第二章 代数基础

第一部分 群

2.1 群的定义与例子

2.2 子群、正规子群与商群

2.3 群的同态与同构

第二章 代数基础

第一部分 群

2.1 群的定义与例子

2.1.1 群的定义

2.1.2 群的性质

2.2 子群、正规子群与商群

2.3 群的同态与同构

2.1.1 第一阶段学习目标

- 能描述代数运算概念
- 能列出几种最常见的代数运算
- 能判断代数运算

2.1.1 群的定义–代数运算

定义1.1 设 M 是一个非空集合，如果存在一个对应规则 f，使得对 M 中任意两个元素 a 和 b，在 M 中都有唯一确定的元素 c 与它们对应，则称 f 为 M 上的一个代数运算（二元运算），记作

$c = f(a, b)$，或简记为 $c = a \cdot b$

问：自然数集上的加法(减法)运算是不是代数运算？

2. 1. 1 群的定义-代数运算

- 判断集合 M 上运算 · 为代数运算方法

(1)如果是，则需要证明

$$\forall a,b \in \mathrm{M} \Rightarrow a \cdot b \in \mathrm{M}$$

(2)如果不是，则需要找到 ***a, b***

$$a,b \in \mathrm{M}，\ a \cdot b \notin \mathrm{M}$$

2.1.1 群的定义-代数运算

- 哪些是代数运算？

（1）自然数集 N上的乘法运算；

（2）整数集 Z上的加法（减法、乘法、除法）运算；

（3）有理数集 Q上的加法（减法、乘法、除法）运算；

（4）实数上全体 **n**阶方阵的加法与乘法运算。

（5）实数上全体 **n**阶可逆方阵的加法与乘法运算。

2.1.1 群的定义-代数运算

- 常见基本代数运算

（1）自然数集 N 上的加法、乘法运算；

（2）整数集 Z 上的加法、减法与乘法运算；

（3）有理数集 Q 上的加法、减法和乘法运算；

（4）非零有理数集 Q^* 上的乘法与除法运算；

（5）有理数、实数上全体 n阶方阵的加法与乘法运算。

（6）有理数、实数上全体 n阶可逆方阵乘法运算。

2.1.1 群的定义-代数运算

- 已知集合，新的运算

(1)实数集合上运算

$$a \square b = a + b - 1$$

(2)整数集合上运算

$$a \# b = a \times b - a + 5$$

2.1.1 群的定义-代数运算

- 新的集合，新的运算

(1)大于0小于97且与97互素的整数集合：

$$G = \{a \mid 0 < a < 97,\ (a,97) = 1\}$$

如下运算为代数运算：

$$a \otimes b = a \times b \mod 97$$

$$a \oplus b = a + b \mod 97 \quad ?\ ?$$

2.1.1 群的定义-代数运算

定义1.2 设 $\boldsymbol{n}$ 是大于1的任意正整数，剩余类集 $\boldsymbol{Z_n}$ 定义为 $\boldsymbol{Z_n = \{0, 1, 2, \dots, n-1\}}$。

- 集合 $\boldsymbol{Z_n}$ 中如下两种运算为代数运算：

模 $\boldsymbol{n}$ 的加法：$\boldsymbol{a \oplus b = a + b \mod n}$

模 $\boldsymbol{n}$ 的乘法：$\boldsymbol{a \otimes b = a \times b \mod n}$

2.1.1 第二阶段学习目标

- 能描述群的定义
- 能判断(并证明)集合关于某运算是否构成群
- 能列出几种最常见的群

定义1.3 设 G 是一个非空集合，$\cdot$ 是 G 上的一个代数运算，如果该运算满足如下三条性质：

（1）结合律：$\forall a,b,c\in G,\qquad (a\cdot b)\cdot c=a\cdot(b\cdot c)$

（2）有单位元：$\exists\, e\in G,\ \forall a\in G,\quad e\cdot a=a\cdot e=a$

（3）有逆元：对 $\forall a\in G$, 存在 $b\in G$ 使得

$$a\cdot b=b\cdot a=e$$

则称 $(G,\ \cdot)$ 为一个**群（Group）**。

注： 在群只有一个运算时可简称 G 为一个群。

2.1.1 群的定义—群的定义

定义 幺元（单位元）、零元

设 $\cdot$ 是定义在集合 A 上的二元运算，

- 如果有一个元素 $e \in A$，对于任意的 $x \in A$ 都有

$$e \cdot a = a \cdot e = a$$

  则称 e 是 A 中关于运算 $\cdot$ 的单位元（或幺元）。

- 如果有一个元素 $\theta \in A$，对于任意的 $x \in A$ 都有

$$\theta \cdot a = a \cdot \theta = \theta$$

  则则称 θ 为 A 中关于运算 $\cdot$ 的零元。

2.1.1 群的定义−群的定义

定理

设 $\langle A, *\rangle$ 是一个代数系统，且 $|A| > 1$。若该代数系统中存在幺元 e 和零元 θ，那么

$$\theta \neq e$$

证 （反证法）若 $\theta = e$，则对任意的 $x \in A$，必有

$$x = e * x = \theta * x = \theta = e$$

矛盾。

2.1.1 群的定义–常见群的例子

例1 整数加群，有理数加群，实数加群。

例2 非零有理数关于乘法构成群，非零实数关于乘法构成群。

例3： 整数、有理数、实数上n阶方阵加群。有理数、实数上n阶可逆方阵乘法群。

2.1.1 群的定义—常见群的例子

例4：全体整数关于如下运算@构成群

$$a@b=a+b-1$$

例5 集合的元素不一定是数，下面是集合元素为二阶方阵的例子：

$$\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix},\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\right\}$$

