群同态基本定理

陶先平，赵建华

南京大学计算机系

内容

- 正规子群
- 商群
- 同态核
- 自然同态
- 群同态基本定理
- 同态基本定理的应用

正规子群的概念

- 定义：群G的子群H是G的***正规子群***，当且仅当：对任意$a \in G$, $Ha=aH$。(记法：$H \trianglelefteq G$)
- 平凡子群是正规子群。
- 阿贝尔群与正规子群
  - 阿贝尔群的***任何***子群一定是正规子群。
- $Ha=aH$的充分必要条件是：

对任意$h_i \in H$, $a \in G$，一定存在某个$h_j \in H$，使得$h_i a = a h_j$。

(**不是**：对任意$h_i \in H$, $a \in G$, 一定有$h_i a = a h_i$。)

正规子群的例子

- S_3, 即$\{1,2,3\}$上所有一一对应的函数构成的群：

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \delta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

- $\{e,\delta,\varepsilon\}$构成正规子群。
  - 注意：$H=\{e,\alpha\}$构成子群，但不是正规子群：
    - $\beta H=\{\beta,\varepsilon\}$, 而$H\beta=\{\beta,\delta\}$

又一个正规子群的例子

- 群的中心C一定是正规子群。
  - C非空(显然单位元素$e\in C$)

    封闭性：$a_1b=ba_1,\ a_2b=ba_2 \Rightarrow (a_1a_2)b=b(a_1a_2)$

    子群：对任意的$a\in C, ab=ba \Rightarrow a^{-1}b=a^{-1}baa^{-1}=ba^{-1} \Rightarrow a^{-1}\in C$.

    正规子群：$ab=ba\ (a\in H) \Rightarrow Hb=bH$

- 设G是群，定义G的子集$H=\{a|a\in G$, 对任意$b\in G$: $ab=ba\}$，则H是正规子群。

正规子群的判定（1）

- 设N是群G的子群，N是群G的正规子群当且仅当：对任意$g\in G$, $n\in N$, 有 $gng^{-1}\in N$。
  - – $\Rightarrow$ 任取$g\in G$, $n\in N$, 有$n_1\in N$, 使得：$gn= n_1g$, 因此：$gng^{-1} = n_1\in N$；
  - – $\Leftarrow$ 先证明 $gN \subseteq Ng$：任取$gn\in gN$，已知$gng^{-1}\in N$，可令$gng^{-1}= n_1$，则$gn= n_1g\in Ng$；类似可证：$Ng\subseteq gN$。

- 设N是群G的子群，N是群G的正规子群当且仅当：对任意$g\in G$, 有 $gNg^{-1}=N$。

正规子群的判定(2)

- 设N是群G的子群，若G的**其它子群都不与N等势**，则N是G的正规子群。
  - 只需证明：$\boldsymbol{gNg^{-1}=N}$。

    首先证明：gNg^{-1}是子群。

    封闭性: $(gn_1g^{-1})(gn_2g^{-1})=gng^{-1}$

    子群判定条件2: $(gn_1g^{-1})\ (gn_2g^{-1})^{-1} = (gn_1g^{-1})(gn_2^{-1}g^{-1})=gng^{-1}$

    其次，因为其它子群都不与N等势，因此只需证明：$\boldsymbol{gNg^{-1}\approx N}$。

    由消去率可得.

正规子群的判定(3)

- 设N是群G的子群，且[G:N]=2,则N是正规子群。
  - 注意：若$g\in N$, 则由子群满足封闭性和消去律可知：$gN=Ng=N$

    若$g\notin N$, 则gN和Ng均不可能与N有公共元素，因此：$gN=Ng=G-N$。

右陪集关系

- 设H是群G的子群。定义G上的关系R如下：
  对任意$a,b\in G$, aRb iff. $ab^{-1}\in H$
  - 实际上： aRb 即：a与b在同一个右陪集中。
    - $aRb \Rightarrow ab^{-1}\in H \Rightarrow ab^{-1}=h_i,\ h_i\in H \Rightarrow a\in Hb$
  - 右陪集关系是等价关系

同余关系

- 狭义的同余关系：
  - 例： 对3同余: a$\equiv$b (mod 3) iff. |a-b|/3是整数。
    - 等价类： π_1={…-3,0,3,6,9,…}

