第八章 群III

计算机系网络所：张小平

清華大學
Tsinghua University

主要内容

- 8.1 半群
- 8.2 群、群的基本性质
- 8.3 循环群 群的同构
- 8.4 变换群和置换群 Cayley定理
- 8.5 陪集和群的陪集分解 Lagrange定理
- **8.6 正规子群与商群**
- 8.7 群的同态、同态基本定理
- 8.8 群的直积

正规子群与商群

- 如果存在群 G 的一个子群 H，根据它的左陪集可以完成群的分解。
- 事实上，子群 H 的右陪集，也有对称的性质
- 但是，在许多情况下，群 G 的子群的左右陪集并不相等
- 思考：
  - 任意给定一个群 G，它是否存在子群 H，使得其左右陪集相等？
  - 子群 $\{e\}$，子群 G

正规子群与商群

- **定义 8.6.1** 设H是G的一个子群，如果对任意的$a \in G$，都有$aH = Ha$，则称H是G的一个**正规子群**（亦称**不变子群**），用符号$H \lhd G$表示。

  因此，对正规子群H就不必区分其左右陪集，而简称为H的**陪集**

正规子群与商群

- **定理 8.6.1** 设 H 是 G 的子群，则以下几个条件等价：

1. $H \triangleleft G$
2. $\forall g \in G, gHg^{-1}=H$
3. $\forall g \in G, gHg^{-1} \subseteq H$
4. $\forall g \in G, h \in H, ghg^{-1} \in H$

正规子群与商群

- 证明： $1.H \triangleleft G \Rightarrow 2.\ \forall g \in G, gHg^{-1}=H$

  - 因为H为正规子群，因此 $\forall g \in G,\ gH = Hg$
  - 因此$\forall x \in gH$，有$x = gh_1 = h_2 g$，其中$h_1, h_2 \in H$
  - $\forall a \in gHg^{-1}$，有$a = ghg^{-1} = h'gg^{-1} = h' \in H$
  - $\forall h \in H$，有$h = hgg^{-1} = gh'g^{-1} \in gHg^{-1}$
  - 故 $gHg^{-1} = H$

正规子群与商群

- 证明： 2. $\forall g \in G, gHg^{-1}=H$ ⇒ 3. $\forall g \in G, gHg^{-1} \subseteq H$

  - $\forall g \in G \qquad gHg^{-1} = H$

    ⇓

    $\forall g \in G \qquad gHg^{-1} \subseteq H$

正规子群与商群

- **证明：** 3. $\forall g \in G, gHg^{-1} \subseteq H$ ⇒ 4. $\forall g \in G, h \in H, ghg^{-1} \in H$

  - $gHg^{-1} \subseteq H$

    ⇓

  - $\forall g \in G,\ h \in H\ ,\ ghg^{-1} \in H$

正规子群与商群

- 证明：4. $\forall g \in G, h \in H, ghg^{-1} \in H \Longrightarrow 1. H \triangleleft G$

  - 求证 $\forall g \in G, \quad gH = Hg$
  - 据已知条件，$\forall g \in G$，$\forall h \in H$，都有 $ghg^{-1} = h_1 \in H$
  - 即 $gh = h_1 g \in Hg$。因此 $\forall g \in G$，$gH \subseteq Hg$
  - 反之，易证 $\forall g \in G$，$Hg \subseteq gH$
  - 因此 $\forall g \in G$，$gH = Hg$

证毕！

正规子群与商群

- **定理 8.6.1** 设 H 是 G 的子群，则以下几个条件等价：

  1. $H \triangleleft G$

  2. $\forall g \in G, gHg^{-1} = H$

  3. $\forall g \in G, gHg^{-1} \subseteq H$

  4. $\forall g \in G, h \in H, ghg^{-1} \in H$

正规子群与商群

- 定理 8.6.2 设 A, B 是 G 的两个子群

  1. 若 $A \lhd G, B \lhd G,$ 则 $A \cap B \lhd G, AB \lhd G$

  2. 若 $A \lhd G, B \leq G,$ 则 $A \cap B \lhd B, AB \leq G$

正规子群与商群

- 证明：1. 若 $A \lhd G, B \lhd G$ ， 则 $A \cap B \lhd G, AB \lhd G$

  - $\forall h \in A \cap B \Rightarrow h \in A,\ h \in B$
  - $\forall g \in G$ ， $ghg^{-1} \in A,\ ghg^{-1} \in B$
  - $\forall g \in G, \forall h \in A \cap B$ ， $ghg^{-1} \in A \cap B \Rightarrow A \cap B \lhd G$
  - $\forall h \in AB \Rightarrow h = ab,\ a \in A,\ b \in B$
  - $\forall g \in G$ ， $ghg^{-1} = gabg^{-1} = gag^{-1}gbg^{-1} = a'b' \in AB$
  - $AB \lhd G$

正规子群与商群

- 证明：2. 若 $A \lhd G, B \leq G$ ， 则 $A \cap B \lhd B, AB \leq G$

  - $\forall h \in A \cap B \Rightarrow h \in A,\ h \in B$
  - $\forall g \in B \Rightarrow ghg^{-1} \in A,\ ghg^{-1} \in B$
  - $\forall g \in B, \forall h \in A \cap B$ ，$ghg^{-1} \in A \cap B \Rightarrow A \cap B \lhd B$

正规子群与商群

- 证明：2. 若 $A \lhd G, B \leq G$ ， 则 $A \cap B \lhd B, AB \leq G$

  - $e \in A,\ e \in B \Rightarrow e \in AB$ 单位元！ 结合律！
  - $\forall ab, a_1b_1 \in AB$ $A \lhd G \Rightarrow bA = Ab \Rightarrow ba = a'b$

    $(ab)(a_1b_1) = a(ba_1)b_1 = a(a_1'b)b_1 = (aa_1')(bb_1) \in AB$ 封闭性！
  - $\forall ab \in AB$ ，$(ab)^{-1} = b^{-1}a^{-1} = (a^{-1})'b^{-1} \in AB$ 逆元素！
  - $AB \leq G$ 证毕！

