第5篇 代数系统

第9章 代数系统

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

本章节目录

- 9.1代数系统的概念及运算性质
  - 9.1.1代数系统的概念
  - 9.1.2二元运算的性质
- 9.2代数系统的同态与同构
  - 9.2.1同态与同构
  - 9.2.2同态的性质
- 9.3群
  - 9.3.1半群与独异点
  - 9.3.2群及其基本性质
  - 9.3.3子群与陪集
  - 9.3.4循环群与置换群
- 9.4环与域
  - 9.4.1环与域的概念
  - 9.4.2环与域的性质*
- 9.5格与布尔代数
  - 9.5.1格的概念与性质
  - 9.5.2分配格、有补格
  - 9.5.3布尔代数

9.1 代数系统的概念及运算性质

9.1.1代数系统的概念

- 定义9.1 设A是一个非空集合，若有n元函数f：$A^n \to A$，则称f为A上的一个n元运算。

当n = 2时，称f为A上的一个二元运算；当n = 1时，称f为A上的一个一元运算。

- 要验证一个运算是否为集合A上的二元运算，应考虑以下两点：

（1）A中任何两个元素都可以进行这种运算，且运算的结果是唯一的。

（2）A中任何两个元素的运算的结果都属于A，即A对该运算是封闭的。

9.1 代数系统的概念及运算性质

- 整数集Z上的加法、减法、乘法是Z上的二元运算，但除法不是。
- 非零实数集R – {0}上乘法、除法都是该集合上的二元运算，而加法、减法不是，因为3 +（–3）= 3 – 3 = 0$\notin$R – {0}。
- 对任意集合A，其任意子集的交、并运算仍是A的子集，因此，交、并是A的幂集ρ（A）上的二元运算，A的任意子集相对于A的补集也是A的子集，因此相对于A的补运算是ρ（A）上的一元运算。
- 合取和析取联结词是集合{T，F}上的二元运算，否定联结词是该集合上的一元运算。
- 集合A = {x | x=2^n，n∈N}，普通的加法运算在集合A上不封闭，例如，$2^2 + 2^3 = 12$；而对于普通的乘法运算，由于对任意m，n∈N，$2^m \times 2^n = 2^{m+n} \in A$，因此，乘法是集合A上的二元运算。

9.1 代数系统的概念及运算性质

- 定义9.2 非空集合A和A上k个运算，$\circ_1$，$\circ_2$，$\circ_3$，…，$\circ_k$组成的系统称为一个代数系统（或代数结构），记作（A，$\circ_1$，$\circ_2$，$\circ_3$，…，$\circ_k$）。

- 一个代数系统要满足以下三个条件：

（1）有一个非空集合A;

（2）若干个建立在集合A上的运算;

（3）这些运算在集合A上是封闭的。

9.1 代数系统的概念及运算性质

- 整数集Z上带有加法运算的系统构成了一个代数系统，因为它有一个非空集合Z，有Z上的加法运算，并且这个加法运算在Z上是封闭的。因此，它构成了一个代数系统（Z，+）。

- 有理数集Q上带有加法和乘法运算的系统构成了一个代数系统，因为它有一个非空集合Q，有Q上的加法和乘法运算，并且这两个运算在Q上是封闭的。因此，它构成了一个代数系统（Q，+，×）。

- 集合A的幂集ρ（A）上带有交、并、补运算的系统构成了一个代数系统，因为它有一个非空集合ρ（A），有ρ（A）上的交、并、补运算，并且这三个运算在ρ（A）上是封闭的。因此，它构成了一个代数系统（ρ（A），∩，∪，⁻）。

9.1 代数系统的概念及运算性质

- 定义9.3 设（A，$\circ_1$，$\circ_2$，$\circ_3$，…，$\circ_k$）是一个代数系统，如果有A的非空子集B对A的每个运算$\circ_i$（$1\le i\le k$）都封闭，则代数系统（B，$\circ_1$，$\circ_2$，$\circ_3$，…，$\circ_k$）称为（A，$\circ_1$，$\circ_2$，$\circ_3$，…，$\circ_k$）的子系统或子代数。

  - 设E表示偶数集，O表示奇数集，则代数系统（E，+，×）是（Z，+，×）的子代数，（O，×）是（Z，×）的子代数。

9.1 代数系统的概念及运算性质

9.1.2二元运算的性质

1.交换律

- 设是集合A上的二元运算，如果对于任意a，b∈A，均有a∘b = b∘a，则称运算满足交换律。
  - 自然数集N、整数集Z、有理数集Q和实数集R上的加法运算和乘法运算都满足交换律。
  - 集合$Z_n = \{0, 1, 2, \ldots, n-1\}$上的$+_n$运算和$\times_n$满足交换律。

9.1 代数系统的概念及运算性质

2.结合律

- 设是集合A上的二元运算，如果对于任意a，b，c∈A，均有a ◦ （ b ◦ c）=（a ◦ b） ◦ c，则称运算满足结合律。
  - 自然数集N、整数集Z、有理数集Q和实数集R上的加法运算和乘法运算都满足结合律。
  - 集合Z_n = {0，1，2，…，n – 1}上的$+_n$运算和$\times_n$运算满足结合律。