该集合对于矩阵的普通乘法是一个群，单位元是

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

2.1.1 群的定义—常见群的例子

例6　设 n 是大于1的任意正整数，剩余类集

$$Z_n=\{0,\ 1,\ 2,\ \cdots,\ n-1\}$$

关于如下模 n 的加法运算为群：

$$a\oplus b= a+b \mod n$$

例7　设 n 是大于1的任意正整数，集合

$$Z_n^{\phi}=\{a \mid a\in Z_n,\ (a,n)=1\}$$

关于如下模 n 的乘法运算为群：

$$a\otimes b = a\times b \mod n$$

注：单位元为 1，$\boldsymbol{a}$ 的逆元 $\boldsymbol{a^{-1}}$ 满足

$$\boldsymbol{a\times a^{-1}=1\ (\mathrm{mod}\ n)}$$

如 $\boldsymbol{n=7}$，$\boldsymbol{3^{-1}=5 \bmod 7}$。

2.1.1 群的定义—常见群的例子

- 当n为素数时，则 $Z_n^{\phi}=Z_n^{*}=Z_n\setminus\{0\}$。对已知的 $a,b\in Z_n^{*}$，求整数 x，使

$$a^{x}=b \mod n$$

成立的问题为离散对数问题。

- 该问题被应用于：**DH**密钥交换协议、**ElGamal**公钥密码算法、**DSA**数字签名算法等

2.1.1 群的定义—常见群的例子

例8 **一般线性群：** $GL(n,\ R)=\left\{A\in R^{n\times n},\ \ |A|\neq 0\right\}$

特殊线性群： $SL(n,R)=\left\{A\,\middle|\,A\in R^{n\times n},\ |A|=1\right\}$

证： 若 $A,B\in GL(n,R)$，则 $|A|\neq 0,|B|\neq 0$，从而有

$$|AB|=|A||B|\neq 0$$

故 $AB\in GL(n,R)$，封闭性成立。矩阵乘法满足结合律，单位矩阵 I 是 $GL(n,R)$ 中单位元。若 $A\in GL(n,R)$，则逆矩阵 $A^{-1}\in GL(n,R)$是 A 的逆元，注意到 $|A^{-1}|=\frac{1}{|A|}\neq 0$。综上，$GL(n,R)$ 是群。同理可证，$SL(n,R)$ 是群。

第二章 代数基础

第一部分 群

2.1 群的定义与例子

2. 1. 1 群的定义

2. 1. 2 群的性质

2.2 子群、正规子群与商群

2.3 群的同态与同构

2.1.2 第三阶段学习目标

- 理解关于群中单位元和逆元性质
- 能描述半群，群幂次，交换群的含义

2.1.2 群的定义-单位元与逆元性质

➢ 以常见的群为例子，请思考

1) 群中的单位元唯一的吗？

2) 设a和b的逆元a^{-1},b^{-1}，则$a \cdot b$的逆元和a^{-1},b^{-1} 有什么样关系?

3) 已知群元素x, a满足$ax=e$,其中e为单位元，则x一定是a的逆元吗？

4) 群中哪些元素可能存在多个逆元？

2.1.2 群的定义-单位元与逆元性质

➢ 给定群G及运算·，则

1) 单位元e是唯一的

2) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

3) x是元素a的逆元充分必要条件是$ax=e$

4) 任何元素的逆元是唯一

2.1.2 群的定义-单位元与逆元性质

证1） 设 e, e' 是 G 中的单位元，

$$e = e \cdot e' = e'$$

证2） $(a \cdot b)^{-1} \cdot (a \cdot b) = e$，

$$(a \cdot b)^{-1} \cdot (a \cdot b) \cdot b^{-1} = e \cdot b^{-1} = b^{-1}$$

$$(a \cdot b)^{-1} \cdot a \cdot (b \cdot b^{-1}) \cdot a^{-1} = b^{-1} \cdot a^{-1}$$

$$(a \cdot b)^{-1} \cdot (a \cdot e \cdot a^{-1}) = b^{-1} \cdot a^{-1}$$

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$$

2.1.2 群的定义-单位元与逆元性质

证3） 设 x 是 a 的逆元，那么

$$a \cdot x = e$$

反之，若 $a \cdot x = e$，则

$$a^{-1} \cdot a \cdot x = a^{-1} \cdot e = a^{-1}$$

$$e \cdot x = a^{-1}$$

那么，$x = a^{-1}$。

2.1.2 群的定义-单位元与逆元性质

证4） 设 a 有两个逆元 b 和 c，那么

$$
\begin{aligned}
b = b * e = b * (a * c) \\
= (b * a) * c \\
= e * c \\
= c
\end{aligned}
$$

因此，a 的逆元是唯一的。

2.1.2 群的定义—群的定义补充

- 由于群里结合律是满足的，把元素g的m次运算记为g^m，称为g的m次幂。

$$g^m = \underbrace{g \cdot g \cdot \ldots \cdot g}_{m}$$

- 当群运算用加法+表示时，

$$mg = m \cdot g = \underbrace{g + g + \ldots + g}_{m}$$

2.1.2 群的定义—群的定义补充

- 若(*G*, .)只满足结合律，则称G为半群；
- 如果(*G*, .) 满足结合律且有单位元，则称G为有单位元的半群，也称含幺半群。
- 如果群$(G,\ \cdot)$ 还满足如下的交换律：

$$\forall a,b \in G,\ \ a \cdot b = b \cdot a$$

则称 $(G,\ \cdot)$ 为交换群。

2.1.2 第四阶段学习目标

- 能描述群阶概念、元素阶概念
- 能证明定理1.6
- 能利用定理1.6结果来求元素的阶

2.1.2 群的定义—群的阶

定义1.4 如果一个群*G*中元素的个数是无限多个，则称*G*是无限群；如果*G*中的元素个数是有限多个，则称*G*是有限群，*G*中元素的个数称为群的阶（**Order**），记为|*G*|。

- 群可分为：有限群与无限群
  - 模*n*的剩余类加法群、乘法群，*n*次对称群等为有限群；
  - 一般线性群，特殊线性群，整数加群等为无限群。

2.1.2 群的定义—群的阶

定义1.5 设 G为一个群，$a \in G$，如果存在正整数 n，使得 $a^n = e$，则称 a为有限阶元，否则称为无限阶元。当 a 为有限阶元时，称使得 $a^n = e$ 的最小正整数为元素 a 的阶（**Order**），记为$|a|$。