正规子群与商群

- 定理 8.6.2 设 A, B 是 G 的两个子群

1. 若 $A \lhd G, B \lhd G,$ 则 $A \cap B \lhd G, AB \lhd G$

2. 若 $A \lhd G, B \leq G,$ 则 $A \cap B \lhd B, AB \leq G$

正规子群的交集仍然是正规子群！
正规子群的乘积仍然是正规子群！

正规子群与普通子群的交集是普通子群的正规子群！
正规子群与普通子群的乘积是普通子群！

正规子群与商群

- 思考：
  - 普通子群和普通子群的交是否是普通子群？
  - 普通子群和普通子群的乘积是否是普通子群？

$\forall ab, a_1b_1 \in AB$ $\quad A \triangleleft G \Rightarrow bA = Ab \Rightarrow ba = a'b$

$(ab)(a_1b_1) = a(ba_1)b_1 = a(a_1'b)b_1 = (aa_1')(bb_1) \in AB$ 封闭性！

正规子群与商群

- 定理 8.6.3 设H是G的一个正规子群，G/H表示H的所有陪集构成的集合，即

$$G/H = \{gH | g \in G\}$$

则G/H关于陪集乘法成群。称之为G关于H的 商群

代数系统的概念

- 定义7.3.1 设A是非空集合，A^2到A的一个映射 f： $A^2 \to A$ 称为 A 的一个二元代数运算，简称二元运算

正规子群与商群

- 证明：陪集乘法对于 G/H 是一个二元运算
  - $\forall aH, bH \in G/H,\ \ aHbH = \{ah_1bh_2 \mid h_1, h_2 \in H\}$
  - $bH = Hb \Rightarrow ah_1bh_2 = a(h_1b)h_2 = a(bh_1')h_2 = (ab)(h_1'h_2) \in abH$
  - 故 $aHbH \subseteq abH$
  - 又 $\forall\ (ab)h \in abH, (h \in H)$，$(ab)h = (ae)(bh) \in aHbH$
  - 故 $abH \subseteq aHbH$
  - 因此 $\forall aH, bH \in G/H,\ \ aHbH = abH \in G/H$

二元运算！

正规子群与商群

- 证明（续）：G/H对陪集乘法成群

  - $\forall aH, bH, cH \in G/H$ 结合律！

$$(aHbH)cH = (abH)cH = (ab)cH = a(bc)H = aH(bc)H = aH(bHcH)$$

  - $eHaH = eaH = aH$，$aHeH = aeH = aH \Rightarrow eH = H$ 是单位元

单位元！

  - $a^{-1}HaH = aHa^{-1}H = eH$ ，因此aH的逆元为$a^{-1}H$

逆元素！

证毕！

正规子群与商群

- 定理8.6.3 设H是G的一个正规子群，G/H表示H的所有陪集构成的集合，即

$$G/H = \{gH | g \in G\}$$

则G/H关于陪集乘法 成群。称之为G关于H的商群。

思考：普通子群的陪集集合关于陪集乘法是否可以成群？

正规子群与商群-小结

- 正规子群
- 正规子群的等价性质
- 正规子群与子群的交、乘积性质
- 商群

主要内容

- 8.1 半群
- 8.2 群、群的基本性质
- 8.3 循环群 群的同构
- 8.4 变换群和置换群 Cayley定理
- 8.5 陪集和群的陪集分解 Lagrange定理
- 8.6 正规子群与商群
- **8.7 群的同态、同态基本定理**
- 8.8 群的直积

循环群 群的同构

- 定义 8.3.2 设 $(G, \bullet)$ 和 $(G', *)$ 是两个群

$f: G \to G'$ 是双射，如果 $\forall a,b \in G$ 都有

$$f(ab) = f(a) * f(b)$$

则称 f 是 G 到 G' 的一个同构，记作 $G \cong G'$

群的同态、同态基本定理

- 定义 8.7.1 设G_1, G_2是两个群，f是G_1到G_2的一个映射。如果对任意的$a, b \in G_1$都有

$$f(ab) = f(a)f(b)$$

则称 f 是 G_1 到 G_2 的一个同态映射，或简称同态。

群同态的充分条件：1. 映射 2. 保持运算！

群的同态、同态基本定理

- 若映射f分别是单射、满射、双射时，分别称之为G_1到G_2的**单一同态**、**满同态**、**同构**
- 用$G_1 \sim G_2$表示满同态，并称G_2是f作用下G_1的**同态象**

群的同态、同态基本定理

- **引理8.7.1**：设H是G的正规子群，$\forall a \in G$令 $f: a \to aH$，则 f是G 到G/H的满同态。

  证明：

  - 显然，f 是 G 到 G/H 的一个映射
  - 同时 $\forall aH \in G/H$，$\exists a \in G$，满足$f(a) = aH$
  - 因此 f 是 G 到 G/H 的一个满射

群的同态、同态基本定理

证明（续）：

- 由于$\forall a,b \in G$，$f(ab) = abH$
- 且G/H中的运算满足$aHbH = abH$
- 故 $f(ab) = abH = aHbH = f(a)f(b)$

保持运算！

- 因此f是G到G/H的满同态

证毕！

群的同态、同态基本定理

- **引理8.7.1**：设H是G的正规子群，$\forall a \in G$，令$f: a \to aH$，则f是G到G/H的满同态。

群G可以和其任意一个商群构成满同态！

群的同态、同态基本定理

- **定理 8.7.1** 若 f 是 G_1 到 G_2 的同态，g 是 G_2 到 G_3 的同态，则 gf 是 G_1 到 G_3 的同态。

证明：显然 gf 是 G_1 到 G_3 的映射，以下只证明它保持运算，$\forall a, b \in G_1$

$$gf(ab) = g(f(ab)) = g(f(a)f(b))$$

$$= g(f(a))g(f(b)) = gf(a)gf(b)$$

因此 gf 是 G_1 到 G_3 的同态。

群的同态、同态基本定理

- **定理8.7.2** 设G是一个群，$(G', \cdot)$是一个有二元运算的代数系统，若$f: G \to G'$是满射，且保持运算，则G'也是群，而且$G \sim G'$