9.1 代数系统的概念及运算性质

3.分配律

- 设∘，*是集合A上的两个二元运算，如果对于任意a，b，c∈A均有a∘（b*c）=（a∘b）*（a∘c），则称运算∘对运算*满足左分配律。同理，如果均有（b*c）∘a =（b∘a）*（c∘a），则称运算∘对运算*满足右分配律。如果运算∘对运算*既满足左分配律，又满足右分配律，则称运算对运算*满足分配律。
  - 自然数集N、整数集Z、有理数集Q和实数集R上的乘法运算对加法运算都满足分配律。
  - 集合A的幂集ρ（A）上的交运算对并运算、并运算对交运算都满足分配律。

9.1 代数系统的概念及运算性质

4.吸收律

❖ 设◦，*是集合A上的两个二元运算，如果对于任意a，b∈A均有a◦（a*b）= a，则称运算◦对运算*满足左吸收律；同理，如果均有（a*b）◦a = a，则称运算◦对运算*满足右吸收律。如果运算◦对运算*既满足左吸收律，又满足右吸收律，则称运算◦对运算*满足吸收律。

- 集合A的幂集ρ（A）上的交运算对并运算、并运算对交运算都满足吸收律。
- 集合{T，F}上的合取运算对析取运算、析取运算对合取运算都满足吸收律。

9.1 代数系统的概念及运算性质

5.幂等元和幂等律

- 设◦设是集合A上的二元运算，如果存在a∈A，满足a ◦ a = a，则称a为A中关于运算的幂等元。如果对于任意的a∈A都是幂等元，则称运算◦满足幂等律。
  - 0是自然数集N、整数集Z、有理数集Q和实数集R上的加法运算的幂等元，1是乘法运算的幂等元。
  - 集合A的幂集ρ（A）上的交运算和并运算都满足幂等律。

9.1 代数系统的概念及运算性质

6.单位元

❖ 设∘是集合A上的二元运算，如果存在e_l∈A，对于任意x∈A均有$e_l \circ x = x$，则e_l称为A中关于运算∘的左单位元（或左幺元）；如果存在e_r∈A，对于任意x∈A均有$x \circ e_r = x$，则e_r称为A中关于运算∘的右单位元（或右幺元）。如果存在e∈A既是运算∘的左单位元，又是运算∘的右单位元，则称e为A中关于运算∘的单位元（或幺元）。

- 0是自然数集N、整数集Z、有理数集Q和实数集R上加法运算的单位元，这几个集合上的乘法运算没有单位元，因为$1 \times 0 = 0 \times 1 = 0$，但是1是N – {0}、Z – {0}、Q – {0}和R – {0}上的乘法运算的单位元。
- 集合A的幂集ρ（A）中，集合A是交运算的单位元，空集Ø是并运算的单位元。

❖ 定理9.1 设是集合A上的二元运算，如果e_l、e_r分别是A中关于运算的左单位元和右单位元， 则$e_l = e_r$且A中的单位元是唯一的。

9.1 代数系统的概念及运算性质

7.零元

- 设∘设是集合A上的二元运算，如果存在$\theta_l \in A$，对于任意$x \in A$均有$e_l \circ x = e_l$，则称是A中关于运算的左零元；如果存在$\theta_r \in A$，对于任意$x \in A$均有$x \circ e_r = e_r$，则称是A中关于运算的右零元。如果存在$\theta \in A$既是运算∘的左零元，又是运算∘的右零元，则称θ是A中关于运算∘的零元。
  - 自然数集N、整数集Z、有理数集Q和实数集R上的加法运算没有零元，0是这几个集合上乘法运算的零元。
  - 集合A的幂集ρ（A）中，空集Ø是交运算的零元，集合A是并运算的零元。
- 若左、右零元都存在，则左零元和右零元是相等的，且零元若存在也是唯一的。

9.1 代数系统的概念及运算性质

8.逆元

- 设∘是集合A上的二元运算，e是A中关于运算∘的单位元，如果对于A中的元素a， 存在$a_l \in A$，使得$a_l \circ a = e$，则称a_l为A中a关于运算∘的左逆元。如果存在$a_r \in A$， 使得$a \circ a_r = e$，则称a_r为A中a关于运算∘的右逆元。如果A中存在a关于运算∘既是左逆元又是右逆元的元素，称该元素为A中a关于运算∘的逆元，并称a关于运算∘可逆。
  - 整数集Z、有理数集Q和实数集R上的加法运算，任何元素x的逆元是–x；但是自然数集N上的加法运算，除了单位元0外，其它元素都没有逆元。N – {0}、Z – {0}上的乘法运算，除了单位元1外，其它元素都没有逆元；但是Q – {0}和R – {0}上的乘法运算，任意元素x的逆元是1/x。
  - 集合A的幂集ρ（A）上的交运算，除了单位元A外，其它元素都没有逆元；ρ（A）上的并运算，除了单位元Ø外，其它元素都没有逆元。
- 定理9.2 设∘是集合A上满足结合律的二元运算，如果对于A中元素a，A中存在a关于运算∘的左逆元a_l和右逆元a_r，则有$a_l = a_r$，并且逆元唯一。

