信息安全数学基础

第二部分 第九章 群的结构

中山大学 数据科学与计算机学院 网络空间安全系

8. 生成子群与循环群

定义（生成子群）

设G是群，X是G的一个子集，设$\{H_i\}_{i\in I}$是G包含X的所有子群，则$\cap_{i\in I}H_i$被称为群G的由X生成的子群，记为$< X >$. X的元素被称为子群$< X >$的生成元. 特别地，如果$X=\{a_1,a_2,\cdots,a_n\}$，则记

$$< X >=< a_1,a_2,\cdots,a_n > .$$

进一步，如果$G=< a_1,a_2,\cdots,a_n >$，其中n为某一正整数，则称G为有限生成的.

8. 生成子群与循环群

定义（生成子群）

设G是群, X是G的一个子集, 设$\{H_i\}_{i\in I}$是G包含X的所有子群, 则$\cap_{i\in I}H_i$被称为群G的由X生成的子群, 记为$< X >$. X的元素被称为子群$< X >$的生成元. 特别地, 如果$X=\{a_1,a_2,\cdots,a_n\}$, 则记

$$< X > = < a_1,a_2,\cdots,a_n > .$$

进一步, 如果$G=< a_1,a_2,\cdots,a_n >$, 其中n为某一正整数, 则称G为有限生成的.

定义（循环群）

设G是群, 如果存在$a\in G$使得$G=< a >$, 则称G为a的生成的循环群.

- 循环群是交换群.

循环群和它的生成元

循环群和它的生成元

- 因为$\mathbb{Z}_7 = \{0 \cdot 1, 1 \cdot 1, 2 \cdot 1, 3 \cdot 1, 4 \cdot 1, 5 \cdot 1, 6 \cdot 1\}$, 所以$\mathbb{Z}_7$关于模7的加法构成的有限群可以由其中的元素1生成.

循环群和它的生成元

- 因为$\mathbb{Z}_7 = \{0\cdot 1, 1\cdot 1, 2\cdot 1, 3\cdot 1, 4\cdot 1, 5\cdot 1, 6\cdot 1\}$, 所以$\mathbb{Z}_7$关于模7的加法构成的有限群可以由其中的元素1生成.
- 因为$\mathbb{Z}_7 \setminus \{0\} = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\} =$

循环群和它的生成元

- 因为$\mathbb{Z}_7 = \{0 \cdot 1, 1 \cdot 1, 2 \cdot 1, 3 \cdot 1, 4 \cdot 1, 5 \cdot 1, 6 \cdot 1\}$, 所以$\mathbb{Z}_7$关于模7的加法构成的有限群可以由其中的元素1生成.
- 因为$\mathbb{Z}_7 \setminus \{0\} = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\} = \{3^0 = 1, 3^2 = 2, 3^1 = 3, 3^4 = 4, 3^5 = 5, 3^3 = 6\}$,

循环群和它的生成元

- 因为$\mathbb{Z}_7 = \{0 \cdot 1, 1 \cdot 1, 2 \cdot 1, 3 \cdot 1, 4 \cdot 1, 5 \cdot 1, 6 \cdot 1\}$, 所以$\mathbb{Z}_7$关于模7的加法构成的有限群可以由其中的元素1生成.
- 因为$\mathbb{Z}_7 \setminus \{0\} = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\} = \{3^0 = 1, 3^2 = 2, 3^1 = 3, 3^4 = 4, 3^5 = 5, 3^3 = 6\}$, 所以$\mathbb{Z}_7 \setminus \{0\}$关于模7的乘法构成的有限群可以由其中的元素3生成.

循环群和它的生成元

- 因为$\mathbb{Z}_7 = \{0\cdot 1, 1\cdot 1, 2\cdot 1, 3\cdot 1, 4\cdot 1, 5\cdot 1, 6\cdot 1\}$, 所以$\mathbb{Z}_7$关于模7的加法构成的有限群可以由其中的元素1生成.
- 因为$\mathbb{Z}_7\setminus\{0\} = \mathbb{Z}_7^* = \{1,2,3,4,5,6\} = \{3^0 = 1, 3^2 = 2, 3^1 = 3, 3^4 = 4, 3^5 = 5, 3^3 = 6\}$, 所以$\mathbb{Z}_7\setminus\{0\}$关于模7的乘法构成的有限群可以由其中的元素3生成.