循环群 群的同构

- 定理 8.3.5 设 G 是一个群，$(G', *)$ 是一个代数系统，如存在 G 到 G' 的双射 f，且保持运算，即 $\forall a,b \in G$，有 $f(ab) = f(a) * f(b)$，则 G' 也是一个群。

与群同构的代数系统，是群！

群的同态、同态基本定理

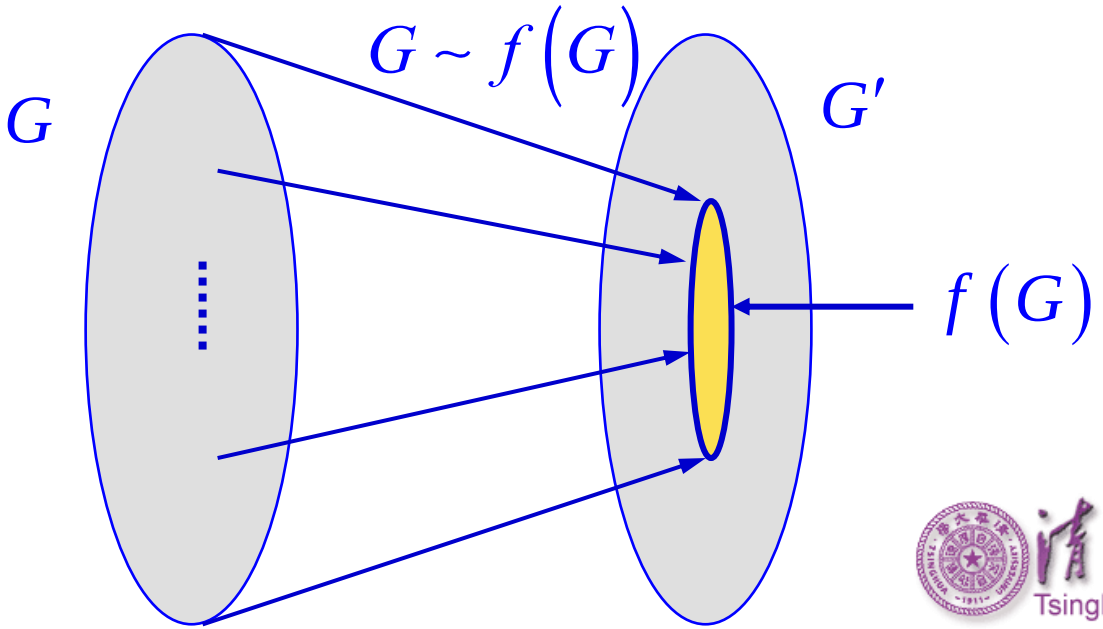
- 定理8.7.2 设G是一个群，$(G', \cdot)$是一个有二元运算的代数系统，若$f: G \to G'$是满射，且保持运算，则G'也是群，而且$G \sim G'$

群的同态象，仍然是群！

群的同态、同态基本定理

- 引理 8.7.2 设f是G到G'的同态，则G的象集$f(G)$是群G'的子群！

  且f是G到$f(G)$的满同态



群的同态、同态基本定理

- **定理 8.7.3** 设 f 是 G 到 G' 的同态，则

1. 若 e 和 e' 分别是 G 和 G' 的单位元，则 $f(e)=e'$
2. $\forall a \in G$，f 将 a 的逆元映射到 G' 中像的逆元，即 $f(a^{-1})=f^{-1}(a)$
3. 如果 H 是 G 的子群，则 H 在 f 下的象 $f(H)=\{f(a)|a \in H\}$ 是 G' 的子群，且 $H \sim f(H)$

群的同态、同态基本定理

- 证明：1. e和e'分别是G和G'的单位元 $\Rightarrow f(e)=e'$
  - $f:G\to G'$，$\forall a,b\in G$，$f(ab)=f(a)f(b)$
  - 因此，$\forall a'\in f(G),\exists a\in G$，满足$a'=f(a)$

$$a'=f(a)=f(ae)=f(a)f(e)=a'f(e)$$

同理，$a'=f(e)\,a'$。 ∴ $f(e)$是$f(G)$的单位元

因为单位元唯一，故$f(e)=e'$

群的同态、同态基本定理

- 证明：2. $\forall a \in G$ ， $f(a^{-1}) = f^{-1}(a)$
  - $\forall a \in G$，有 $a^{-1} \in G$
  - 因此，$f\left(aa^{-1}\right) = f\left(e\right) = e' = f\left(a\right) f\left(a^{-1}\right)$
  - 同理，$f\left(a^{-1}a\right) = f\left(e\right) = e' = f\left(a^{-1}\right) f\left(a\right)$
  - 故 $f^{-1}\left(a\right) = f\left(a^{-1}\right)$

群的同态、同态基本定理

- 证明：3. $H \le G \Rightarrow f(H) \le G'$，且 $H \sim f(H)$

  - $\forall a,b \in f(H)$，由于 f 为满射，因此必定存在 $a',b' \in H$，使得 $f(a')=a, f(b')=b$。
  - 则 $ab = f(a')f(b') = f(a'b') \in f(H)$　　封闭性！
  - $e \in H \Rightarrow f(e) \in f(H)$　　单位元！

群的同态、同态基本定理

- 证明：3. $H \le G \Rightarrow f(H) \le G'$，且 $H \sim f(H)$

  - $\forall a \in f(H)$，由于 f 为满射，因此必定 $\exists a' \in H$，使得 $f(a') = a$
  - 显然 $(a')^{-1} \in H$，则 $f\left((a')^{-1}\right) \in f(H)$
  - $f\left((a')^{-1}\right)a = f\left((a')^{-1}\right)f(a') = f\left((a')^{-1}(a')\right) = f(e) = e'$
  - 同理，$af\left((a')^{-1}\right) = e'$ 逆元素！
  - 即 $\forall a \in f(H)$，在 $f(H)$ 中有逆元素