9.2 代数系统的同态与同构

9.2.1同态与同构

- 定义9.4 设有两个代数系统（A，$\circ_1$，$\circ_2$，$\circ_3$，…，$\circ_k$）和（B，$*_1$，$*_2$，$*_3$，…，$*_k$），如果$\circ_i$和$*_i$具有相同的元数，称这两个代数系统具有相同的类型。
  - 代数系统（N，+）与代数系统（Z，×）具有相同的类型，因为它们都有一个二元运算。
  - 设A是一个非空集合，代数系统（{T，F}，∧，∨，Ø）与代数系统（ρ（A），∩，∪，⁻）具有相同的类型，因为它们都有三个运算，并且，∧和∩都是二元运算，∨和∪都是二元运算，Ø和⁻都是一元运算。

9.2 代数系统的同态与同构

- 定义9.5 设（A，◦）和（B，*）是两个同类型的代数系统，如果存在映射f：$A \to B$，对任意的x，$y \in A$都有 f（x◦y）= f（x）* f（y），则称f：$A \to B$为从（A，◦）到（B，*）的同态映射，简称同态，也称这两个代数系统同态。
  - 代数系统（R，+）与（R，×）同态。因为存在映射f：$R \to R$，f（x）= e^x使得对任意的x，$y \in R$都有

$$f(x+y) = f(x)f(y)。$$

  - 代数系统（Z，+，×）与（Z_n，$+_n$，$\times_n$）同态。其中，$Z_n = \{0，1，2，…，n–1\}$，$x + y = x +_n y \bmod n$，$x \times y = x \times_n y \bmod n$。因为存在映射f：$Z \to Z_n$，f（x）= x mod n，使得对任意的x，$y \in Z$都有

$$f(x+y) = f(x) +_n f(y)，f(xy) = f(x) \times_n f(y)$$

9.2 代数系统的同态与同构

- 定义9.6 设f是从（A，◦）到（B，*）的同态映射。

（1）如果f是满射，则称f是从（A，◦）到（B，*）的满同态；

（2）如果f是单射，则称f是从（A，◦）到（B，*）的单同态；

（3）如果f是双射，则称f是从（A，◦）到（B，*）的同构映射，并称（A，◦）和（B，*）是同构的。

- 代数系统（Z，+，×）与（Z_n，$+_n$，$\times_n$）是满同态；代数系统（R，+）与（R，×）单同态。
- 代数系统（R，+）与（R^+，×）同构。

9.2 代数系统的同态与同构

9.2.2同态的性质

- 定理9.3 设f是从（A，◦）到（B，*）的满同态，则有

（1）如果运算◦满足交换律， 则运算*也满足交换律。

（2）如果运算◦满足结合律， 则运算*也满足结合律。

（3）如果a是A中关于运算◦的幂等元，则f（a）是B中关于运算*的幂等元。

（4）如果e是A中关于运算◦的单位元，则f（e）是B中关于运算*的单位元。

（5）如果θ是A中关于运算◦的零元，则f（θ）是B中关于运算*的零元。

（6）如果a^{-1}是A中a关于运算◦的逆元，则f（ a^{-1} ）是B中f（a）关于运算*中的逆元。

9.2 代数系统的同态与同构

- 定理9.4 设f是从（A，◦，△）到（B，*，☆）的满同态，如果运算△对运算◦满足分配律，则运算☆对运算*也满足分配律。

- 对于代数系统A和B的满同态，它能够保持运算的性质具有单向性，即，如果A具有某性质，则B也具有，但反之不一定成立。只有A与B是同构的，保持运算的性质才是双向的。

9.3 群

9.3.1半群与独异点

- 定义9.7 设（A，◦）是一个代数系统，其中◦是二元运算且满足结合律，则称此代数系统为半群。如果◦还满足交换律，则称为可交换半群。
  - 代数系统（N，+），（Z，+），（Q，+），（R，+）是半群，而且是可交换半群
  - （N，×），（Z，×），（Q，×），（R，×）也是可交换半群
  - （N，–），（Z，–），（Q，–），（R，–）不是半群
  - （N，/），（Z，/），（Q，/），（R，/）不是半群

9.3 群

- 半群的重要性质：

（1）半群的子代数仍是半群。

（2）半群（A，◦）如果A为有限集，则必有幂等元。

（3）如果f是从半群（A，◦）到（B，*）的满同态，则（B，*）也是半群。

9.3 群

- 定义9.8 设（A，∘）是一个代数系统，其中∘是二元运算且满足结合律，并且，A中存在关于运算∘的单位元，则称此代数系统为独异点（或含幺半群）。如果∘还满足交换律，则称为可交换独异点（或可交换含幺半群）。
  - 代数系统（N，+），（Z，+），（Q，+），（R，+）的各集合含有关于加法的单位元0，因此它们都是独异点，而且是可交换独异点
  - （N，×），（Z，×），（Q，×），（R，×）的各集合含有关于乘法的单位元1，因此，它们都是可交换独异点