定理1.6 1）对于整数n，a 为群G的元素，则

$$a^n = e \Leftrightarrow |a| \mid n$$

2）$|a^i| = \dfrac{|a|}{(|a|, i)}$，$(*, *)$表示最大公约数。

2.1.2 群的定义—群的阶

例 模6的剩余类加法集合$(Z_6, +)$ 中

- 0是 1 阶元；
- 3是 2 阶元；
- 2和4是 3 阶元；
- 1和5是 6 阶元。

2.1.2 群的定义–群的阶

定理 1.6 证1） 如果 $|a|\mid n$，则

$$a^n=a^{|a|\cdot k}=\left(a^{|a|}\right)^k=e^k=e$$

反之，如果 $a^n=e$， 令 $n=l|a|+r$，$0\le r<|a|$,则 $e=a^n=a^{l|a|+r}=\left(a^{|a|}\right)^l\cdot a^r=a^r$，由 $|a|$ 的最小性知 $r=0$。

证 2） 令 a^i 的阶为 r，则 $\left(a^i\right)^{\frac{|a|}{(|a|,i)}}=\left(a^{|a|}\right)^{\frac{i}{(|a|,i)}}=e$。

故 $r\mid\frac{|a|}{(|a|,i)}$。又 $a^{ir=e}$ 知 $|a|\mid ir$，故$\frac{|a|}{(|a|,i)}\mid\frac{ir}{(|a|,i)}$，又知 $\left(\frac{|a|}{(|a|,i)},\frac{i}{(|a|,i)}\right)=1$，得$\frac{|a|}{(|a|,i)}\mid r$，即 $r=\frac{|a|}{(|a|,i)}$。

定义1.7 设 G 为一个群，如果 G 中每个元素都可以表示成某个确定元素 a 的方幂，则称 G 为**循环群**，a 为循环群 G 的一个**生成元**。通常用 $G=<a>$ 表示 G 是由 a 生成的循环群。

由循环群的定义知，循环群一定是交换群。循环群中的运算通常用乘法表示。如果循环群中的生成元 a 为无限阶元，则

$$G=\{\cdots,a^{-2},a^{-1},e,a,a^{2},\cdots\}$$

生成元 a 为 n 阶元，则

$$G=\{e,a,a^{2},\cdots,a^{n-1}\}$$

2.1.2 群的定义—群的阶

例 整数加法群为无限循环群，模 n 的剩余类加法群是 n 阶循环群。

证：对每个整数 $m \in Z$，均有 $m = m \cdot 1$，从而 $Z =< 1 >$，同理 $Z =< -1 >$。

对每个剩余类 $i \in Z_n$，均有 $i = 1 + \cdots + 1 = i \cdot 1$，从而 $Z_n =< 1 >$。

注意到，当 $(k, n) = 1$ 时，

$$Z_n = \langle k \rangle = \{0, k, 2k, \ldots, (n-1)k\}$$

如果对某个整数 i，有 $ik = 0 \bmod n$，由于 $(k, n) = 1$，则 $i = 0 \bmod n$，即 $n \mid i$，故 k 的阶为 n，Z_n 是 n 阶循环群。

第二章 代数基础

第一部分 群

- 2.1 群的定义与例子
- 2.2 子群、正规子群与商群
  - 2. 2. 1 子群
  - 2. 2. 2 正规子群与商群
- 2.3 群的同态与同构

2.2.1 学习目标

- 能描述子群概念
- 能利用已有定理能判断(证明)子集合是否为子群

2.2.1 子群—子群定义

定义1.7 设G是一个群，H是G的非空子集，如果H关于群G的运算也构成一个群，那么称H是G的子群（ subgroup ），记为$H \le G$。

例1 整数加群是有理数加群的子群；非零有理数乘法群是非零实数乘法群的子群.

例2 特殊线性群是一般线性群的子群，即

$$SL(n, R) \le GL(n, R)$$

2.2.1 子群—子群定义

定理1.8 群G至少有两个子群：G本身；只包含单位元的子集$\{e\}$，它们称为G的平凡子群，其他子群为真子群。

问题：

(1) e是否属于 H， 如何找出H的单位元？

(2) 如果$a \in H$，a^{-1}是a在G中的逆元， a在H中的逆元是什么？

2.2.1 子群—子群定义

解：

(1) e是否属于 H， 如何找出H的单位元？

若 e_h 和 e_g 分别是子群 H 和群 G 中的单位元，在 H 中任取一元素 h，得到

$$e_h h = h e_h = h, e_g h = h e_g = h$$

故 $e_h h = e_g h$，右乘 h^{-1}，得到 $e_h = e_g$。

解：

(2) 如果$a \in H$，a^{-1}是a在G中的逆元，a在H中的逆元是什么？

若 a_h^{-1} 和 a_g^{-1} 分别是 a 在子群 H 和群 G 中的逆元，得到

$$a \cdot a_h^{-1} = a_h^{-1} \cdot a = e, \qquad a \cdot a_g^{-1} = a_g^{-1} \cdot a = e$$

故 $a \cdot a_h^{-1} = a \cdot a_g^{-1}$，左乘 a_g^{-1}，得到

$$(a_g^{-1} \cdot a) \cdot a_h^{-1} = (a_g^{-1} \cdot a) \cdot a_g^{-1}$$

故 $e \cdot a_h^{-1} = e \cdot a_g^{-1}$，$a_h^{-1} = a_g^{-1}$。

2.2.1 群的性质—子群

定理1.9 一个群G和它的一个子群H有：

1）G的单位元和H的单位元是同一元素；

2）如果$a\in H$，b是a在H中的逆元，a^{-1}是a在G中的逆元，则$b=a^{-1}$.