定义（循环群）

如果一个群G的每一个元素都是G的某一个固定元素a的乘方或者是G的某一个固定元素a的倍数, 即

$$G = \{a^0, a^1, a^2, a^3, a^4, \cdots\},$$

或

$$G = \{0a, a, 2a, 3a, 4a, \cdots\},$$

则称G为循环群, G是由元素a生成的, 用符号$G = < a >$来表示.

更多的(乘法)循环群和它们的生成元

- $\mathbb{Z}_5 \setminus \{0\} = \mathbb{Z}_5^* = \{1, 2, 3, 4\} =$

更多的(乘法)循环群和它们的生成元

- $\mathbb{Z}_5 \setminus \{0\} = \mathbb{Z}_5^* = \{1,2,3,4\} = \{2^0 = 1, 2^1 = 2, 2^3 = 3, 2^2 = 4\}$, 它关于模5的乘法构成的有限群可以由其中的元素2生成.

更多的(乘法)循环群和它们的生成元

- $\mathbb{Z}_5 \setminus \{0\} = \mathbb{Z}_5^* = \{1, 2, 3, 4\} = \{2^0 = 1, 2^1 = 2, 2^3 = 3, 2^2 = 4\}$, 它关于模5的乘法构成的有限群可以由其中的元素2生成.
- $\mathbb{Z}_{11} \setminus \{0\} = \mathbb{Z}_{11}^* = \{2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6\}$, 它关于模11的乘法构成的有限群可以由其中的元素2生成.

更多的(乘法)循环群和它们的生成元

- $\mathbb{Z}_5 \setminus \{0\} = \mathbb{Z}_5^* = \{1,2,3,4\} = \{2^0 = 1, 2^1 = 2, 2^3 = 3, 2^2 = 4\}$, 它关于模5的乘法构成的有限群可以由其中的元素2生成.
- $\mathbb{Z}_{11} \setminus \{0\} = \mathbb{Z}_{11}^* = \{2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6\}$, 它关于模11的乘法构成的有限群可以由其中的元素2生成.
- $\mathbb{Z}_7^*$可以由2生成吗?

更多的(乘法)循环群和它们的生成元

- $\mathbb{Z}_5 \setminus \{0\} = \mathbb{Z}_5^* = \{1, 2, 3, 4\} = \{2^0 = 1, 2^1 = 2, 2^3 = 3, 2^2 = 4\}$, 它关于模5的乘法构成的有限群可以由其中的元素2生成.
- $\mathbb{Z}_{11} \setminus \{0\} = \mathbb{Z}_{11}^* = \{2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6\}$, 它关于模11的乘法构成的有限群可以由其中的元素2生成.
- $\mathbb{Z}_7^*$可以由2生成吗? 不能. $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 1$, 元素2总是无法生成3，5和6.

更多的(乘法)循环群和它们的生成元

- $\mathbb{Z}_5 \setminus \{0\} = \mathbb{Z}_5^* = \{1,2,3,4\} = \{2^0 = 1, 2^1 = 2, 2^3 = 3, 2^2 = 4\}$, 它关于模5的乘法构成的有限群可以由其中的元素2生成.
- $\mathbb{Z}_{11} \setminus \{0\} = \mathbb{Z}_{11}^* = \{2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6\}$, 它关于模11的乘法构成的有限群可以由其中的元素2生成.
- $\mathbb{Z}_7^*$可以由2生成吗? 不能. $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 1$, 元素2总是无法生成3，5和6.
- $\mathbb{Z}_{11}^*$可以由3生成吗?