9.3 群

- 独异点的重要性质：

（1）独异点的子代数如果包含单位元仍是独异点。

（2）独异点（ A，◦）关于的运算表中不会有任何两行或两列是相同的。

（3）如果f是从独异点（ A，◦）到（B，*）的满同态，则（B，*）也是独异点。

9.3 群

9.3.2群及其基本性质

- 定义9.9 设（ G，◦ ）是一个半群，如果G中存在关于运算◦的单位元，并且，对任意元素$a \in G$都有$a^{-1} \in G$，则称此代数系统为群。

- 定义9.10 设（ G，◦ ）是一个群，如果满足交换律，则称（ G，◦ ）为可交换群（或阿贝尔群）。

- 定义9.11 设（ G，◦ ）是一个群，如果G为有限集，则称（ G，◦ ）为有限群，并称G的基数|G|（即G的元素个数）为群的阶；如果G为无限集，则称（ G，◦ ）为无限群。

9.3 群

设e是群（G，◦）的单位元，我们可以定义任意元素a的任意整数次幂为：

$$a^n=\begin{cases} e & n=0 \\ a^{n-1}\circ a & n>1, n\in Z \\ (a^{-n})^{-1} & n<0, n\in Z \end{cases}$$

- 定义9.12　　设e是群（G，◦）的单位元，对任意元素a∈G，使得$a^k = e$的最小正整数k称为a的阶（或周期）。如果不存在这样的正整数k，称a的阶是无限的。

9.3 群

- 代数系统（Z，+），（Q，+），（R，+）的各集合中元素x的逆元是–x，因此它们都是群，而且是无限可交换群，除了单位元0的阶为1外，其余元素的阶都是无限的，但是（N，+）不是群；（N，×），（Z，×），（Q，×），（R，×）都不是群，因为0不可逆，但是（Q – {0}，×）和（R – {0}，×）是无限可交换群，任意元素x的逆元是1/x，除了单位元1的阶为1，–1的阶为2外，其他元素的阶都是无限的。

- 代数系统（Z_6，$+_6$）是有限可交换群，其阶为6，单位元为0，元素x的逆元是（6 – x） mod 6，其元素0，1，2，3，4，5的阶分别为1，6，3，2，3，6；代数系统（ Z_6，$\times_6$）不是群，因为0不可逆。

9.3 群

- 群具有下面的重要性质：

（1）阶大于1的群没有零元。

（2）群中唯一的幂等元是单位元。

（3）群（G，∘）关于的运算表中不会有任何两行或两列是相同的。

（4）对于群（G，∘）的任意元素a，b，存在唯一的元素x使得a ∘ x = b，存在唯一的元素y使得y ∘ a = b。

（5）对于群（G，∘）的任意元素a，b，c，如果a ∘ b = a ∘ c 或者 b ∘ a = c ∘ a，则b = c。

9.3 群

（6）对于群（G，◦）的任意元素a，b，$(a^{-1})^{-1} = a$ ，$(a \circ b)^{-1} = b^{-1} \circ a^{-1}$，$(a^n)^{-1} = (a^{-1})^n$。

（7）对于群（G，◦）的任意元素a，a的阶与a^{-1}的阶相同。

（8）如果f是从群（G，◦）到（H，*）的满同态，则（H，*）也是群。

（9）如果f是从群（G，◦）到群（H，*）的同态，e_G和e_H分别为（G，◦）和（H，*）的单位元，则f（e_G）= e_H，对于群（G，◦）的任意元素a，$f(a^{-1}) = f(a)^{-1}$。

9.3 群

9.3.3子群与陪集

1.子群

- 定义9.13 设（G，◦）是一个群，如果H是G的非空子集，并且（H，◦）也是一个群，则称（H，◦）是（G，◦）的一个子群。如果H是G的真子集，则称（H，◦）是（G，◦）的一个真子群。
- 设e是群（G，◦）的单位元，则（G，◦）和（{e}，◦）都是（G，◦）的子群，称它们为（G，◦）的平凡子群。
  - 群（Z，+）是群（Q，+）和群（R，+）的真子群，（Q，+）也是群（R，+）真子群，但是（N，+）只是上述几个群的子代数；群（Q – {0}，×）也是群（R – {0}，×）的真子群。
  - 群（Z_6，$+_6$）有（{0}，$+_6$），（{0，2，4}，$+_6$），（{0，3}，$+_6$）和（{0，1，2，3，4，5}，$+_6$）共四个子群，其中（{0}，$+_6$），（{0，2，4}，$+_6$）（{0，3}，$+_6$）是真子群，（{0}，$+_6$）（{0，1，2，3，4，5}，$+_6$）是平凡子群。

9.3 群

- 定理9.5 设（G，◦）是一个群，H是G的一个非空子集，则（H，◦）是（G，◦）的子群的充分必要条件是

  （1）如果a，b∈H，则a◦b∈H；

  （2）如果a∈H，则a^{-1}∈H。

  - 推论 设（H，◦）是群（G，◦）的一个子群，则群（G，◦）的单位元也是（H，◦）的单位元，H中元素a的逆元也是G中a的逆元。

- 定理9.6 设（G，◦）是一个群，H是G的一个非空子集，则（H，◦）是（G，◦）的子群的充分必要条件是对于任意的a，b∈H，有 $a \circ b^{-1}$∈H。

