信息安全数学基础

第三章 群

陈大江

信息与软件工程学院

3.4 正规子群、商群和同态

定义3.4.1 若H是G的子群，且对于任意元素$a \in G$，均有$aH = Ha$，则称H是G的正规子群，记为$H \lhd G$。

交换群的所有子群都是正规子群。例如：整数加法群Z是交换群，所以它的子群nZ是正规子群。

例3.4.1 设N是群G中所有满足下列条件的元素构成的集合

$$na = an, \forall a \in G, n \in N$$

那么N是G的正规子群，这个正规子群称为G的中心。

证明思路 严格按照子群和正规子群的定义进行验证。

证明：因为$\forall a \in G$,有$ea = ae$，所以 $e \in N$，N非空。又$\forall n_1, n_2 \in N$ ，有

$$n_1 a = a n_1, n_2 a = a n_2 \implies a n_2^{-1} = n_2^{-1} a \implies n_1 n_2^{-1} a = n_1 a n_2^{-1} = a n_1 n_2^{-1}$$

根据定理3.3.1，有N是G的子群。由G的每一个元素可以同N中的每一个元素交换，所以显然有$Na = aN$，即N是G的正规子群。

3.4 正规子群、商群和同态

正规子群的等价定义

定理3.4.1 设H是G的子群,$a \in G$。令$a^{-1}Ha = \{a^{-1}ha \mid h \in H\}$

则下列条件等价:

（1）H是G的正规子群;

（2）$\forall a \in G, h \in H$，有$a^{-1}ha \in H$；

（3）$\forall a \in G, a^{-1}Ha \subseteq H$；

（4）$\forall a \in G, a^{-1}Ha = H$。

3.4 正规子群、商群和同态

定理3.4.1的证明

（1）⇒（2）：H是G的正规子群，所以$\forall a \in G$，有$aH = Ha$。故$\forall h \in H$，$ha \in Ha = aH$，从而存在$h' \in H$使得 $ha = ah'$，即$a^{-1}ha = h' \in H$。

（2）⇒（3）：显然。

（3）⇒（4）：$\forall a \in G$，有$a^{-1}Ha \subseteq H$。同样,$\forall a^{-1} \in G$，也有$(a^{-1})^{-1}Ha^{-1} \subseteq H$，即$aHa^{-1} \subseteq H$，从而有 $H \subseteq a^{-1}Ha$。因此,$a^{-1}Ha = H$。

（4）⇒（1）：$Ha = aa^{-1}Ha = aH$。

商群

定理3.4.2 设H是G的正规子群，记$G/H=\{aH \mid a\in G\}$，在集合记G/H上定义运算：

$$(aH)\cdot(bH)=(ab)H$$

则上述定义的运算给出了记G/H上的一个乘法，且记G/H在这个乘法下构成群，称为G关于正规子群H的**商群**。

证明思路： 首先，要证明定理中定义的运算不依赖陪集代表元的选择。其次，要证明G/H在这个乘法下构成群。

- 证明：首先证明当$a_1H=a_2H$，$b_1H=b_2H$时，有
  $(a_1b_1)H=(a_2b_2)H$，即证：$(a_2b_2)^{-1}(a_1b_1)\in H$
  $a_1H=a_2H$，$b_1H=b_2H$ => $a_2^{-1}a_1\in H, b_2^{-1}b_1\in H$

而 $(a_2b_2)^{-1}(a_1b_1)=b_2^{-1}a_2^{-1}a_1b_1=(b_2^{-1}b_1)(b_1^{-1}(a_2^{-1}a_1)b_1)$

又H是正规子群，所以 $b_1^{-1}(a_2^{-1}a_1)b_1\in H$

从而 $(a_2b_2)^{-1}(a_1b_1)\in H$，即有$(a_1b_1)H=(a_2b_2)H$.