更多的(乘法)循环群和它们的生成元

- $\mathbb{Z}_5 \setminus \{0\} = \mathbb{Z}_5^* = \{1,2,3,4\} = \{2^0 = 1, 2^1 = 2, 2^3 = 3, 2^2 = 4\}$, 它关于模5的乘法构成的有限群可以由其中的元素2生成.
- $\mathbb{Z}_{11} \setminus \{0\} = \mathbb{Z}_{11}^* = \{2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6\}$, 它关于模11的乘法构成的有限群可以由其中的元素2生成.
- $\mathbb{Z}_7^*$可以由2生成吗? 不能. $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 1$, 元素2总是无法生成3，5和6.
- $\mathbb{Z}_{11}^*$可以由3生成吗? 不能. 因为$3^5 = 1 \bmod 11$.
- $\mathbb{Z}_{11}^*$可以由5生成吗?

更多的(乘法)循环群和它们的生成元

- $\mathbb{Z}_5 \setminus \{0\} = \mathbb{Z}_5^* = \{1, 2, 3, 4\} = \{2^0 = 1, 2^1 = 2, 2^3 = 3, 2^2 = 4\}$, 它关于模5的乘法构成的有限群可以由其中的元素2生成.
- $\mathbb{Z}_{11} \setminus \{0\} = \mathbb{Z}_{11}^* = \{2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6\}$, 它关于模11的乘法构成的有限群可以由其中的元素2生成.
- $\mathbb{Z}_7^*$可以由2生成吗? 不能. $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 1$, 元素2总是无法生成3，5和6.
- $\mathbb{Z}_{11}^*$可以由3生成吗? 不能. 因为$3^5 = 1 \bmod 11$.
- $\mathbb{Z}_{11}^*$可以由5生成吗? 还是不可以的. 因为$5^5 = 1 \bmod 11$.

群元素的阶和群的本原元

定义（群元素的阶）

1. 设G是一个乘法群，对任意的$a \in G$，a的阶是使得$a^k = 1$的最小正整数k.
2. 设G是一个加法群，对任意的$a \in G$，a的阶是使得$ka = 0$的最小正整数k.
3. 如果对于a不存在满足上述条件的最小正整数，则定义a的阶为无穷大∞，有些书籍和文献中也定义a的阶为0.
4. 如果a的阶k恰好等于整个群G的阶，则称元素a是群G的一个本原元(生成元).
5. 一般地，群元素a的阶记为$\mathrm{ord}(a)$.

群元素的阶和群的本原元

定义（群元素的阶）

1. 设G是一个乘法群，对任意的$a \in G$，a的阶是使得$a^k = 1$的最小正整数k.
2. 设G是一个加法群，对任意的$a \in G$，a的阶是使得$ka = 0$的最小正整数k.
3. 如果对于a不存在满足上述条件的最小正整数，则定义a的阶为无穷大∞，有些书籍和文献中也定义a的阶为0.
4. 如果a的阶k恰好等于整个群G的阶，则称元素a是群G的一个本原元*(生成元)*.
5. 一般地，群元素a的阶记为$\mathrm{ord}(a)$.

设p为素数，在$\mathbb{Z}_p^*$中，元素a的阶实际上是a作为整数在模p下的指数.

- 在$\mathbb{Z}_5^*$中，元素2的阶(指数)为4。
- 在$\mathbb{Z}_7^*$中，元素3的阶(指数)为6，而元素2阶(指数)为3。
- 在$\mathbb{Z}_{11}^*$中，元素2的阶(指数)为10，而元素3和元素5的阶(指数)都等于5。

群元素的阶和群的本原元

定义（群元素的阶）

1. 设G是一个乘法群，对任意的$a \in G$，a的阶是使得$a^k = 1$的最小正整数k.
2. 设G是一个加法群，对任意的$a \in G$，a的阶是使得$ka = 0$的最小正整数k.
3. 如果对于a不存在满足上述条件的最小正整数，则定义a的阶为无穷大∞，有些书籍和文献中也定义a的阶为0.
4. 如果a的阶k恰好等于整个群G的阶，则称元素a是群G的一个本原元*(生成元)*.
5. 一般地，群元素a的阶记为$\mathrm{ord}(a)$.

设p为素数，在$\mathbb{Z}_p^*$中，元素a的阶实际上是a作为整数在模p下的指数.