2.2.1 群的性质—子群

定理1.10 设 G是一个群（不妨设其中的运算为乘法），H 为G 的非空子集，则

$$H \le G \Leftrightarrow \forall a,b \in H, ab^{-1} \in H$$

证：$\Rightarrow$ 显然。

$\Leftarrow$ 若 $a \in H \le G$，令 a^{-1} 为 a 在 G 中的逆元，由条件 $aa^{-1} \in H$，从而 $e \in H$。（幺元）

又 $e, a \in H$，故 $ea^{-1} \in H$，即 $a^{-1} \in H$。（逆元）

又 $a, b \in H$，则 $a, b^{-1} \in H$，于是$ab = a\left(b^{-1}\right)^{-1} \in H$。（封闭性）

结合律在 H 中显然成立。

2.2.1 群的性质—子群

例3 群G的任意多个子群的交集仍为G的子群。

证：设$\boldsymbol{H_1, H_2 \leq G}$，则对任意的$\boldsymbol{a, b \in H_1 \cap H_2}$，有$\boldsymbol{ab^{-1} \in H_1}$，且$\boldsymbol{ab^{-1} \in H_2}$（由定理1.10），故$\boldsymbol{ab^{-1} \in H_1 \cap H_2}$，再由定理1.10得

$$\boldsymbol{a, b \in H_1 \cap H_2 \leq G}。$$

例4 设 G 是一个群，$a \in G$，令

$$C_a(G) = \{x \mid x \in G, ax = xa\}$$

$$C(G) = \{x \mid x \in G, \forall y \in G, yx = xy\}$$

则 $C_a(G), C(G) \leq G$，分别称为 a 的中心化子和 G 的中心。

证：只需证明 $C(G) \leq G$，$C_a(G) \leq G$ 类似可证。

令 e 为 G 中单位元，则 $\forall y \in G$，$ey = ye = y$，故 $e \in C(G)$，$C(G) \neq \emptyset$。取 $x_1, x_2 \in C(G)$，则对任意 $y \in G$，$x_1 y = y x_1$，$x_2 y = y x_2$，有 $y x_2^{-1} = x_2^{-1} y$，代入后得

$$(x_1 x_2^{-1})y = x_1(x_2^{-1}y) = x_1(yx_2^{-1}) = (x_1 y)x_2^{-1} = y(x_1 x_2^{-1})$$

故 $x_1 x_2^{-1} \in C(G)$，由定理1.10知，$C(G) \leq G$。

第二章 代数基础

第一部分 群

2.1 群的定义与例子

2.2 子群、正规子群与商群

2.2.1 子群

2.2.2 正规子群与商群

2.3 群的同态与同构

2.2.2节第一阶段学习目标

- 能描述陪集概念
- 能解释陪集的性质
- 能利用陪集的Lagrange定理解释关于有限群的阶

2.2.2 正规子群与商群–陪集及其分解

定义 1.14 设 $\langle G,\cdot\rangle$ 是一个群，$H \le G$，$a \in G$，令

$$aH = \{a \cdot h \mid h \in H\}, \qquad Ha = \{h \cdot a \mid h \in H\}$$

称 aH 为 G 中 a 关于 H 的左陪集，Ha 为 G 中 a 关于 H 的右陪集。

例1：H={0, 2, 4, 6}为$(Z_8, \oplus)$的4阶子群，以3为代表元的右陪集为 $H3 = \{1, 3, 5, 7\}$

2.2.2 正规子群与商群–陪集及其分解

定理1.15 设 $H \le G$，$a \in G$，$h \in H$，则

1） $|Ha| = |H|$，$Hh = H$

2） $Ha = Hb \Leftrightarrow ab^{-1} \in H$

3） $b \in Ha \Rightarrow Ha = Hb$

4） $\forall Ha, Hb \Rightarrow Ha = Hb$ 或 $Ha \cap Hb = \varnothing$

注：类似于右陪集定义，可以定义左陪集，并且上述定理结论对左陪集也成立。

定理1.15

证1： $|Ha| = |H|$

因 $a \in G\backslash H$，故 $Ha \neq H$，令 $f: h \rightarrow h \cdot a$ 是 $|H|$ 到 $|Ha|$ 的映射，该映射为一一对应（双射），得证。

证1： $Hh = H$。

$\forall h_1 \in Hh$，有 $h_1 = h_0 \cdot h \in H$，$h_0 \in H$，故 $Hh \subseteq H$。

$\forall h_2 \in H$，令 $h_0 = h_2 h^{-1}$，显然 $h_0 \in H$，故 $h_2 = h_0 h \in Hh$，即 $H \subseteq Hh$。

定理1.15

证2： $Ha = Hb \Leftrightarrow ab^{-1} \in H$

$\Rightarrow$ 因 $Ha = Hb$，故 $\exists h_1, h_2 \in H$，使得 $h_1 a = h_2 b$，故 $ab^{-1} = h_1^{-1} h_2 \in H$。

$\Leftarrow$ 因 $ab^{-1} \in H$，故 $\exists h \in H$ 使得 $ab^{-1} = h$，因此

$$a = hb \in Hb$$

由（3）得，$Ha = Hb$。

定理1.15

证3： $Ha = Hb \Leftrightarrow b \in Ha$

$\Rightarrow$ 因 $Ha = Hb$，故 $\exists h_1, h_2 \in H$，使得 $h_1 a = h_2 b$，故 $b = h_2^{-1} h_1 a \in Ha$。

$\Leftarrow$ 因 $b \in Ha$，故 $\exists h \in H$ 使得 $b = ha$，因此

$\forall\, h_1 b \in Hb$， $h_1 b = h_1 ha \in Ha$，即 $Hb \subseteq Ha$。

$\forall\, h_2 a \in Ha$，令

$$h_0 = h_2 ab^{-1} = h_2 a(ha)^{-1} = h_2 aa^{-1}h^{-1} = h_2 h^{-1} \in H$$

即 $\exists h_0 \in H$，使得 $h_0 b = h_2 a$，即 $h_2 a \in Hb$， $Ha \subseteq Hb$。

2.2.2 正规子群与商群-陪集及其分解

定理1.15

证4： $\forall Ha, Hb \Rightarrow Ha = Hb$ 或 $Ha \cap Hb = \emptyset$。

1. 若 $ab^{-1} \in H$，由（2）知，$Ha = Hb$ 。
2. 若 $ab^{-1} \notin H$，假设 $c \in Ha \cap Hb$，则 $\exists h_1, h_2 \in H$ 使得 $c = h_1 a = h_2 b$，则 $ab^{-1} = h_1^{-1} h_2 \in H$ 与 $ab^{-1} \notin H$ 矛盾。故 $Ha \cap Hb = \emptyset$。