群的同态、同态基本定理

- 证明：3. $H \le G \Rightarrow f(H) \le G'$，且 $H \sim f(H)$

  - $\forall a \in f(H)$，根据 $f(H)$ 的定义，必定存在 $a' \in H$，使得 $f(a') = a$ 满射！
  - 说明 f 是从 H 到 $f(H)$ 的满射！
  - $\forall a, b \in H$，$f(ab) = f(a) f(b) \in f(H)$ 保持运算！
  - 故 $H \sim f(H)$ 证毕！

群的同态、同态基本定理

- **定理 8.7.3** 设 f 是 G 到 G' 的同态，则

1. 若 e 和 e' 分别是 G 和 G' 的单位元，则 $f(e)=e'$

在同态映射下，单位元的象仍然是单位元

2. $\forall a \in G$，f 将 a 的逆元映射到 G' 中像的逆元，

即 $f(a^{-1})=f^{-1}(a)$ 在同态映射下，逆元素的象是象的逆元素

3. 如果 H 是 G 的子群，则 H 在 f 下的象

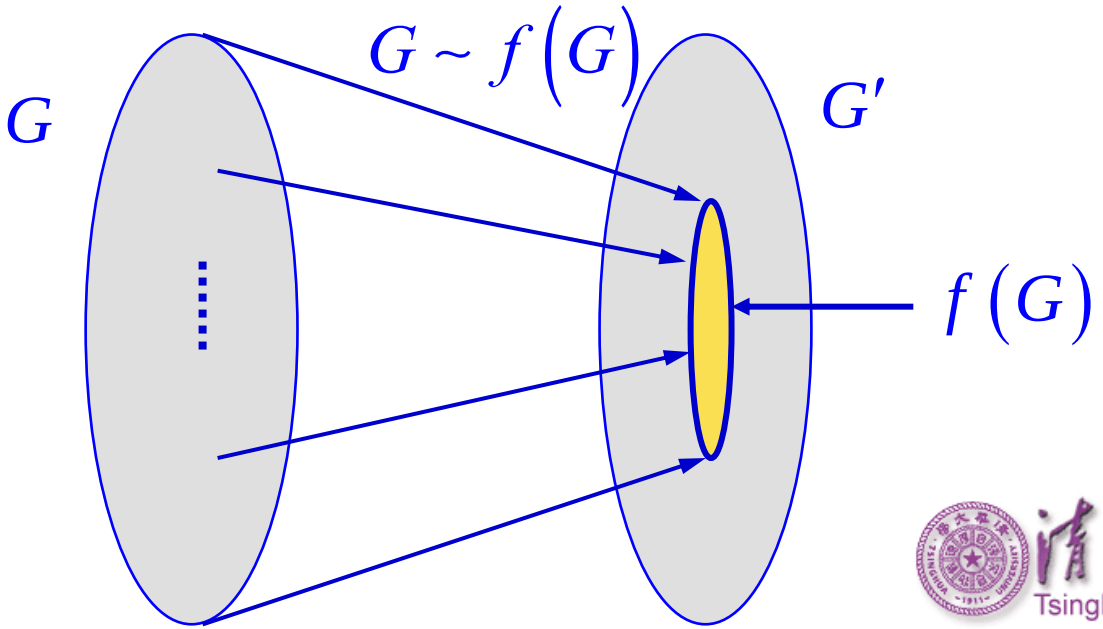
$f(H)=\{f(a)|a \in H\}$ 是 G' 的子群，且 $H \sim f(H)$

在同态映射下，子群的象仍然是子群，且该同态映射形成二者之间的满同态

群的同态、同态基本定理

- 引理 8.7.2 设f是G到G'的同态，则G的象集$f(G)$是群G'的子群！

  且f是G到$f(G)$的满同态



群的同态、同态基本定理

- 定理 8.7.5 设 f 是 G 到 G' 的同态，e 是 G 的单位元，令 $K = \{a \in G | f(a) = f(e)\}$，则 K 是 G 的正规子群，K 称为同态 f 的核，记作 Ker f

群的同态、同态基本定理

- 证明：$K=\{a\in G|f(a)=f(e)\} \quad \Rightarrow \quad K\lhd G$
  - 显然，e 为 K 中的元素
  - 由于 f 是同态，因此 $f(e)=e'$ 是 G' 的单位元
  - $\forall k,k_1\in K$，$f(kk_1)=f(k)f(k_1)=f(e)f(e)=e'=f(e)$
  - $\forall k\in K$，$f(k^{-1})=f^{-1}(k)=f^{-1}(e)=e'=f(e)$