- 定理9.7 设（G，◦）是一个群，若H是G的一个有限非空子集，则（H，◦）是（G，◦）的子群的充分必要条件是对于任意的a，b∈H，a◦b∈H。

9.3 群

2.陪集

- 定义9.14　　设（H，∘）是群（G，∘）的子群，对于a∈G，集合aH = {a∘h | h∈H }称为元素a所确定的子群（H，∘）的左陪集，而集合Ha = {h∘a | h∈H }称为元素a所确定的子群（H，∘） 的右陪集。

- 如果群（G，∘）是可交换群，并且（H，∘）是其子群，则aH = Ha，即任意元素所确定的左陪集等于它确定的右陪集。
  - 群（Z_6，$+_6$）是可交换群，H = {0，2，4}，子群（H，$+_6$）的左陪集为0H = {0，2，4}，1H = {1，3，5}，2H = {2，4，0}，3H = {3，5，1}，4H = {4，0，2}，5H = {5，1，3}，即，不同的左陪集只有0H和1H。

9.3 群

- 定理9.8 设（H，∘）是群（G，∘）的一个子群，H的所有左陪集构成了G的一个划分，H的所有右陪集也构成了G的一个划分。

- 定理9.9 设（H，∘）是群（G，∘）的一个子群，对任意$a \in G$，有$|aH| = |Ha| = |H|$。

9.3 群

- 定理9.10（拉格朗日定理） 设（G，∘）是有限群，子群（H，∘）的左陪集的个数是|G|/|H|。

- 推论

（1）任一个阶为素数的有限群没有非平凡子群。

（2）设有限群（G，∘）的阶为n，则它的任一子群的阶都是n的因子。

（3）设有限群（G，∘）的阶为n，则对于任意的a∈G，都有$a^n=e$。

（4）任一个阶为素数的有限群，对于任意的元素a，g∈G且g不是单位元，存在i∈Z使得$a = g^i$。

9.3 群

- 群（Z_6，$+_6$）的阶为6，它的单位元为0，并且，$0^6 = 1^6 = 2^6 = 3^6 = 4^6 = 5^6 = 0$。它有四个子群（{0}，$+_6$），（{0，2，4}，$+_6$），（{0，3}，$+_6$）和（{0，1，2，3，4，5}，$+_6$）。其中，

  （1）子群（{0}，$+_6$）的阶为1，它的左陪集有6 / 1 = 6个，即，0H = {0}，1H = {1}，2H = {2}，3H = {3}，4H = {4}，5H = {5}；

  （2）子群（{0，2，4}，$+_6$）的阶为3，它的左陪集有6 / 3 = 2个，即，0H ={0，2，4}，1H = {1，3，5}；

  （3）子群（{0，3}，$+_6$）的阶为2，它的左陪集有6 / 2 = 3个，即，0H ={0，3}，1H = {1，4}，2H = {2，5}；

  （4）子群（{0，1，2，3，4，5}，$+_6$）的阶为6，它的左陪集有6 / 6 = 1个，就是它自身。

- 群（Z_5，$+_5$）的阶为5，它的单位元为0，并且，$0^5 = 1^5 = 2^5 = 3^5 = 4^5 = 0$。它只有两个平凡子群（{0}，$+_5$）和（{0，1，2，3，4}，$+_5$）。并且，$2 = 1^2$，$3 = 1^3$，$4 = 1^4$；$1 = 2^3$，$3 = 2^4$，$4 = 2^2$；$1 = 3^2$，$2 = 3^4$，$4 = 3^3$；$1 = 4^4$，$2 = 4^3$，$3 = 4^2$。

9.3 群

3.正规子群*

- 定义9.15　　设（H，∘）是群（G，∘）的子群，若对于任意的a∈G，都有aH = Ha，则称（H，∘）是群（G，∘）的正规子群。
  - 群（Z，+）是群（Q，+）和群（R，+）的正规子群，（Q，+）又是群（R，+）正规子群；群（Q – {0}，×）也是群（R – {0}，×）的正规子群。
  - 群（Z_6，$+_6$）的四个子群（{0}，$+_6$），（{0，2，4}，$+_6$），（{0，3}，$+_6$）和（{0，1，2，3，4，5}，$+_6$）都是正规子群。

9.3 群

- 定理9.11 设（G，◦）是一个群，H是G的一个非空子集，则（H，◦）是（G，◦）的正规子群的充分必要条件是对任意$a \in G$，$h \in H$，有$a \circ h \circ a^{-1} \in H$。

- 定理9.12 设（H，◦）是群（G，◦）的正规子群，定义商集G/H上的运算*为aH * bH =（a◦b）H，则得到的代数系统（G/H，*）是一个群。

- 定理9.13 设（H，◦）是群（G，◦）的正规子群，定义映射f：G→G/H，f（a）= aH，则f是从（G，◦）到（G/H，*）的满同态映射。

  定理9.13定义的映射称为自然映射。

9.3 群

- 定义9.16 设f是从（G，◦） 到（H，*）的群同态，e_H 是（H，*）的单位元，则G的子集K = {k | k∈G，f（k）= e_H}称为同态f的核。