2.2.2 正规子群与商群–陪集及其分解

我们容易证得如下结论：

令 H 是群 G 的子群，定义如下二元关系：$\forall x, y \in G$，有

$$x \sim y \Leftrightarrow xy^{-1} \in H$$

则该二元关系为群 G 中的一个**等价关系**，即满足

1. **自反性：** 若 $x \in G$，则 $x \sim x$ 。
2. **对称性：** 若 $x, y \in G$，且 $x \sim y$ ，则 $y \sim x$。
3. **传递性：** 若 $x, y, z \in G$，且 $x \sim y, y \sim z$ ，则 $x \sim z$ 。

这表明：等价类 $\{Hy\}$ 组成群 G 的一个**划分**。

2.2.2 正规子群与商群-Lagrange定理

定理 1.16（**Lagrange定理**）设G为有限群，H为G的子群， 令$\{Ha_1, Ha_2, Ha_3, \cdots, Ha_t\}$ 为H关于G的全体右陪集的集合，则 $t = |G|/|H|$.

注1：记 $t = [G:H]$ 为 H 在 G 中的指数.

注2：有限群中子群的阶整除群的阶，即 $|H|\,\big|\,|G|$.

2.2.2 正规子群与商群-Lagrange定理

定理 1.17 关于有限群的阶有如下性质

(1) 有限群中每一个元素的阶均整除群的阶.

(2) 设群G的阶数是素数，则G是循环群，且G中任意非单位元为生成元。

2.2.2 正规子群与商群-Lagrange定理

定理1.17证（2）： 设 $|G| = p$，p 为素数。任取 $a \in G$，$a \neq e$，设 $|a| = t > 1$，容易证明

$$H = \{e, a, a^2, \dots, a^{t-1}\}$$

一定为 G 的子群。由Lagrange定理知，$|H| \mid p$，故 $t \mid p$。由 $t > 1$ 且 p 为素数知，$t = p$，即 $G = H = \langle a \rangle$。$G$ 为循环群。

2.2.2 小结

- 陪集概念
- 陪集的性质
- 能利用陪集的Lagrange定理解释关于有限群的阶

2.2.2第二阶段学习目标

- 能描述正规子群概念
- 能判断正规子群
- 能理解商群运算

2.2.2 正规子群与商群–正规子群

定义1.17 设$H \le G$，如果对$\forall a \in G$，均有

$$a^{-1}Ha = \{a^{-1}ha \mid h \in H\} \subseteq H$$

则称H为G的正规子群（不变子群），记为

$$H \lhd G.$$

注1：交换群的任意子群为正规子群。

注2：循环群的任意子群为正规子群。

注3：正规子群的条件也可写为$Ha = aH$。

2.2.2 正规子群与商群-正规子群

问题1：模9加群G={0,1,2,3,4,5,6,7,8}，子群H={0,3,6}是不是正规子群？写出所有右陪集？

问题2：模7乘群G={1,2,3,4,5,6}，子群H={1,6}是不是正规子群？写出所有右陪集？

2.2.2 正规子群与商群-正规子群

问题1：模9加群G={0,1,2,3,4,5,6,7,8}，子群H={0,3,6}是不是正规子群？写出所有右陪集？

答：是。G 是循环群，H 的所有右陪集为：

$H = \{0,3,6\}$

$H + 1 = \{1,4,7\}$

$H + 2 = \{2,5,8\}$

注，　$H + i = i + H, i = 0,1,2$。

2.2.2 正规子群与商群-正规子群

问题2：模7乘群G={1,2,3,4,5,6}，子群H={1,6}是不是正规子群？写出所有右陪集？

答：是。 G 是循环群，H 的所有右陪集为：

$H = \{1,6\}$

$H2 = \{2,5\}$

$H3 = \{3,4\}$

注， $Hi = iH, i = 1,2,3$。

2.2.2 正规子群与商群–正规子群

定理 1.19 设 $H \le G$，则 H 为 G 的正规子群

$$\Leftrightarrow \forall a \in G, a^{-1}Ha \subseteq H$$

$$\Leftrightarrow \forall a \in G, a^{-1}Ha = H$$

$$\Leftrightarrow \forall a \in G, aH = Ha$$

注3：指数为2的子群一定为正规子群。

证：设$H \le G$，指数$[G:H] = 2$，$\forall a \in G$，

1. 若 $a \notin H$，则$aH \ne H$， $Ha \ne H$，故陪集分解
   $G = H \cup aH = H \cup Ha$，所以$aH = Ha$。
2. 若 $a \in H$，则显然 $H = aH = Ha$

因此， $H \lhd G$。

2.2.2 正规子群与商群–正规子群

➢如果 H为$(G,\cdot)$ 的子群，令

$$W=\{H, Ha_1,\ Ha_2,\ \cdots\}$$

则集合W关于如下运算是否是代数运算？是否构成群？为什么？

$$Ha\circ Hb=H(a\cdot b)$$

2.2.2 正规子群与商群-商群

➢如果 H为$(G,\cdot)$ 的正规子群，令

$$G/H=\{H, Ha_1,\ Ha_2,\ \cdots\}$$

则集合***G/H***关于如下运算也构成群，称之为商群.

$$Ha\circ Hb=H(a\cdot b)$$

注：如何求商群的单位元和逆元?