- 在$\mathbb{Z}_5^*$中，元素2的阶(指数)为4。
- 在$\mathbb{Z}_7^*$中，元素3的阶(指数)为6，而元素2阶(指数)为3。
- 在$\mathbb{Z}_{11}^*$中，元素2的阶(指数)为10，而元素3和元素5的阶(指数)都等于5。

- 2是$\mathbb{Z}_5^*$的一个生成元，其阶(指数)为$\varphi(5) = 4$.
- 3是$\mathbb{Z}_7^*$的一个生成元，其阶(指数)为$\varphi(7) = 6$，而2不是$\mathbb{Z}_7^*$的生成元.
- 2都是$\mathbb{Z}_{11}^*$的生成元，其阶(指数)为$\varphi(11) = 10$. 而和3和5都不是$\mathbb{Z}_{11}^*$的生成元.

群的同态

定义

设$(\mathbb{G}, \cdot)$ 和$(\mathbb{G}', \circ)$是两个群. 如果存在映射$f : \mathbb{G} \longrightarrow \mathbb{G}'$使得:

$$\forall a, b \in \mathbb{G} : f(a \cdot b) = f(a) \circ f(b),$$

则称f是一个$\mathbb{G}$到$\mathbb{G}'$的同态映射, 并称$\mathbb{G}$与$\mathbb{G}'$关于f同态*(homomorphism)*.

- 如果f是单射, 则称f是单同态;
  如果f是满射,则称f是满同态;
  如果f是自映射, 则称f是自同态.
- 称$Imf = f(G)$为G在f下的同态像.

群的同构

定义

设$(\mathbb{G},\cdot)$, $(\mathbb{G}',\circ)$是两个群, 如果存在双射$f:\mathbb{G}\longrightarrow\mathbb{G}'$使得:

$$\forall a,b\in\mathbb{G}: f(a\cdot b)=f(a)\circ f(b),$$

则称f是一个$\mathbb{G}$到$\mathbb{G}'$的同构映射, 并称$\mathbb{G}$与$\mathbb{G}'$关于f同构*(isomorphism)*, 记做$\mathbb{G}\cong\mathbb{G}'$.

- 同构映射保持了群的运算关系, 还使得两个群的所有代数性质都一一对应.
  1. 它把$\mathbb{G}$中的单位元e映射到$\mathbb{G}'$中的单位元e':$e'=f(e)$;
  2. 如果它把$\mathbb{G}$中的任一元素a映射到$\mathbb{G}'$中的元素$f(a)$中, 则它也会把a的逆元a^{-1}映射到$f(a)$的逆元$f(a)^{-1}$: $f(a^{-1})=(f(a))^{-1}$
  3. 把$\mathbb{G}$中的子群映射成$\mathbb{G}'$中的子群: $H\leq G\Longleftrightarrow f(H)\leq\mathbb{G}'$;
  4. 保持元素的阶不变: $\mathrm{ord}(a)=\mathrm{ord}(f(a))$;
  5. 保持元素的可交换性:$a\cdot b=b\cdot a\Leftrightarrow f(a)\circ f(b)=f(b)\circ f(a)$
  6. 等等......
- 如果两个群同构, 可以将它们看作完全相同, 仅在于两个集合中的元素表示符号不一样.

同构的例子

例1：设$G=(R^+,\cdot),G'=(R,+)$，其中R^+是所有正实数的集合，证明$G\cong G'$.

证明:
作G到G'的关系

$$f:x\mapsto \lg x,(R^+\to R).$$

显然这是一个映射．因为

$$\lg x_1=\lg x_2\Rightarrow x_1=x_2.$$

所以f是单射．对于任意$b\in G'$，取$x=10^b$，则$f(x)=b$，所以f也是满射．
于是，G是一一映射．

$$\forall x_1,x_2\in G,f(x_1\cdot x_2)=\lg(x_1\cdot x_2)=\lg x_1+\lg x_2=f(x_1)+f(x_2)$$

所以由定义知$G\cong G'$.

同构的例子

例2: 复数域上的所有n次单位根的集合

$$U_n = \{e^{\frac{2k\pi}{n}i} \mid k = 0, 1, \cdots, n-1\}$$

关于复数的乘法构成群. 其中e是自然常数, 约等于2.71828. 证明$(U_n, \cdot) \cong (\mathbb{Z}_n, +)$.