    $\Longrightarrow \quad k^{-1}\in K$
  - 因此，K 为 G 的 子群。

群的同态、同态基本定理

- 证明：
  - $\forall g \in G, \forall k \in K$

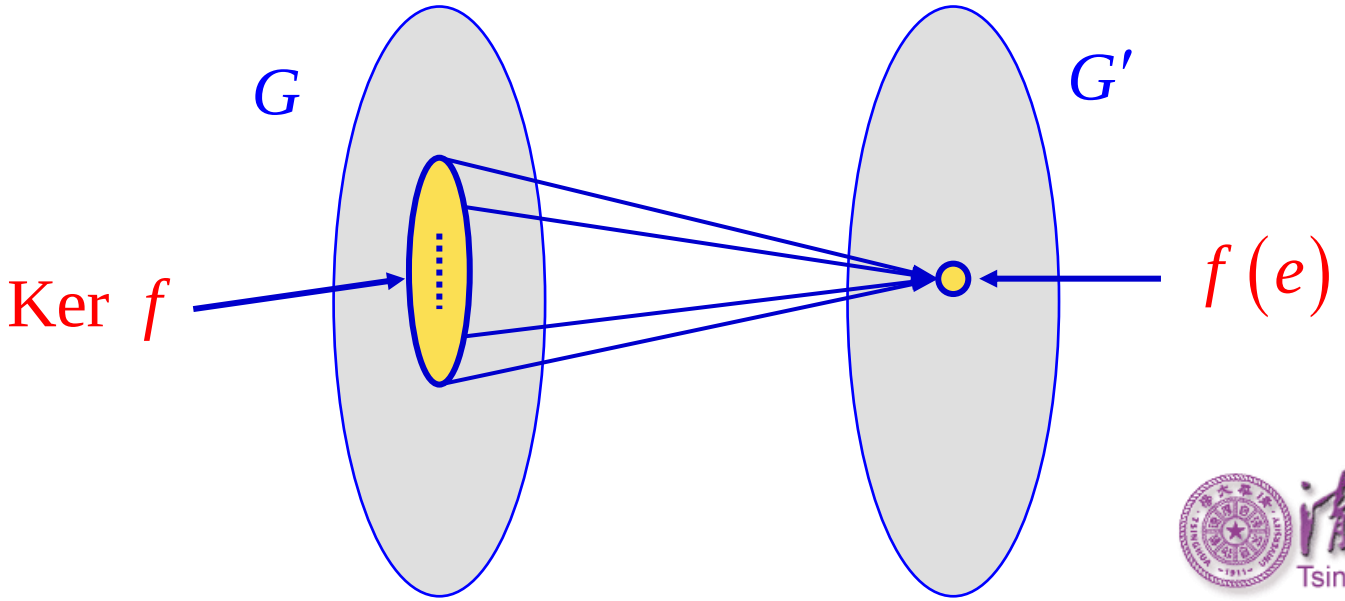
$$f(g^{-1}kg) = f(g^{-1})f(k)f(g) = f^{-1}(g)f(k)f(g)$$

$$= f^{-1}(g)f(g) = e' = f(e)$$

  - 即 $\forall g \in G, \forall k \in K$， $g^{-1}kg \in K$
  - 因此， $K \lhd G$ 证毕！

群的同态、同态基本定理

- 定理 8.7.5 设 f 是 G 到 G' 的同态，e 是 G 的单位元，令 $K=\{a\in G|f(a)=f(e)\}$，则 K 是 G 的正规子群，K 称为同态 f 的核，记作 Ker f



群的同态、同态基本定理

- 定理 8.7.6 设 f 是 G 到 G' 的同态，K 是同态的核，那么对任意的 $a,b \in G$，$f(a)=f(b)$ 的充要条件是 $b \in aK$

群的同态、同态基本定理

- 证明：
  - 充分性：已知 $b \in aK \Rightarrow \forall a,b \in G$，$f(a)=f(b)$
  - $\exists k \in K$，使得 $b=ak$

$$f(b)=f(ak)=f(a)f(k)=f(a)f(e)=f(a)$$

  - 必要性：已知 $\forall a,b \in G$，$f(a)=f(b) \Rightarrow b \in aK$

$$e'=f^{-1}(a)f(a)=f^{-1}(a)f(b)=f\left(a^{-1}\right)f(b)=f\left(a^{-1}b\right)$$

  - 说明 $a^{-1}b \in K$，即 $b \in aK$ 证毕！

群的同态、同态基本定理

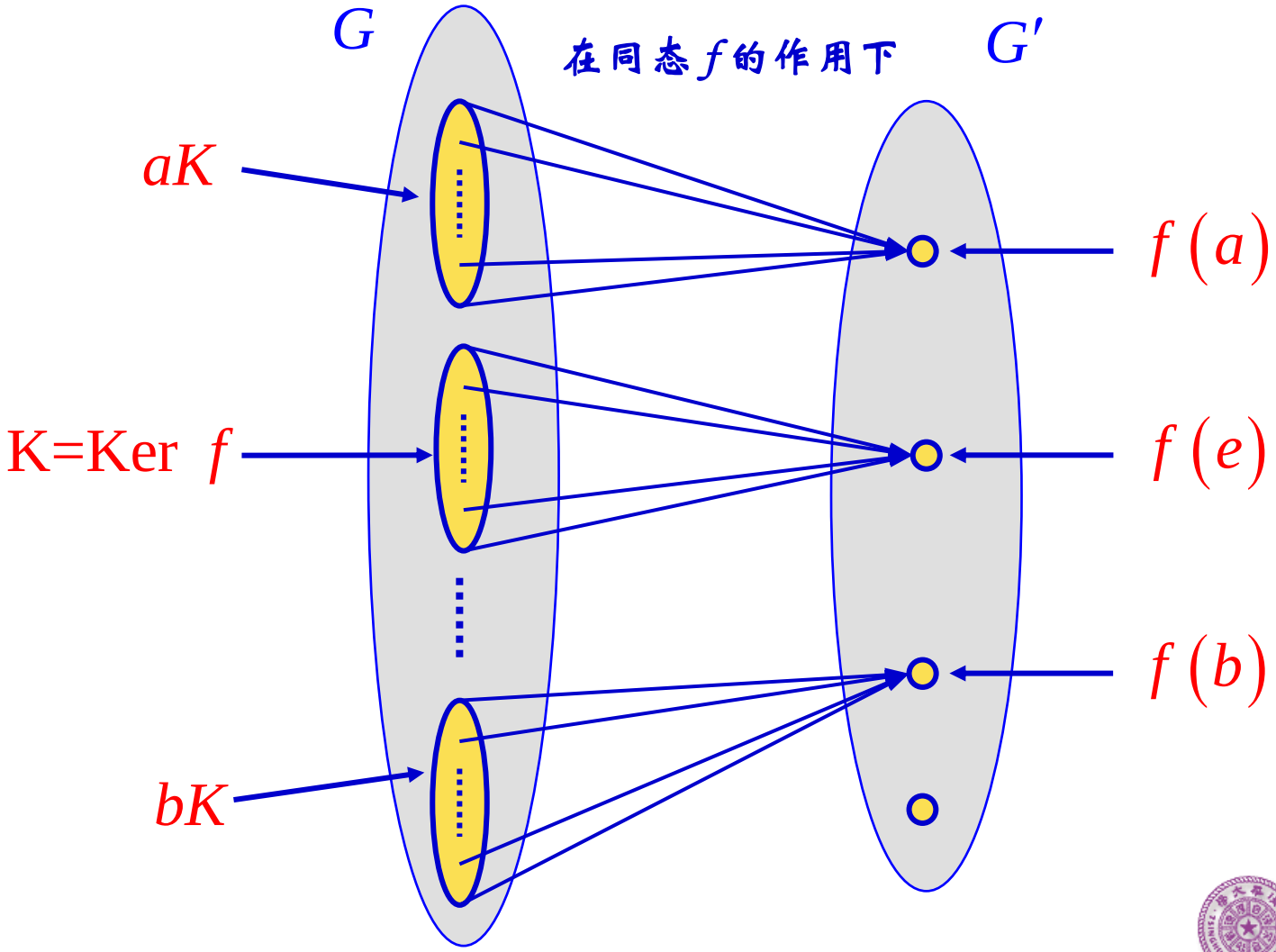
- 定理 8.7.6设 f 是 G 到 G'的同态，K 是同态的核，那么对任意的$a,b \in G$，$f(a)=f(b)$的充要条件是 $b \in aK$　　$a \in bK$