      π_2={…-2,1,4,7,10,…}

      π_3={…-1,2,5,8,11,…}
- "*运算按照等价类保持*。"
  - $aRb,\ cRd \Rightarrow ac\ R\ bd$
- 同余关系

正规子群的陪集关系是同余关系

- 设N是群G的正规子群，可以证明：

  若$ap^{-1} \in N$, $bq^{-1} \in N$，则$(ab)(pq)^{-1} \in N$

  – 令$ap^{-1}=n_1$, $bq^{-1}=n_2$ $(n_1,n_2 \in N)$

    则: $(ab)(pq)^{-1} = abq^{-1}p^{-1} = an_2p^{-1}$

    而N是正规子群，$an_2=n_3a$ $(n_3 \in N)$

    所以：$(ab)(pq)^{-1} = n_3ap^{-1} = n_3n_1 \in N$

陪集的运算

- 设H是群G的正规子群。
- 在H的右陪集构成的集合上定义如下运算：

  Ha*Hb = H(ab) 这里ab是指G中的运算。
- 关于上述定义的合法性：
  - 运算结果是以右陪集的代表元素之间的运算表示的，*运算结果必须与代表元素的选择无关*。
  - 这一点由"H是正规子群"来保证。
    - 同余关系！

商群

- 设N是群G的正规子群，(G/N, *)是群
  - 封闭性：*的定义保证。
  - 结合律：G的运算满足结合律。
  - 单位元素：N本身(注意：G的单位元素$e \in N$)
  - 逆元素：Na的逆元素是Na^{-1}。
- (G/N, *)称为G的***商群***。

自然同态

- 任意的群G总与其商群满同态, 称为***自然同态***
  - 假设N是G的正规子群
  - G/N是由N所确定的商群
    - (G/N的元素是N的(右)陪集)
  - 定义g:G→G/N, 对任意a∈G, g(a)=Na, 显然： g是满射。
  - g是满同态映射：
    - 对任意a,b∈G: g(a b)=N(a b) =Na*Nb= g(a)*g(b)

自然同态的几个例子

- 例：群G本身也是G的正规子群。自然同态g:G→G/G是零同态。
  - 注意：G/G = {G}, 对任意x∈G, g(a)=G。
- 例：设e_1是群G的单位元，$\{e_1\}$是G的正规子群，定义函数g:G→G/{e1}如下：

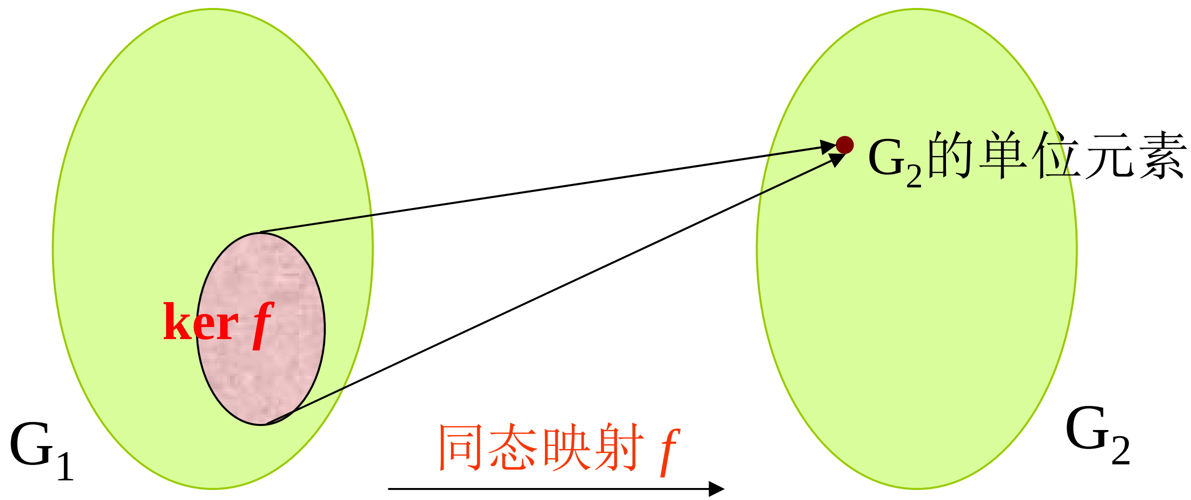
  对任意x∈G, $g(x)=\{x\}$

  则g是G到$G/\{e_1\}$的自然同态，这也是同构。
  - 注意：$G/\{e_1\} = \{ \{x\} \mid x\in G\}$
- 设G_1，G_2是群，其单位元分别是e_1,e_2。定义：
  - $f:G_1\times G_2\to G_1$: 对任意$<a,b>\in G_1\times G_2$, $f(<a,b>)=a$