2.2.2 正规子群与商群-商群

说明1： 商群中定义的陪集运算与陪集代表元选取无关。

令 $Ha_1 = Ha, Hb_1 = Hb$，则

$$h_1 = aa_1^{-1} \in H, \qquad h_2 = bb_1^{-1} \in H$$

并且由正规子群定义知 $H = a_1 H a_1^{-1}$，即$a_1 h_2 a_1^{-1} \in H$，于是有

$$\begin{aligned}(ab)(a_1 b_1)^{-1} &= (ab)(b_1^{-1} a_1^{-1}) \\ &= a(bb_1^{-1})a_1^{-1} = ah_2 a_1^{-1} \\ &= a(a_1^{-1} a_1)h_2 a_1^{-1} = (aa_1^{-1})(a_1 h_2 a_1^{-1}) \\ &= h_1(a_1 h_2 a_1^{-1}) \in H\end{aligned}$$

故 $H(ab) = H(a_1 b_1)$。

2.2.2 正规子群与商群−商群

说明2： 商群中定义的乘积运算·使 $\langle \boldsymbol{G/H}, \circ \rangle$ 构成群。

封闭性： 对任意 $Ha, Hb \in G/H$，有

$$(Ha) \circ (Hb) = H(ab) \in G/H$$

结合律： $\big((Ha) \circ (Hb)\big) \circ (Hc) = H(ab) \circ Hc = H(abc)$

$$(Ha) \circ \big((Hb) \circ (Hc)\big) = H(a) \circ H(bc) = H(abc)$$

单位元： H 为 G/H 中单位元。对任意 $Ha \in G/H$，有

$$(Ha) \circ H = H \circ (Ha) = Ha$$

逆元： 对任意 $Ha \in G/H$，均有 $Ha^{-1} \in G/H$，

$$(Ha) \circ (Ha^{-1}) = (Ha^{-1}) \circ (Ha) = H$$

称 G/H 为 **G 关于 H 的商群**。

2.2.2 正规子群与商群–商群

例 设 Z 为整数加法群，$m \in Z$，令

$$H = \{mn \mid n \in Z\} = \{0, \pm m, \pm 2m, \ldots\}$$

则 $H \leq Z$。又由于 Z 为交换群，故 $H \lhd Z$。

对任意的 $a, b \in Z$，

$$H + a = H + b \Leftrightarrow a - b \in H \Leftrightarrow a \equiv b \pmod m$$

故商群

$$Z/H = Z_m = \{0,1,2, \ldots, m-1\}$$

为模 m 的剩余类加法群。

注：因 Z 中代数运算为 $+$，故右陪集 Ha 用 $H + a$ 表示。

第二章 代数基础

第一部分 群

2.1 群的定义与例子

2.2 子群、正规子群与商群

2.3 群的同态与同构

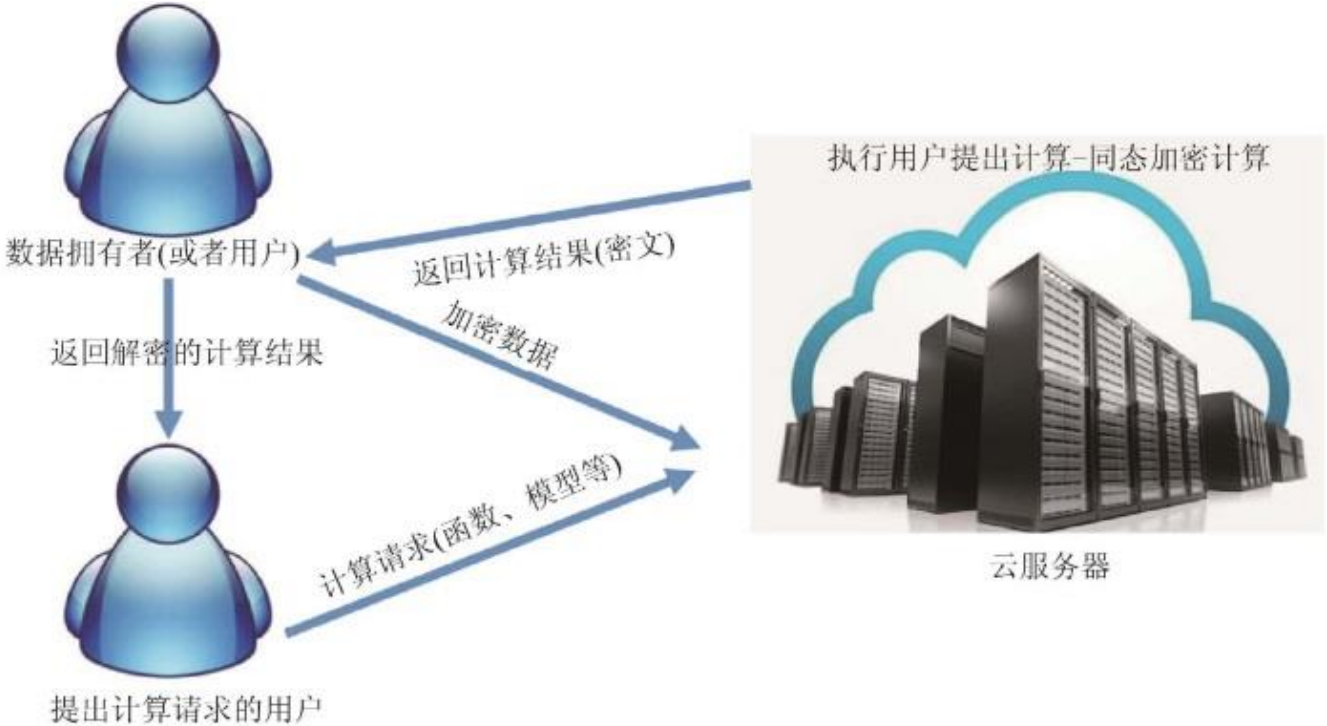
2. 3. 1 同态与同构基本概念

2. 3. 2 同态核与同构基本定理

小节引入

- 同态加密技术： 对经过同态加密的密文进行处理得到一个输出进行解密，其结果与用同一方法处理未加密的原始数据得到的输出结果是一样的

同态计算模型：



小节学习目标

- 能描述同态概念和列举同态映射例子
- 能解释同态性质、同构概念

2.3.1 群的同态与同构-基本概念

定义1.19 设$(G_1,\cdot)$和$(G_2,*)$为两个群，f 为G_1 到G_2 的映射，如果 f 满足：对 $\forall a, b\in G$，

$$f(a\cdot b)=f(a)*f(b)$$

则称 f 为从群 G_1 到 G_2 的**同态映射**.