- 定理9.14 设K是从（G，◦）到（H，*）的群同态的核，则（K，◦）是（G，◦）的一个正规子群。

- 定理9.15（同态基本定理） 设f是从群（G，◦）到（G’，*）的满同态，K是f的同态核，则必有（G/K，△）与（G’，*）同构。其中，（G/K，△）为正规子群（K，◦）的商群。

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

9.3 群

9.3.4循环群与置换群

1.循环群

- 定义9.17 设（G，◦）是一个群，如果存在$g \in G$，使得对于任意元素$a \in G$，都能表示成$a = g^i$，$i \in Z$，则称群（G，◦）是由g生成的循环群，g称为群（G，◦）的生成元。
  - （Z，+）是一个无限循环群，1是该群的生成元，–1也是该群的生成元。
  - （Z_6， $+_6$ ）是一个6阶循环群，显然1及其逆元5都是该群的生成元，Z_6的其它元素都不是该群的生成元，而Z_6中只有1、5与6互素。

9.3 群

- 定理9.16 对于由g生成的循环群（G，◦）

  （1）如果g的阶无限，则（G，◦）与（Z，+）同构，G只有两个生成元，即，g和g^{-1}。

  （2）如果g的阶为n，则（G，◦）与（Z_n，◦）同构，对于任何小于n且与n互素的正整数r，g^r是G的生成元，即，G含有φ（n）个生成元。

- 推论

  （1）阶为素数的循环群，除了单位元外，其它元素都是该群的生成元。

  （2）循环群的子群一定是循环群，且子群的阶是该群的阶的因子。

  （3）由循环群中任意元素可生成一个该群的循环子群。

9.3 群

2.置换群

- 定义9.18 有限集合S上的任何双射称为集合S的一个置换。

- 设有限集合S集合有n个元素，不妨设S = {1，2，…，n}，S上的一个置换P：S→S通常表示为

$$P=\begin{pmatrix} 1 & 2 & \cdots & n \\ P(1) & P(2) & \cdots & P(n) \end{pmatrix}$$

9.3 群

- 定义9.19 n个元素的有限集S上所有的置换所组成的集合S_n及其复合运算构成的群（S_n，◦）称为S的对称群。S的对称群的子群（S’，◦）称为S的置换群。

- 定理9.17　　每个有限群都与一个置换群同构。

9.4 环与域

9.4.1环与域的概念

❖ 定义9.20 设（R，◦，*）是代数系统，如果

（1）（R，◦）是可交换群；

（2）（R，*）是半群；

（3）运算*对运算满足分配律；

则称（R，◦，*）为一个环。

9.4 环与域

❖ 定义9.21 设（R，◦，*）是一个环，如果

（1）（R，*）为可交换群，则称（R，◦，*）为可交换环。

（2）（R，*）含有单位元，则称（R，◦，*）为单位环（含幺环）。

（3）R中不含零因子，则称（R，◦，*）为无零因子环。

（4）R是可交换环、单位环和无零因子环，则称（R，◦，*）为整环。

9.4 环与域

- 代数系统（Z，+，×），（Q，+，×），（R，+，×）都是环，而且是可交换环、单位环和无零因子环，因此都是整环。

- 代数系统（Z_n，$+_n$，$\times_n$）是环，而且是可交换环和单位环，但不一定是整环。（ Z_6，$+_6$，$\times_6$）不是整环，因为0是Z_6关于的单位元，$2^3 = 0$，因此Z_6含有零因子；但（Z_5，$+_5$，$\times_5$）是整环。

9.4 环与域

- 定义9.22 设（R，∘，*）是一个环，S是R的非空子集，并且（S，∘，*）也是一个环，则称（S，∘，*）是（R，∘，*）的子环。如果S是R的真子集，则称（S，∘，*）是（R，∘，*）的真子环。

- 环（Z，+，×）是环（Q，+，×）和（R，+，×）的真子环。
- 设B是集合A的非空子集，（ρ（B），∩，∪）是环（ρ（A），∩，∪）的子环。

9.4 环与域

- 定义9.23 环（F，∘，*）满足下列条件：

（1）F中至少有两个元素；

（2）（F，*）为可交换群；

（3）（F，*）含有单位元；

（4）（F – {θ}，*）都有逆元。

则称（F，∘，*）为一个域。其中θ为（F，∘）的单位元。

- 整环（Z，+，×）不是域，因为（Z，+）的单位元是0，Z – {0}中的元素除了±1外，关于×没有逆元。但是，整环（Q，+，×），（R，+，×）都是域。
- 环（Z_6，$+_6$，$\times_6$）不是域，因为2、3、4关于没有逆元；而整环（Z_5，$+_5$，$\times_5$）是域。