$$f(a)=f(b) \Leftrightarrow b \in aK \Leftrightarrow bK=aK$$

同态核的　陪集所有元素映射到一个象！

同态核不同　陪集的象一定不同！

群的同态、同态基本定理



群的同态、同态基本定理

- 定理 8.7.7 设 f 是 G 到 G' 的同态，则 f 是单同态的充要条件是 $\mathrm{Ker}\, f = \{e\}$

群的同态、同态基本定理

- 证明：
  - 必要性：已知 f 为单同态 $\Rightarrow$ $\mathrm{Ker}\, f = \{e\}$
  - G' 中单位元 e' 在 G 中只有一个原象 e，即 $\mathrm{Ker}\, f = \{e\}$
  - 充分性：已知 $\mathrm{Ker}\, f = \{e\}$ $\Rightarrow$ f 为单同态
  - $\forall a, b \in G$，若 $f(a) = f(b)$

    $$f(a)f^{-1}(b) = f(a)f(b^{-1}) = f(ab^{-1}) = f(b)f^{-1}(b) = e'$$

  - 由已知条件，$ab^{-1} = e \Rightarrow a = b$ 证毕！

群的同态、同态基本定理

- 定理 8.7.7设 f 是 G 到 G'的同态，则 f 是单同态的充要条件是 $\mathrm{Ker}\, f = \{e\}$

- 推论：设 f 是 G 到 G'的满同态，则 f 为同构的充要条件是 $\mathrm{Ker}\, f = \{e\}$

群的同态、同态基本定理

- 同态基本定理：设G是一个群，则G的任一商群都是G的同态象；反之，若G'是G的同态象，f是G到G'的满同态，则

$$G' \cong G/K \quad \text{其中 } K = Ker\, f$$

群的同态、同态基本定理

- 同态基本定理：设G是一个群，则G的任一商群都是G的同态象；反之，若G'是G的同态象，f是G到G'的满同态，则

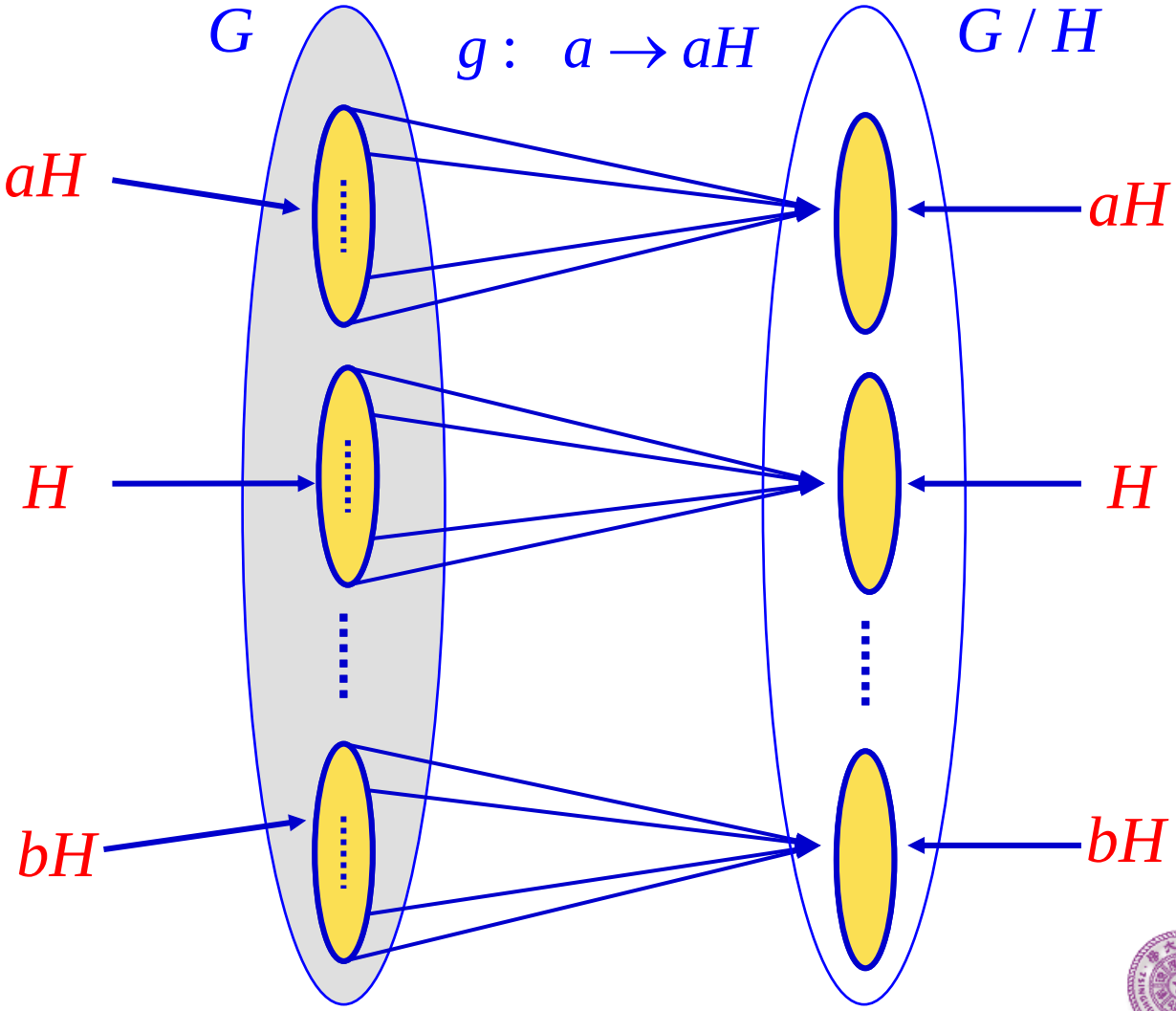
$$G' \cong G/K \quad \text{其中 } K = Ker\, f$$