证明: 作$\mathbb{Z}_n$到U_n的关系

$$f : \bar{k} \mapsto e^{\frac{2k\pi}{n}i}, k = 0, 1, \cdots, n-1.$$

因为$\bar{k_1} = \bar{k_2} \Leftrightarrow k_1 = k_2 + qn \Leftrightarrow e^{\frac{2k_1\pi}{n}i} = e^{\frac{2k_2\pi}{n}i}$, 所以$f$是一一映射.
并且

$$f(\bar{k_1} + \bar{k_2}) = f(\overline{k_1 + k_2}) = e^{\frac{2(k_1+k_2)\pi}{n}i} = e^{\frac{2k_1\pi}{n}i} e^{\frac{2k_2\pi}{n}i} = f(\bar{k_1})f(\bar{k_2})$$

所以由定义知$\mathbb{Z}_n \cong U_n$.

同态的例子

- 设$\mathbb{R}$实数集合关于加法构成的群, $\mathbb{R}^*=\mathbb{R}\setminus\{0\}$非零实数集合关于乘法构成的群, 则$\mathbb{R}$和$\mathbb{R}^*$关于映射$f$同态, 其中$f: a\mapsto e^a$, 且$e$是自然常数.
- 设$\mathbb{Z}$整数集合关于加法构成的群, $\mathbb{Z}/n\mathbb{Z}$是模n的剩余类群, 则$\mathbb{Z}$和$\mathbb{Z}/n\mathbb{Z}$关于映射f同态, 其中$f: k\mapsto k+n\mathbb{Z}$.
- 设$\mathbb{Z}$整数集合关于加法构成的群, $\mathbb{Z}_p^*$是模p的简化剩余系关于模p的乘法构成的群, 则$\mathbb{Z}$和$\mathbb{Z}_p^*$关于映射f同态, 其中$f: n\mapsto g^n$, 且g是模p的原根.
- 设$\mathbb{Z}$整数集合关于加法构成的群, $U_n=\{e^{\frac{2k\pi}{n}i}\mid k=0,1,\cdots,n-1\}$是复数域上的所有$n$次单位根的集合关于复数的乘法构成的群, 则$\mathbb{Z}$和$U_n$关于映射$f$同态, 其中$f: k\mapsto e^{\frac{2k\pi}{n}i}$.
- 设G是一个乘法群, a是G中的一个元素, 作映射$f: b\mapsto aba^{-1}$, 则f是G到G自身的同态映射.

同态的一些性质

1. $e' = f(e)$
2. $f(a^{-1}) = (f(a))^{-1}$
3. $H \leq G \iff f(H) \leq f(G)$
4. $H \trianglelefteq G \iff f(H) \trianglelefteq f(G)$

例: 设G是群, $H \trianglelefteq G$, $G' = G/H$, 作G到G/H映射:

$$\varphi : a \mapsto aH.$$

因为$\varphi(ab) = abH = aHbH = \varphi(a)\varphi(b)$, 所以$\varphi$是同态, 而且是满同态.
所以$G \sim G/H$. 此同态称为群G到它的商群的自然同态.

同态映射的核(kernel)

定义

设f是G到G'的同态映射, e'是G'的单位元. G的子集

$$f^{-1}(e') = \{a \mid a \in G, f(a) = e'\}$$

被称为同态映射f的**核(kernel)**, 记作$\ker f$, 即$\ker f$是G'单位元的对于f原像集合.

- 设实数集合$\mathbb{R}$关于加法构成的群, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$是非零实数集合关于乘法构成的群, 则$\mathbb{R}$和$\mathbb{R}^*$关于映射$f$ 同态, 其中

$$f : a \mapsto e^a,$$

且e是自然常数. 这里, f的核是

同态映射的核(kernel)

定义

设f是G到G'的同态映射，e'是G'的单位元. G的子集

$$f^{-1}(e') = \{a \mid a \in G, f(a) = e'\}$$

被称为同态映射f的**核(kernel)**，记作$\ker f$，即$\ker f$是G'单位元的对于f原像集合.