9.4 环与域

9.4.2环与域的性质*

❖ 对于环（R，◦，*），如果θ为R关于◦的单位元，对任意a∈R，用–a表示a在R中关于◦的逆元，环的重要性质如下：

（1）对任意a∈R，$a * \theta = \theta * a = \theta$。

（2）对任意a，b∈R，$a * (-b) = (-a) * b = -(ab)$，$(-a) * (-b) = a * b$。

（3）环（R，，*）无零因子的充分必要条件是，对任意元素a，b，c∈R，a≠θ，如果$a * b = a * c$ 或者$b * a = c * a$，则$b = c$。

9.4 环与域

- 定理9.18 环（Z_n，$+_n$，$\times_n$）是整环的充分必要条件是n为素数。

- 定理9.19 域一定是整环，至少有两个元素的有限整环一定是域。

9.5 格与布尔代数

9.5.1格的概念与性质

- 定义9.24 设（L，∧，∨）是一个代数系统，∧和∨是L上的两个二元运算，如果这两个运算满足交换律、结合律和吸收律，则称（L，∧，∨）为一个代数格。

- 定义9.25 设（L，≦）是一个偏序集，如果任意两个元素构成的子集均存在最大下界和最小上界，则称偏序集（L，≦）为偏序格。

- 定理9.20 代数格和偏序格是等价的。

9.5 格与布尔代数

- 设A是一个非空集合，在代数系统（ρ（A），∩，∪）中，由集合论的介绍，集合的交运算和并运算满足交换律、结合律和吸收律，因此（ρ（A），∩，∪）是一个代数格。对偏序集（ρ（A），⊆），ρ（A）的任意两个元素是A的两个子集，二者的最大下界是其交集，最小上界是其并集，因此，（ρ（A），⊆）是一个偏序格。

- 对集合{1，2，3，4，6，12}上整除关系“|”，偏序集（{1，2，3，4，6，12}，|）的任意两个元素构成的子集的最大下界是这两个整数的最大公因子，最小上界是这两个整数的最小公倍数，因此，（{1，2，3，4，6，12}，|）是一个偏序格。如果记gcd（x，y）为求两个整数x和y的最大公因子的运算，记lcm（x，y）为求两个整数的最小公倍数的运算，显然，这两个运算满足交换律、结合律和吸收律，因此，（{1，2，3，4，6，12}，gcd，lcm）是一个代数格。

9.5 格与布尔代数

- 定义9.26 设（L，∧，∨）是一个格，S是L的非空子集，并且（S，∧，∨）也是一个格，则称（S，∧，∨）是（L，∧，∨）的子格。
  - {1，2，3，12}$\subseteq${1，2，3，4，6，12}，并且，集合{1，2，3，12}及其上的整除关系可以构成一个格，但是2和3的最小上界是6，因而它不是（{1，2，3，4，6，12}，gcd，lcm）的子格。
  - 映射f：{1，2，3，6}→ρ（{a，b}），f（1）=Ø，f（2）= {a}，f（3）= {b}，f（6）= {a，b}，显然这是一个双射，并且，gcd（x，y）= f（x）∩f（y），lcm（x，y）= f（x）∪f（y），因此，f是一个同构映射。格（{1，2，3，6}，gcd，lcm）与（ρ（{a，b}），∩，∪）同构。

9.5 格与布尔代数

- 除了定义中要求格的运算满足交换律、结合律和吸收律外，格还满足下面的重要性质：

（1）格的两个运算∧和∨满足幂等律。

（2）格的子代数必为格。

（3）格满足对偶原理，即，如果（L，∧，∨）是一个格，（L，∨，∧）也是一个格；或者说，如果（L，≤）是一个格，（L，≥）也是一个格。

9.5 格与布尔代数

9.5.2分配格、有补格

- 定义9.27 设（L，∧，∨）是一个格，如果格的两个运算∧和∨还满足分配律，则称（L，∧，∨）为分配格。
  - 设A是一个非空集合，则格（ρ（A），∩，∪）是一个分配格。

- 定理9.21 在格（L，∧，∨）中，如果∧对∨是可分配的，则∨对∧也是可分配的；如果∨对∧是可分配的，则∧对∨也是可分配的。

- 定理9.22 设（L，∧，∨）是分配格，对于任意a，b，c∈L，b∨a = c∨a，b∧a = c∧a的充分必要条件是b = c。

9.5 格与布尔代数

- 定义9.28 设（L，∧，∨）是一个格，如果L中存在有最小元和最大元，则称（L，∧，∨）为有界格。
  - 设A是一个非空集合，格（ρ（A），∩，∪）的最大元是A，最小元是Ø，因此，（ρ（A），∩，∪）是一个有界格。
  - 格（{1，2，3，4，6，12}，gcd，lcm）的最大元是12，最小元是1，因此，（{1，2，3，4，6，12}，gcd，lcm）是一个有界格。

- 定理9.23 有限格都是有界格。

9.5 格与布尔代数

- 定义9.29 设（L，∧，∨）是有界格，对于任意$a \in L$，如果存在$b \in L$，使得$a \vee b = 1$，$a \wedge b = 0$，则称元素b是a的补元。如果L中每个元素都有补元，则称（L，∧，∨）为有补格。
  - 设A是一个非空集合，有界格（ρ（A），∩，∪）的任意元素x的补元是$A - x$，即x相对于A的补集，因此，（ρ（A），∩，∪）是有补格。
  - 格（{1，2，3，4，6，12}，gcd，lcm）不是有补格，因为2、6没有补元。