群的同态、同态基本定理

- 证明：$G \sim G/H$

  - G/H 为任一商群，则 $H \lhd G$
  - 则可构造映射 $g: a \to aH \ (\forall a \in G)$
  - 由引理8.7.1可知，g 为满同态。
  - 而 G/H 为 G 在 g 下的同态象
  - 即 $G \sim G/H$

群的同态、同态基本定理



群的商群可以成为其同态象！

清華大學 Tsinghua University

群的同态、同态基本定理

- 同态基本定理：设G是一个群，则G的任一商群都是G的同态象；反之，若G'是G的同态象，f是G到G'的满同态，则

$$G' \cong G/K \quad \text{其中 } K = Ker\, f$$

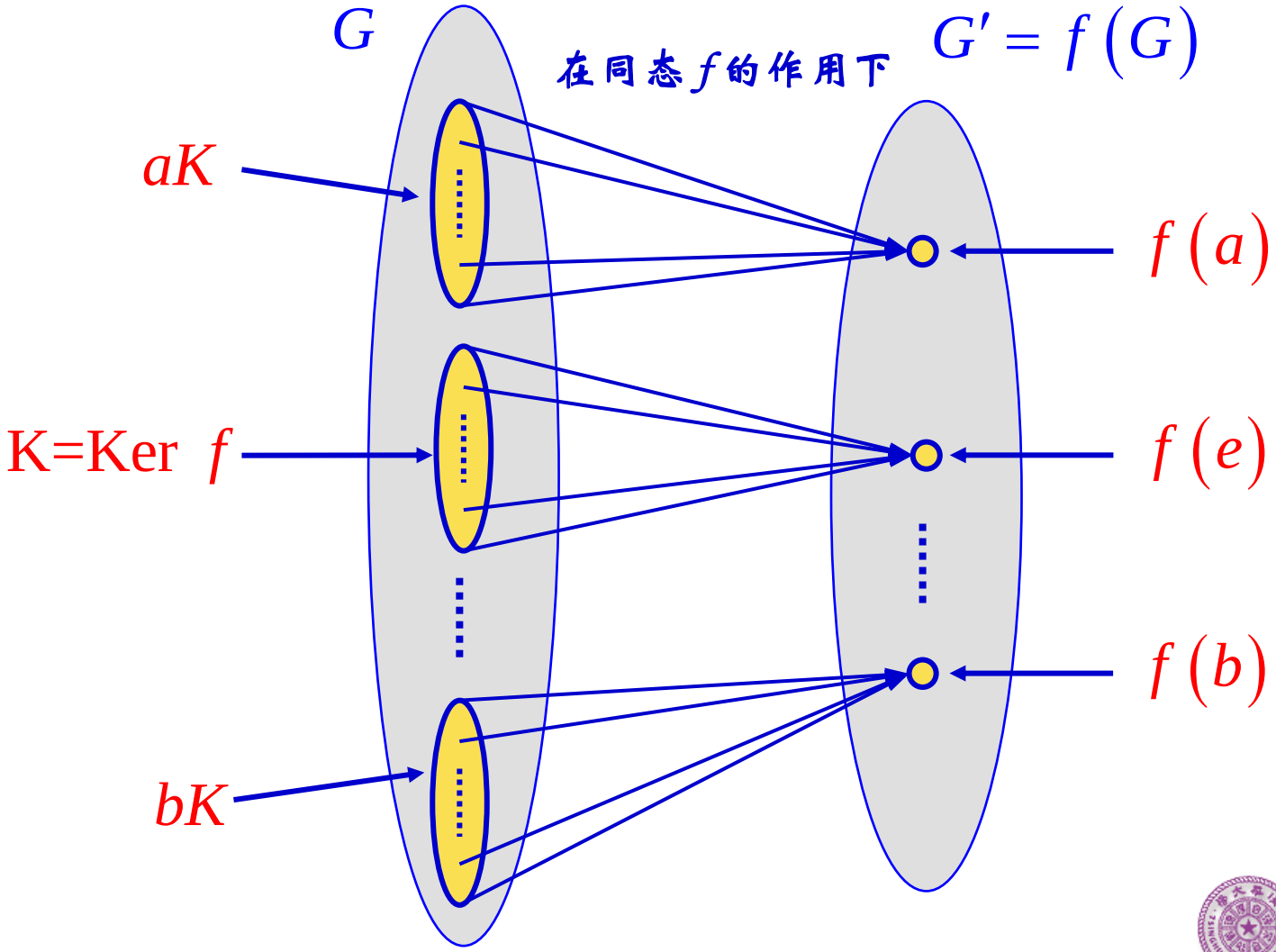
群的同态、同态基本定理

- 证明：f是G到G'的满同态 $\Rightarrow$ $G/K \cong G'$ $(K = Ker\, f)$
  - 令 $\varphi: aK \to f(a)$， 显然符合映射条件
  - $\forall x \in G'$，由于 f 是满同态，因此必定 $\exists a \in G$，使得 $f(a) = x$，且$aK \in G/K$， 即 $\varphi(aK) = f(a) = x$
  - 因此 φ 是G/K到 G' 的满射
  - 据定理8.7.6，$\varphi(aK) = \varphi(bK) = f(a) = f(b) \Leftrightarrow aK = bK$
  - 因此 φ 是G/K 到 G'的单射