    易证：f是满同态映射，$\ker f = \{e_1\}\times G_2$

同态核

- 假设G_1, G_2是群， f: $G_1 \to G_2$是同态映射， 定义集合 **ker f = {x|x∈G_1,且f(x)=e_2}**,其中e_2是G_2的单位元素， ker f称为***同态核***。

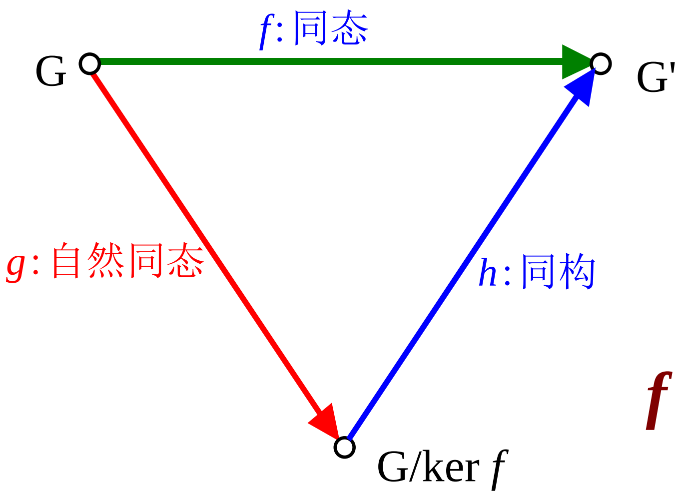


同态核是正规子群

- $\ker f$是G_1的**正规子群**。
  - 非空： G_1的单位元必在$\ker f$ 中。
  - 子群： 任取$a,b\in \ker f$, 则： $f(a)=f(b)=e_2$; 因此： $f(a \quad b^{-1}) = f(a)*[f(b)]^{-1}= e_2$ 。
  - 正规子群： 任取$a\in \ker f$,$x\in G_1$, 则： $f(a)=e_2$; 因此： $f(x \quad a \quad x^{-1}) = f(x)* f(a)*[f(x)]^{-1} =e_2$ 。
    - $g*a*g^{-1}\in \ker f$

同态基本定理

- 假设G, G’是群， f: G→G’是满同态映射，则G/ker $f \cong$ G’。



$f = g \circ h$

同态基本定理的证明

- 令ker f =K, 即K是关于f的同态核
- 对任意a,b$\in$G, Ka=Kb当且仅当f(a)=f(b)
  - 注意： Ka=Kb $\Leftrightarrow$ a,b在同一右陪集中 $\Leftrightarrow$

    $ab^{-1}\in K \Leftrightarrow f(ab^{-1})=e' \Leftrightarrow f(a) * f(b^{-1})=e' \Leftrightarrow$

    f(a)与$[f(b)]^{-1}$互为逆元素 $\Leftrightarrow f(a)=f(b)$
- 定义h:G/K$\to$G': h(Ka)=f(a)。
  - 由上述讨论可知：h是一对一的；由于f是满射，显然h也是满射，$\therefore h$是从G/K到G'的双射。对任意Ka,Kb$\in$G/K,
    $h(Ka\otimes Kb)=h(K(ab))=f(ab)=f(a)*f(b)=h(Ka)*h(Kb)$
- ***所以：G/K≅G'***

循环群与群同态

- G和G'分别是阶为m,n的循环群，G与G'满同态 当且仅当 n整除m
  - $\Rightarrow$ 设f是G到G'的同态映射。则$G' \cong G/\ker f$, 因此，$G/\ker f$的阶为n，$\ker f$是G的子群, 根据拉格朗日定理，n能整除m。
  - $\Leftarrow$ 定义f: $G \rightarrow G'$, 对任意$a^k \in G$, $f(a^k)=b^k$。其中a,b分别是G和G'的生成元素。
    - 若$a^j=a^k$，则j,k对m同余，也对n同余，所以：$b^j=b^k$，因此f是函数。
    - $f(a^j \quad a^k) = f(a^{j+k}) = b^{j+k} = b^j * b^k = f(a^j)*f(a^k)$