- 设实数集合$\mathbb{R}$关于加法构成的群，$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$是非零实数集合关于乘法构成的群，则$\mathbb{R}$和$\mathbb{R}^*$关于映射$f$ 同态，其中

$$f : a \mapsto e^a,$$

  且e是自然常数. 这里，f的核是$\{0\}$.
- 设$\mathbb{Z}$整数集合关于加法构成的群，$\mathbb{Z}_p^*$是模p的简化剩余系关于模p的乘法构成的群，g是模p的原根，则$\mathbb{Z}$和$\mathbb{Z}_p^*$关于映射f同态，其中

同态映射的核(kernel)

定义

设f是G到G'的同态映射, e'是G'的单位元. G的子集

$$f^{-1}(e') = \{a \mid a \in G, f(a) = e'\}$$

被称为同态映射f的核*(kernel)*, 记作$\ker f$, 即$\ker f$是G'单位元的对于f原像集合.

- 设实数集合$\mathbb{R}$关于加法构成的群, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$是非零实数集合关于乘法构成的群, 则$\mathbb{R}$和$\mathbb{R}^*$关于映射$f$ 同态, 其中

$$f : a \mapsto e^a,$$

  且e是自然常数. 这里, f的核是$\{0\}$.
- 设$\mathbb{Z}$整数集合关于加法构成的群, $\mathbb{Z}_p^*$是模p的简化剩余系关于模p的乘法构成的群, g是模p的原根, 则$\mathbb{Z}$和$\mathbb{Z}_p^*$关于映射f同态, 其中

$$f : n \mapsto g^n.$$

  这里, f的核是

同态映射的核(kernel)

定义

设f是G到G'的同态映射, e'是G'的单位元. G的子集

$$f^{-1}(e') = \{a \mid a \in G, f(a) = e'\}$$

被称为同态映射f的核(kernel), 记作$\ker f$, 即$\ker f$是G'单位元的对于f原像集合.

- 设实数集合$\mathbb{R}$关于加法构成的群, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$是非零实数集合关于乘法构成的群, 则$\mathbb{R}$和$\mathbb{R}^*$关于映射$f$ 同态, 其中

$$f: a \mapsto e^a,$$

  且e是自然常数. 这里, f的核是$\{0\}$.
- 设$\mathbb{Z}$整数集合关于加法构成的群, $\mathbb{Z}_p^*$是模p的简化剩余系关于模p的乘法构成的群, g是模p的原根, 则$\mathbb{Z}$和$\mathbb{Z}_p^*$关于映射f同态, 其中

$$f: n \mapsto g^n.$$

  这里, f的核是$(p-1)\mathbb{Z}$.

命题（核的性质）

设f是G到G'的同态，$K=Kerf$，则:

1. $K \trianglelefteq G$
2. $\forall a' \in Imf$，若$f(a)=a'$，则$f^{-1}(a')=aK$
3. f是单同态 $\iff K=e$

(1) K是G的子群，因为$\forall g \in G$，$k \in K$，所以有

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

于是$gkg^{-1} \in K$，因而$K \trianglelefteq G$.
(2) $\forall k \in K$ 有$f(ak)=f(a)f(k)=a'$，所以$ak \in f^{-1}(a')$，因而$aK \subseteq f^{-1}(a')$.
反之，$\forall x \in f^{-1}(a')$ 有$f(x)=a'$，即$f(x)=f(a)$，$f(a)^{-1} \cdot f(x)=e'$，得$a^{-1}x \in K$，因而$x \in aK$，$f^{-1}(a') \subseteq aK$. 所以，$f^{-1}(a')=aK$.
(3) f是单射 $\iff \forall a' \in f(G)$有

$$|f^{-1}(a')|=1 \iff |aK|=1 \iff |K|=1 \iff K=\{e\}.$$

定理（同态基本定理）

设f是G到G'的满同态，$K = \ker f$，则:

1. $G/K \cong G'$
2. 设φ是G到G/K的自然同态，则存在G/K到G'的同构σ使$f = \sigma\varphi$.