问: F(x)=x mod n是不是(Z,+)到(Z_n ,⊕)的同态映射?

答： 是。由

$$(x+y)\bmod n=\big((x \bmod n)+(y \bmod n)\big)\bmod n$$

知 $F(x+y)=F(x)\oplus F(y)$。

2.3.1 群的同态与同构-基本概念

例 1　 F(x)=x mod n 是(Z,+)到(Z_n ,⊕)的同态映射

例 2　F(x)=2x是(Z,+)到偶数加法群*E*的同态映射

例 3　把群G所有元素映射成为群H单位元的映射也为同态映射

你发现关于原群和像群中单位元和逆元的什么规律?

2.3.1 群的同态与同构-基本概念

定理1.20 同态映射具有如下性质：

1) $f(e_{G_1})=e_{G_2}$ $\quad f(a^{-1})=f(a)^{-1}$

证：令 $f(G_1)=\{f(g)\mid g\in G_1\}$，称为 G_1 的同态像。

我们证 $f(G_1)\le G_2$。

- 封闭性：由 $f(e_{G_1})\in f(G_1)$ 知 $f(G_1)\neq\emptyset$。故 $\forall f(g_1),f(g_2)\in f(G_1)$，$f(g_1)*f(g_2)=f(g_1\cdot g_2)\in f(G_1)$
- 结合律：显然。
- 单位元：对任意 $f(g)\in f(G_1)$，有

$$f(e_{G_1})*f(g)=f(e_{G_1}\cdot g)=f(g)=f(g\cdot e_{G_1})=f(g)*f(e_{G_1})$$

- 逆元：$f(g)*f(g^{-1})=f(g^{-1})*f(g)=f(e_{G_1})$。故 $f(g)$ 在 $f(G_1)$ 中的逆元是$f(g^{-1})$。

定理1.20 同态映射具有如下性质：

1） $f(e_{G_1}) = e_{G_2}$ $\qquad f(a^{-1}) = f(a)^{-1}$

证：已证 $f(G_1) \le G_2$。注意到，

- 子群的单位元就是群的单位元；
- 子群的元素的逆元就是这个元素在群的逆元。

因此，

- $f(G_1)$ 的单位元 $f\left(e_{G_1}\right)$ 就是 G_2 的单位元。
- $f(g^{-1})$是 $f(g)$ 在 G_2 中的逆元。

2.3.1 群的同态与同构-基本概念

- 如果 f 为满射，则称 f 为**满同态**，记为 $G_1 \sim G_2$.
- 如果 f 既为单射又是满射，则称 G_1 与 G_2 **同构**，记为 $G_1 \cong G_2$.

例 4 整数加法群Z和偶数加法群E同构.

构造映射 $f: x \to 2x$，f 是 Z 到 E 的同态，

$$f(x+y)=2(x+y)=2x+2y=f(x)+f(y)$$

单射：$f(x_1)=2x_1 \neq 2x_2=f(x_2), x_1 \neq x_2$。

满射：$\forall\, 2k \in E, \exists k \in Z, s.t., f(k)=2k$。

例 5 任意一个二阶群都与乘法群{1，–1}同构.

设二阶群 $A=\{a,e\}$（注：$a*a=e$），构造映射

$$f(x)=\begin{cases}-1, & x=a\\ 1, & x=e\end{cases}$$

同态：$f(xy)=\begin{cases}1, & x=a,y=a\\ -1, & x=a,y=e\\ -1, & x=e,y=a\\ 1, & x=e,y=e\end{cases}$，

$f(x)f(y)=\begin{cases}1, & x=a,y=a\\ -1, & x=a,y=e\\ -1, & x=e,y=a\\ 1, & x=e,y=e\end{cases}$，故 $f(xy)=f(x)f(y)$。

例 5（续）任意一个二阶群都与乘法群{1，−1}同构.

设二阶群 $A=\{a,e\}$（注：$a*a=e$），构造映射

$$f(x)=\begin{cases}-1, & x=a\\ 1, & x=e\end{cases}$$

单射：$f(a)\neq f(e)$

满射：显然。

本小节的总结

- 同态概念、例子
- 同态性质、同构概念

第二章 代数基础

第一部分 群

2.1 群的定义与例子

2.2 子群、正规子群与商群

2.3 群的同态与同构

2. 3. 1 同态与同构基本概念

2. 3. 2 同态核与同构基本定理

小节学习目标

- 能描述同态核概念
- 能理解同态基本定理

2.3.2 群的同态与同构-同态核和同构基本定理

定义 1.21 设 f 是从群 G 到群 H 的同态，定义

$\mathrm{Ker}(f)=\{a\mid a\in G, f(a)=e\}$，$e$ 是 G 的单位元，

则称 $\mathrm{Ker}(f)$ 为 f 的同态核。

例 1 $F(x)=x \bmod n$ 是 $(Z,+)$ 到 $(Z_n,\oplus)$ 的同态映射。

同态核

$$\mathrm{Ker}(F)=\{a\mid a\in Z, F(a)=0\}$$
$$=\{n\cdot k\mid k=0,1,2,\ldots\}$$

定理 1.22 设 $\boldsymbol{f}$ 是从群 $\boldsymbol{G}$ 到群 $\boldsymbol{H}$ 的同态，则

1. 同态核是 $\boldsymbol{G}$ 的正规子群， $\mathbf{Ker}(\boldsymbol{f}) \lhd \boldsymbol{G}$;
2. 同态像是 $\boldsymbol{H}$ 的子群， $\boldsymbol{f}(\boldsymbol{G}) \leq \boldsymbol{H}$。