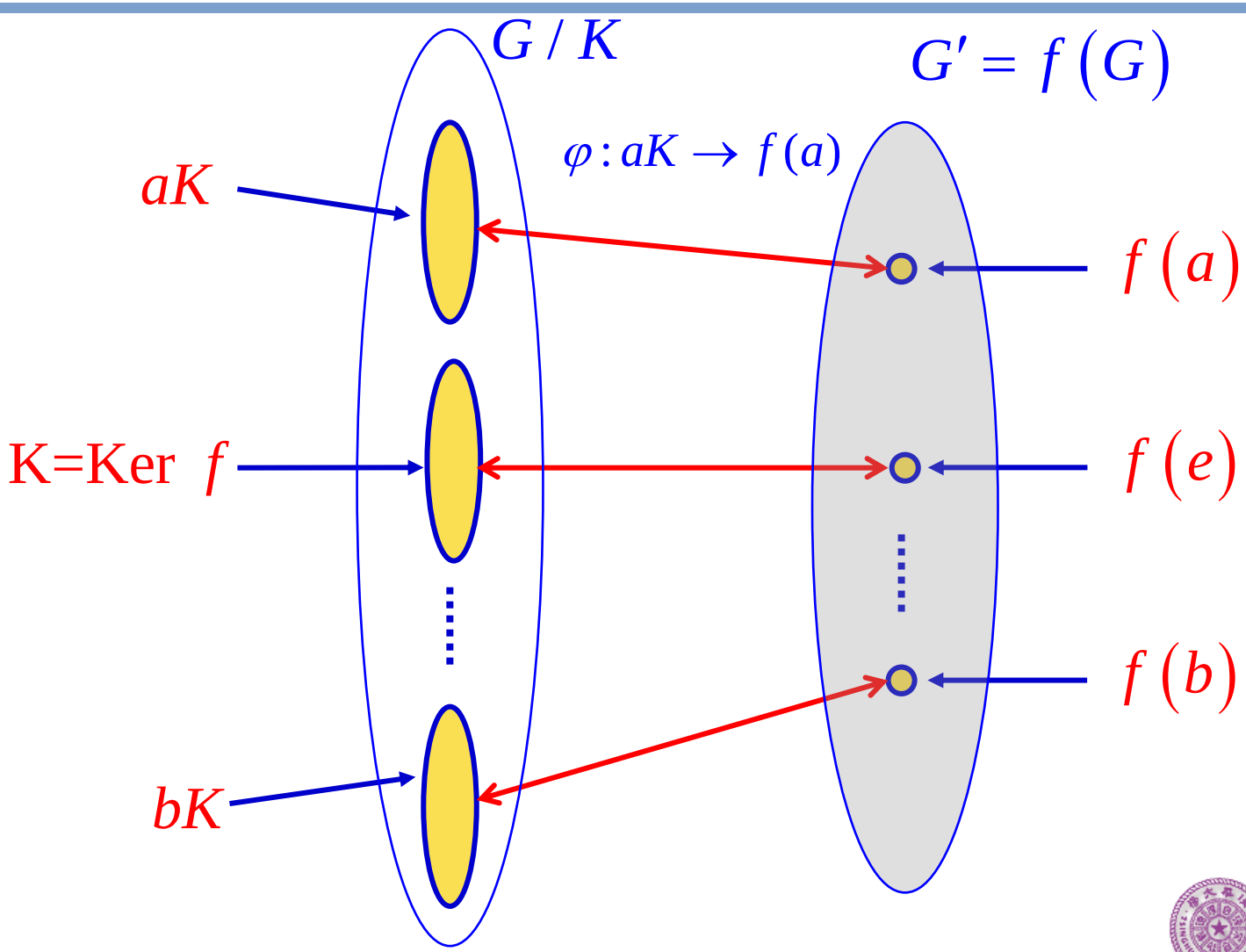
群的同态、同态基本定理

- 证明：f是G到G'的满同态 $\Rightarrow$ $G/K \cong G'$ $(K = Ker\, f)$
  - $\varphi(aKbK) = \varphi(abK) = f(ab) = f(a)f(b) = \varphi(aK)\varphi(bK)$
  - 因此φ是G/K到G'的同构映射，即$G/K \cong G'$。

群的同态、同态基本定理



群的同态、同态基本定理



群的同态象与该同态核的商群同构！

群的同态、同态基本定理-小结

- 群的同态、同态象
- 同态性质：单位元、逆元、子群
- 同态核，同态核性质
- 同态基本定理

主要内容

- 8.1 半群
- 8.2 群、群的基本性质
- 8.3 循环群 群的同构
- 8.4 变换群和置换群 Cayley定理
- 8.5 陪集和群的陪集分解 Lagrange定理
- 8.6 正规子群与商群
- 8.7 群的同态、同态基本定理
- **8.8 群的直积**

总 复 习

练习题

- 若G为非交换群，则G中存在着非单位元a和b

  $a \neq b$，且 $ab = ba$

- 群 G_1 到 G_2 存在满同态映射，H是 G_1 的子群，若

  $|H|$ 与 $|G_2|$ 互素，证明 $H \subseteq \ker\varphi$