1K\cdot g_2K \\ \| & & \| \\ g_1g_2K & \overset{\checkmark}{=\!=} & g_1g_2K \end{array}$$

* ϕ 是满射. 显然.

* $\ker\phi = \{gH\in G/H \mid \underset{\Downarrow\atop g\in K}{gK=K}\} = \{gH\mid g\in K\} = K/H$

特别地 $K/H \trianglelefteq G/H$

由第一同构定理知 $\dfrac{G/H}{K/H}\cong G/K$

例：$m,n\in\mathbb{N}$, $n\geq 3, m\geq 2$ 考虑：$\varphi: D_{2n} \longrightarrow D_{2mn} = \langle r_2, s \mid \cdots \rangle$

$$\langle r_1, s \mid r_1^{2n} = s^2 = 1, sr_1s = r_1^{-1} \rangle$$

旋转正2n边形

$$\varphi(r_1) = r_2^m.$$

带动正2mn边形

验：$\varphi(sr_1s) = sr_2^m s = sr_2s \cdot \underbrace{sr_2s \cdots sr_2s}_{m次} = r_2^{-1} \cdots r_2^{-1} = r_2^{-m}.$

$\psi: D_{2mn} \longrightarrow D_{2n}$

$$\psi(r_2) = r_1, \quad \psi(s) = s$$

需要验证：$\psi(r_2^{2mn}) = r_1^{2mn} = 1$ ✓ $\psi(s^2) = s^2 = 1$ ✓

$$\psi(sr_2s) = sr_1s = r_1^{-1} = \psi(r_2) \ ✓$$

$\ker\psi = \langle r_2^{2n} \rangle = \{1, r_2^{2n}, \cdots r_2^{2n(m-1)}\}$ ← 特别地，这是一个正规子群

结论：$D_{2mn} / \langle r_2^{2n} \rangle \cong D_{2n}$

练习：对任意 $n,m,s\in\mathbb{N}$, $n,m\geq 3$, $s\geq 2$. 刻画 $\varphi_s: D_{2n} \longrightarrow D_{2m}$

$\mathrm{Im}\,\varphi_s$？ $\ker\varphi_s$？ 第一同构定理？

<u>第四同构定理</u>. 设 N 是 G 的一个正规子群，记 $\pi: G \to \bar{G} := G/N$ 为对应的满射

则有如下的一一对应 $\{G$ 中包含 N 的子群 $A\} \longleftrightarrow \{\bar{G}$ 的子群$\}$

$$A \longmapsto \bar{A} := A/N$$

$$\pi^{-1}(C) \longleftarrow C$$

这一一对应满足如下性质：对子群 $A,B\leq G$ 满足 $N\leq A$ 和 $N\leq B$

有 (1) $A\leq B \iff \bar{A}\leq\bar{B}$

(2) 若 $A\leq B$，则 $[B:A] = [\bar{B}:\bar{A}]$

(3) $\overline{\langle A, B\rangle} = \langle \bar{A}, \bar{B}\rangle$

(4) $\overline{A\cap B} = \bar{A} \cap \bar{B}$

(c) $A \trianglelefteq G$ 当且仅当 $\bar{A} \trianglelefteq \bar{G}$

* "交换图表"初识

设 $N \trianglelefteq G$ 是一个正规子群，$\phi: G \to H$ 是一个同态. ← 希望更精细地理解 ϕ.

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "\pi"'] & H \\ G/N \arrow[ur, dashed, "??"'] & \end{tikzcd}$$

例

$$\begin{tikzcd} G = D_{24} \arrow[rr, "r \mapsto r^5"] \arrow[dr] & & D_{30} = H \\ & D_{24}/\langle r^3\rangle \cong D_6 \arrow[ur, dashed] & \end{tikzcd}$$

本质上就是

$$\begin{tikzcd} \mathbb{Z}/12\mathbb{Z} \arrow[rr, "\times 5"] \arrow[dr] & & \mathbb{Z}/15\mathbb{Z} \\ & \mathbb{Z}/3\mathbb{Z} \arrow[ur, "\times 5"'] & \end{tikzcd}$$

希望定义 $\Phi: G/N \longrightarrow H$

$$gN \longmapsto \phi(g)$$

引理：此 Φ 是良好定义的当且仅当 $N \subseteq \ker\phi$

证：必要性显然. 充分性：若 $g_1N = g_2N$，则 $\exists\, n \in N$ 使 $g_1 = g_2 n$.

则 $\phi(g_1) = \phi(g_2 n) = \phi(g_2)\phi(n) = \phi(g_2)$. $\square$

引理：当 $N \subseteq \ker\phi$ 时，Φ 是一个同态.

证明与前面诸多证明类似.

*抽象的语言：当 $N \subseteq \ker\phi$ 时，我们说 $\phi: G \to H$ 穿过 G/N (factors through G/N)

即存在同态 $\Phi: G/N \to H$ 使得如下图表交换

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "\pi"'] & H \\ G/N \arrow[ur, dashed, "\exists!\,\Phi"'] & \end{tikzcd}$$

交换指对

$$\begin{tikzcd} g \in G \arrow[r, mapsto] \arrow[d, mapsto] & \phi(g) \arrow[d, phantom, "\shortparallel"] \\ gN \arrow[r, mapsto] & \Phi(gN) \end{tikzcd}$$

← 相等.