同态基本定理的应用

- G是群， H和K都是G的正规子群， 且 $H \subseteq K$，证明： $G/K \cong (G/H)/(K/H)$
  - 比较同态基本定理， $G/\ker f \cong G'$
  - 定义f: $G/H \to G/K$, 对任意$Ha \in G/H$, $f(Ha)=Ka$
    - 注意： $Ha=Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow ab^{-1} \in K \Leftrightarrow Ka=Kb$
  - 易证 f 是满同态映射， 且同态核是K/H
  - $\therefore$ ***$G/K \cong (G/H)/(K/H)$***

同态群的商群的关系

- 设f是群G到G'的满同态，H'是G'的不变子群，H={a|a∈G, f(a)∈H'}, 则H也是G的不变子群，并且：**G/H≅G'/H'**
  - 证明思路：
    - 建立从G到(G'/H')的满同态h
    - 证明h的同态核即为H
    - 立即由同态基本定理得到结论
  - 令G'到商群G'/H'的自然同态为g, 则$h=f\ \ g$
  - H=ker h
    - H⊆ker h：对任意a∈H, f(a)∈H', h(a)=g(f(a))=H', ∴a ∈ker h
    - ker h ⊆H：对任意a∈ker h， 则h(a)=H', 即g(f(a))=H', 所以f(a)∈H', 即a ∈H

单同态

- **代数系统** $(G_1,\ \ )$与$(G_2,*)$**单同态** 当且仅当：

  存在**一对一**的函数f: $G_1 \rightarrow G_2$, 满足：

  对任意$x,y \in G_1$, $f(x\ \ y) = f(x) * f(y)$

- 假设G_1, G_2是群， f: $G_1 \rightarrow G_2$是同态映射。f是单同态映射 当且仅当 $\ker f = \{e_1\}$, e_1是G_1的单位元

  $\Rightarrow$ 设$a \in \ker f$, 且$a \neq e_1$, 但$f(a)=f(e_1)=e_2$, f不是单射。

  $\Leftarrow$ 假设有$a,b \in G_1$, 满足$f(a)=f(b)$，则 $f(a)*[f(b)]^{-1} = f(a\ \ b^{-1}) = e_2$， $\therefore a\ \ b^{-1} \in \ker f = \{e_1\}$， $\therefore a\ \ b^{-1} = e_1$, 由逆元素唯一：$a=b$，所以$f$是单同态。

作 业

- 假设f从群G到G'的映射，H是G的一个子集，证明：
  - (1) $H \subseteq f^{-1}(f(H))$, 但是$H = f^{-1}(f(H))$不一定成立。

    这里：对任意$S' \subseteq G'$, $f^{-1}(S') = \{x | x \in G, 且 f(x) \in S'\}$
  - (2) 若H包含ker f，则$f^{-1}(f(H))=H$

- 设H，K是群G的两个正规子群，则HK，$H \cap K$均是G的正规子群，且：$HK/K \cong H/H \cap K$

  这里：$HK = \{ab \mid a \in A, b \in B\}$

同态群的子群的对应

- 设f是群G到G'的满同态。A={H|H⊆G, 且ker f⊆H}，A'是G'的幂集。定义g: A→A': 对任意H ∈ A，g(H)=f(H)。则g是双射。
  - g是映射：对任意H∈A, f(H)是G'的子集
  - g是满射：对任意H'∈A', 令H={a|a∈G, f(a)∈H'}，则a,b∈H⇒f(a), f(b)∈H'⇒f(a)f(b) ∈H'⇒f(ab)∈H'⇒ab∈H (封闭性)；又：a∈H' ⇒f(a)∈H' ⇒$[f(a)]^{-1}$∈H'⇒$f(a^{-1})$∈H'⇒a^{-1}∈H (逆元素)；所以H是子群。任给x∈ker f, f(x)=e'∈H'，即x∈H, 所以：ker f⊆H。
  - g是单射：注意：若H包含ker f，则$f^{-1}(f(H))=H$(这里的f^{-1}不是反函数，表示集合的完全原象集);

    因此：$f(H_1)=f(H_2) \Rightarrow f^{-1}(f(H_1))= f^{-1}(f(H_2)) \Rightarrow H_1=H_2$。
- 注意：H是G的不变子群 当且仅当 f(H)是G'的不变子群。