证1： 设 e, e' 分别是 G 和 H 的单位元，有 $f(e) = e'$，从而 $e' \in \mathrm{Ker}(f)$，$\mathrm{Ker}(f) \neq \emptyset$。$\forall\, a, b \in \mathrm{Ker}(f)$，则 $f(a) = f(b) = e'$，从而

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

故 $ab^{-1} \in \mathrm{Ker}(f)$，$\mathbf{Ker}(\boldsymbol{f}) \leq \boldsymbol{G}$。

又 $\forall g \in G$，$\forall a \in \mathrm{Ker}(f)$，有

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

故 $g^{-1}ag \in \mathrm{Ker}(f)$， $\mathbf{Ker}(\boldsymbol{f}) \lhd \boldsymbol{G}$。

定理 1.22 设 $\boldsymbol{f}$ 是从群 $\boldsymbol{G}$ 到群 $\boldsymbol{H}$ 的同态，则

1. 同态核是 $\boldsymbol{G}$ 的正规子群， $\mathbf{Ker}(\boldsymbol{f}) \lhd \boldsymbol{G}$;
2. 同态像是 $\boldsymbol{H}$ 的子群， $\boldsymbol{f}(\boldsymbol{G}) \leq \boldsymbol{H}$。

证2： $\forall a, b \in f(G)$, $\exists\, x_1, x_2 \in G$ 使得 $f(x_1) = a, f(x_2) = b$,

则 $ab^{-1} = f(x_1)f(x_2)^{-1} = f(x_1)f(x_2^{-1}) = f(x_1x_2^{-1})$，故

$$ab^{-1} \in f(G)$$

因此， $f(G) \leq H$。

2.3.2 群的同态与同构-同态核和同构基本定理

定理 1.23 设 f 是从群 G_1 到群 G_2 的满同态，则

$$G_1/\mathrm{Ker}(f) \cong G_2$$

证： 对每个右陪集 $\mathrm{Ker}(f)g \in G_1/\mathrm{Ker}(f)$，令 $\phi(g) = f(g)$，则可证 ϕ 是 $G_1/\mathrm{Ker}(f)$ 到 G_2 的同构映射。

1. 如果 $g_1 \in \mathrm{Ker}(f)g$，则存在 $k \in \mathrm{Ker}(f)$ 使得 $g_1 = kg$，则 $\phi(g_1) = \phi(kg) = f(kg) = f(k)f(g) = f(g) = \phi(g)$。故 ϕ 的取值与代表元选取无关。
2. $\phi(g_1g_2) = f(g_1g_2) = f(g_1)f(g_2) = \phi(g_1)\phi(g_2)$，$\phi$ 为同态。

2.3.2 群的同态与同构–同态核和同构基本定理

定理 1.23 设 f 是从群 G_1 到群 G_2 的满同态，则

$$G_1/\mathrm{Ker}(f) \cong G_2$$

证（续）： 对每个右陪集 $\mathrm{Ker}(f)g \in G_1/\mathrm{Ker}(f)$，令 $\phi(g) = f(g)$，则可证 ϕ 是 $G_1/\mathrm{Ker}(f)$ 到 G_2 的同构映射。

3. 若$\phi(g_1) = \phi(g_2)$，则 $f(g_1) = f(g_2)$，故

$$f(g_1 g_2^{-1}) = f(g_1)f(g_2^{-1}) = f(g_1)f(g_2)^{-1} = e'$$

$g_1 g_2^{-1} \in \mathrm{Ker}(f)$，$g_1 \in \mathrm{Ker}(f)g_2$，故 ϕ 是单射。

4. 对任意 $g' \in G_2$，由于 f 为满射，故存在 $g \in G_1$使得 $f(g) = g'$，于是 $\phi(g) = f(g) = g'$，ϕ 为满射。
5. 综上，ϕ 是 $G_1/\mathrm{Ker}(f)$ 到 G_2 的同构映射。

推论 1.24 设 $\boldsymbol{G_1}$ 和 $\boldsymbol{G_2}$ 分别为 $\boldsymbol{m}$ 和 $\boldsymbol{n}$ 阶循环群，则存在 $\boldsymbol{G_1}$到 $\boldsymbol{G_2}$ 的满同态 $\Leftrightarrow \boldsymbol{n \mid m}$

证：

$\Rightarrow$ 设 f 是 G_1到 G_2 的满同态，由同态基本定理知，

$G_1/\mathrm{Ker}(f) \cong G_2$，于是有

$$n = |G_2| = |G_1/\mathrm{Ker}(f)| = \frac{|G_1|}{|\mathrm{Ker}(f)|} = \frac{m}{|\mathrm{Ker}(f)|},$$

故 $n \mid m$。

2.3.2 群的同态与同构-同态核和同构基本定理

推论 1.24 设 $\boldsymbol{G_1}$ 和 $\boldsymbol{G_2}$ 分别为 $\boldsymbol{m}$ 和 $\boldsymbol{n}$ 阶循环群，则

存在 $\boldsymbol{G_1}$ 到 $\boldsymbol{G_2}$ 的满同态 $\Leftrightarrow \boldsymbol{n \mid m}$

证（续）：$\Leftarrow$ 设 $G_1 = \langle a \rangle, G_2 = \langle b \rangle$，令 $f: a^k \to b^k$，可证 f 是 G_1 到 G_2 的满同态。

事实上，若 $a^k = a^l$，则 $a^{k-l} = e$，从而 $m \mid (k-l)$，又 $n \mid m$，则 $n \mid (k-l)$，有 $b^{k-l} = e'$。说明 f 映射下的像唯一，即 $\boldsymbol{f}$ **是映射**。又 $\forall x \in G_2, \exists l \leq n, s.t., x = b^l$，注意到 $f(a^l) = b^l = x$，故 $\boldsymbol{f}$ **是满射**。最后，我们有

$$f(a^{l_1}a^{l_2}) = f(a^{l_1+l_2}) = b^{l_1+l_2} = b^{l_1}b^{l_2} = f(a^{l_1})f(a^{l_2})$$

故 $\boldsymbol{f}$ **是同态映射**。