3.4 正规子群、商群和同态

定理3.4.2的证明

其次证明G/H上在该乘法下构成群。

（1）结合律显然满足；

（2）$\forall aH \in G/H$，存在 eH，使得$eH \cdot aH = aH \cdot eH = aH$

即 eH 是 G/H中的单位元。

（3）$\forall aH \in G/H$，则$a^{-1}H \in G/H$，

且 $a^{-1}H \cdot aH = (a^{-1}a)H = eH$

即 aH 的逆元是$a^{-1}H$ 。

综上所述，G/H所述在定理中所定义的乘法下构成群。

定义 3.4.2 群G/H称为G 关于正规子群的H 的商群。

例 3.4.2 对于正整数m ,mZ是整数加法群Z的正规子群，其所有加法陪集为

$$r+mZ=\{mk+r \mid k\in Z\},0\leq r\leq m$$

可分别用 $[0],[1],\cdots,[m-1]$ 表示这m个陪集

$$Z/mZ=\{[0],[1],\cdots,[m-1]\}$$

定义加法

$$[a]+[b]=[a+b \pmod m]$$

显然，在这个运算下，Z/mZ 构成一个加群。由于$[a]$又表示a这个整数所在的剩余类，因此，Z/mZ又称为剩余类群。

3.4 正规子群、商群和同态

为了研究群与群之间的关系，引入同态和同构的概念。

定义3.4.3 设G和G'是两个群，f是群G到G'的一个映射。如果$\forall a,b \in G$，映射满足

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

则称f是群G到G'的一个同态映射。

当该映射是满射时，称f是群G到群G'的一个满同态映射。

若该映射是一一映射，则称f是群G到群G'的一个同构映射。

3.4 正规子群、商群和同态

定义3.4.3（续）

若群 G 与群 G' 之间存在同态（同构）映射，则称群 G 和群 G' 同态（同构）。用符号

$$G \cong G'$$

表示群 G 和群 G' 同构。

G 到 G 自身的同构称为内自同构。

在满同态映射下，单位元映射到单位元，逆元映射到映射象的逆元。

同态

例3.4.3 整数加法群Z与商群Z/mZ同态。

证明：定义映射$f: Z \to Z/mZ$, $\forall a \in Z$,

$$f(a) = [a]$$

显然，这是一个满射。根据对于Z中任意两个整数a, b，有

$$f(a+b) = [a+b] = [a] + [b]$$

所以，f是整数加法群Z到商群Z/mZ的一个同态映射，即整数加法群Z与商群Z/mZ同态。

自然同态

定理3.4.4（自然同态）一个群G与它的每一个商群G/H同态。

证明：设H是G的正规子群。定义映射 $\varphi: G \to G/H$为：

$$\varphi(a) = aH$$

根据定理3.4.2很容易证明这个结论。

上述定理证明过程中定义的映射φ为群G到它的商群的自然同态。

3.4 正规子群、商群和同态

同态的象与核

定义3.4.4 设f是群G到群G'的一个同态映射，称

$$f(G)=\{f(a)\mid a\in G\}$$

为同态f的象。对于任意$a'\in G'$，集合：

$$\{a\in G\mid f(a)=a'\}$$

称为元素a'的完全逆象，记为$f^{-1}(a')$。单位元素$e'\in G'$的完全逆象$f^{-1}(e')$称为同态f的核，记为$\ker(f)$。

$f(G)$是G'的一个子群。自然同态的核为正规子群H。

同态基本定理

定理3.4.5（群同态基本定理）设f是群G到群G'的一个满同态映射，N为f的核，则N是G的一个正规子群，且

$$G/N \cong G'$$

证明思路

(1)利用正规子群的等价定义证明N是G的正规子群。

(2)构造 与G'之间的同构映射

同态基本定理的证明

证明：设e是群G的单位元，e'是群G'的单位元。又设$a,b\in N$，则有$f(a)=f(b)=e'$。

因此$f(ab^{-1})=f(a)f(b^{-1})=e'(e')^{-1}=e'$。也就是说

$$a,b\in N\Rightarrow ab^{-1}\in N$$

即N是G的子群。又$\forall c\in G,a\in N$

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

也就是说

$$\forall c\in G,a\in N\Rightarrow cac^{-1}\in N$$

所以N是G的正规子群。

定义$\psi: G/N \to G'$为$\psi(aN) = f(a)$

这个映射就是G/N与G'之间的同构映射。因为:

(1)$aN = bN \Rightarrow b^{-1}a \in N \Rightarrow e' = f(b^{-1}a) = (f(b))^{-1}f(a)$

$\Rightarrow f(a) = f(b)$，这就是说，在ψ之下G/N 的一个元素只有一个惟一的象。（映射的单值性）

（2）给定G'中的任意一个元素a'，在G中至少有一个元素a 满足$f(a) = a'$，则有$\psi(aN) = f(a) = a'$，也就是说，ψ是G/N到G'的满射。

(3)$aN \neq bN \Rightarrow b^{-1}a \notin N \Rightarrow (f(b))^{-1}f(a) \neq e' \Rightarrow f(a) \neq f(b)$。这说明$\psi$是单射。

(4)$aNbN = abN \Rightarrow \psi(aNbN) = \psi(abN) = f(ab) = f(a)f(b)$

$= \psi(aN)\psi(bN)$综上所述，有$G/N \cong G'$。（保运算）