9.5 格与布尔代数

9.5.3布尔代数

- 定义9.30 如果一个格既是有补格又是分配格，则称它为有补分配格或布尔代数。
  - 设A是一个非空集合，格（ρ（A），∩，∪）既是有补格，又是分配格，因此，格（ρ（A），∩，∪）是一个布尔代数。

- 定理9.24 在布尔代数中，每个元素都存在唯一的补元。

9.5 格与布尔代数

- 布尔代数（B，∧，∨，⁻）具有的重要性质：

（1）交换律：对任意元素a，b∈B，a∧b = b∧a，a∨b = b∨a。

（2）结合律：对任意元素a，b，c∈B，a∧（b∧c）=（a∧b）∧c，a∨（b∨c）=（a∨b）∨c。

（3）吸收律：对任意元素a，b∈B，a∧（a∨b）= a，a∨（a∧b）= a。

（4）幂等律：对任意元素a∈B，a∧a = a，a∨a = a。

（5）分配律：对任意元素a，b，c∈B，a∧（b∨c）=（a∧b）∨（a∧c），a∨（b∧c）=（a∨b）∧（a∨c）。

9.5 格与布尔代数

（6）互补律：对任意元素a∈B，$a \wedge \bar{a} = 0$ ，$a \vee \bar{a} = 1$。

（7）对合律：对任意元素a∈B，$\bar{\bar{a}} = a$ 。

（8）同一律：对任意元素a∈B，$a \wedge 1 = a$，$a \vee 0 = a$。

（9）零一律：对任意元素a∈B，$a \wedge 0 = 0$，$a \vee 1 = 1$。

（10）德•摩根律：对任意元素a，b∈B，$\overline{a \wedge b} = \bar{a} \vee \bar{b}$ ，$\overline{a \vee b} = \bar{a} \wedge \bar{b}$ 。

9.5 格与布尔代数

- 定义9.31 设（B，∧，∨，⁻）是一个代数系统，∧和∨是B上的两个二元运算，⁻是B上的一元运算，如果

（1）对任意a，b∈B，a∧b = b∧a，a∨b = b∨a;

（2）对任意a，b，c∈B，a∧（b∨c）=（a∧b）∨（a∧c），a∨（b∧c）=（a∨b）∧（a∨c）；

（3）存在B中元素0和1，对任意a∈B，a∧1 = a，a∨0 = a;

（4）对任意a∈B，$a \wedge \bar{a} = 0$ ，$a \vee \bar{a} = 1$

则称（B，∧，∨，⁻）是一个布尔代数。

- 由非空集合A的幂集ρ（A）及其上的交、并、补运算构成的布尔代数（ρ（A），∩，∪，⁻），称为集合代数。

9.5 格与布尔代数

- 定义9.32 设（B，∧，∨，⁻）是一个布尔代数，S是B的非空子集，如果运算∧、∨和–对S封闭，并且0，1∈B，则称（S，∧，∨，⁻）是（B，∧，∨，⁻）的子布尔代数。
  - 设A = {a，b，c}，对集合A的非空子集B = {b，c}，代数系统（ρ（B），∩，∪，⁻）是布尔代数，但不是（ρ（A），∩，∪，⁻）的子布尔代数，因为，虽然Ø∈ρ（B），但是A∉ρ（B）。而代数系统（{Ø，{a}，{b，c}，{a，b，c}}，∩，∪，⁻）是布尔代数，并且是（ρ（A），∩，∪，⁻）的子布尔代数。
  - 布尔代数（{Ø，{a}，{b，c}，{a，b，c}}，∩，∪，⁻）与集合代数（ρ（{a，b}），∩，∪，⁻）同构。因为可构造同构映射g：{Ø，{a}，{b，c}，{a，b，c}}→ρ（{a，b}），g（Ø）= Ø，g（{a}）= {a}，g（{b，c}）= {b}，g（{a，b，c}）= {a，b}。

9.5 格与布尔代数

- 定理9.25 设（B，∧，∨，－）是一个有限布尔代数，则必有含有n个元素的集合A，使得（B，∧，∨，–）与（ρ（A），∩，∪，－）同构。

- 推论

  （1）任意有限布尔代数的元素个数必为2的整数次幂。

  （2）所有含有2^n个元素的布尔代数都同构。

  （3）布尔代数的最少元素个数是2个。

本章小结

- 代数系统
  - 运算的定义
  - 交换律、结合律、分配律等运算性质
  - 单位元、零元、逆元等特殊元素
  - 代数系统同态与同构
- 群
  - 半群、独异点和群的概念与性质
  - 子群与正规子群的判定定理
  - 拉格朗日定理
  - 循环群和置换群的概念与性质
- 环与域
- 格
  - 代数格和偏序格的定义
  - 对偶原理
  - 分配格、有补格、有界格
  - 布尔代数