(1) 设$G/K = \{gK \mid g \in G\}$，作$G/K$到$G'$对应关系$\sigma : gK \mapsto f(g)$. 因为

$$g_1K = g_2K \iff g_1^{-1}g_2 \in K \iff f(g_1^{-1}g_2) = e' \iff f(g_1) = f(g_2),$$

所以f是映射且是单射. 对于任意的$b \in G'$，由于f是满同态，存在$a \in G$，使$f(a) = b$，所以$aK \in G/K$，所以$aK \in G/K$ 使$\sigma(aK) = f(a) = b$. 所以σ 是满射.

$$\sigma(g_1Kg_2K) = \sigma(g_1g_2K) = f(g_1g_2) = f(g_1)f(g_2) = \sigma(g_1K)\sigma(g_1K)$$

所以σ是同构映射，$G/K \cong G'$.

(2) 取(1)中所述的G/K到G'的同态映射$\sigma : gK \mapsto f(g)$，则对于任意的$x \in G$ 有:

$$(\sigma\varphi)(x) = \sigma(\varphi(x)) = \sigma(xK) = f(x)$$

所以$\sigma\varphi = f$.

定理

在同构的意义下，循环群的结构是完全确定的. 设$\mathbb{G} =< a >$是循环群，运算记为‘$\cdot$’.
如果$\mathrm{ord}(a) = \infty$，即$\mathbb{G}$是一个无限循环群，则$(\mathbb{G}, \cdot) \cong (\mathbb{Z}, +)$，即同构于整数加群.
如果$\mathrm{ord}(a) = n$，即$\mathbb{G}$是一个n阶循环群，则$(\mathbb{G}, \cdot) \cong (\mathbb{Z}_n, +)$，即同构于模$n$剩余类群.

- 如果$\mathbb{G}$是无限循环群时，$\mathbb{G} = \{a^k \mid k \in \mathbb{Z}\}$，此时可以建立双射

$$f : \mathbb{G} \longrightarrow \mathbb{Z}, f(a^k) = k,$$

且$f(a^i \cdot a^j) = f(a^{i+j}) = i + j = f(a^i) + f(a^j)$，所以同构.

- 如果$\mathbb{G}$是有限循环群时，$\mathbb{G} = \{a^0, a^1, a^2, \cdots, a^{n-1}\}$，此时可以建立双射

$$f : \mathbb{G} \longrightarrow \mathbb{Z}_n, f(a^k) = k, k = 0, 1, 2, \cdots, n-1,$$

且$f(a^i \cdot a^j) = f(a^{i+j}) = i + j = f(a^i) + f(a^j)$，所以同构.

群小结

1. 理解群, 子群, 陪集, 正规子群, 商群, 对称群, 置换群和循环群的基本概念.
2. 理解群的同态与同构的基本概念, 理解同态核的基本概念, 理解理解群同态基本定理的结论.
3. 给定集合和运算能够判断是否构成群, 给定群的子集合能够判断是否构成子群, 以及能判断两个群是否同态或同构.
4. 理解群的阶和群元素的阶的基本概念, 以及Lagrange定理的结论.
5. 理解无限循环群同构于整数加群, 而n阶循环群同构于模n剩余类群, 能够判断一个群是否为循环群.

作业

1. 验证全体2×2非奇异有理矩阵对于矩阵乘法构成群, 并分别确定矩阵
$$A=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{和} \quad B=\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix},$$
以及矩阵AB在该群中的阶.
2. 给出4元置换群的一个3阶子群.
3. 设H是群G的有限子集, 且对于任何$a,b\in H$都有$ab\in H$, 证明H是G的子群.
4. 设K,N是G的子群, 且$N\trianglelefteq G$, 证明$N\cap K\trianglelefteq K$且$N\trianglelefteq K\times N$.
5. 证明循环群的商群一定是循环群.
6. 设p是奇素数, 选择合适的运算, 使得$(p-1)\mathbb{Z}$和$\mathbb{Z}/p\mathbb{Z}$是两个同态的群, 并求同态映射的核.
7. 证明素数阶群一定是循环群.
8. 设p是奇素数, 证明$\mathbb{Z}/p^2\mathbb{Z}$中的所有可逆元对于模p^2的乘法构成一个循环群, 并求该群的阶.