5-9 环与域

以上，我们已初步研究了具有一个二元运算的代数系统——半群、独异点、群。接着，我们将讨论具有两个二元运算的代数系统。对于给定的两个代数系统<A,★>和<A,*>，容易将它们组合成一个具有两个二元运算的代数系统<A,★,*>。我们感兴趣于两个二元运算★和*之间有联系的代数系统<A,★,*>，通常，我们把一个二元运算★称为“加法”，把第二个运算*称为“乘法”。

例如，具有加法和乘法这两个二元运算的实数系统<R,+,×>和整数系统<I,+, ×>都是我们很熟悉的代数系统。

它们运算之间的联系是乘法对加法满足分配律。

定义5-9.1： 设<A,★,*>是一个代数系统，如果满足：

1.<A,★>是阿贝尔群。

2.<A,*>是半群。

3.运算*对于运算★是可分配的。

则称<A,★,*>是环。

根据定义可以清楚地看到，整数集合、有理数集合、偶数集合、复数集合以及定义在这些集合上的普通加法和乘法运算都是可构成环的例子。

例1 系数属于实数的所有x的多项式所组成的集合记作R[x]，那么，R[x]关于多项式的加法和乘法构成一个环。

例2 元素属于实数的所有n阶矩阵所组成的集合记作$(R)_n$，那么，$(R)_n$关于矩阵的加法和乘法构成一个环。

定理5-9.1： 设<A,+, ·>是一个环，则对于任意的a,b,c∈A，有

1. $a \cdot \theta = \theta \cdot a = \theta$
2. $a\cdot(-b) =(-a) \cdot b = -(a\cdot b)$
3. $(-a) \cdot (-b) = a\cdot b$
4. $a\cdot(b-c) = a\cdot b - a\cdot c$
5. $(b-c) \cdot a =b\cdot a -c\cdot a$

其中，θ是加法幺元，- a是a的加法逆元，并将a+(-b)记为a-b。

我们还可以根据<A , ·>的结构来定义一些常见的特殊环。

定义5-9.2：设<A ,+, ·>是环。如果<A , ·>是可交换的，则称<A ,+,·>是交换环。如果<A , ·>含有幺元，则称<A ,+, ·>是含幺环。

设S是一个集合，P(S)是它的幂集，如果在P(S)上定义二元运算+和·如下：对任意的A，B∈ P(S)

$$A+B=\{x|(x\in S)\wedge(x\in A\vee x\in B)\wedge(x\notin A\cap B)\}$$

$$A\cdot B= A\cap B$$

容易证明<P(S) , + ,·>是一个环，称它为S的子集环。

由于集合交运算是可交换的，且<P(S) , ·>含有幺元S，因此子集环是含幺交换环。

定义5-9.3：设<A ,+, ·> 是一个代数系统，如果满足：

1. <A,+>是阿贝尔群。
2. <A, ·>是可交换独异点，且无零因子，即对任意的a,b∈A , a≠θ , b≠θ , 必有a · b≠θ。
3. 运算 · 对于运算 + 是可分配的。

则称<A ,+, ·>是整环。

下面我们来考察<I ,+, ·>是否为整环

因为<I, +>是一个具有加法幺元0，且对任意n有逆元-n的阿贝尔群；

<I, ·>是可交换独异点，

且满足无零因子条件；

运算 · 对于运算 + 是可分配的，

故<I ,+, ·>是整环。

定理5-9.2： 在整环<A ,+, ·>中的无零因子条件等价于乘法消去律，即对于c≠θ和 c ·a=c · b，必有a=b。

证明：“⇒”若无零因子并设c≠θ和 c ·a=c · b，

则有 c ·a - c · b = c · (a-b)= θ

所以，必有a=b。

“⇐” 反之，若消去律成立，

设a≠θ，a · b=θ

则a · b= a · θ 消去a

即得b= θ。

定义5-9.4：设<A ,+, ·> 是一个代数系统，如果满足：

1. <A,+>是阿贝尔群。
2. <A-{θ} , ·>是阿贝尔群。
3. 运算 · 对于运算 + 是可分配的。

则称<A ,+, ·>是域。

例如，<Q ,+, ·>，<R ,+, ·>，<C ,+, ·>都是域，这里，Q为有理数集合，R是实数集合，C是复数集合，而+, ·分别是各数集上的加法和乘法运算。

必须指出，<I ,+, ·>是整环，但不是域，

因为<I-{0} , ·>不是群。这说明，整环不一定是域。

定理5-9.4：有限整环必定是域。

证明：见P226

定义5-9.5：设<A ,+, ·> 和<B ,⊕ ,⊙>是两个代数系统，如果一个从A到B得映射f，满足如下条件：

对于任意的a,b∈A，有

$f(a+b)=f(a)\oplus f(b)$

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

则称f为由<A ,+, ·> 到<B , ⊕, ⊙>的一个同态映射，并称<f(A) , ⊕, ⊙>是<A ,+, ·>的同态象。

定理5-9.5：任一环的同态象是一个环。

证明：**P228**

作业：(5-9)

P228 (4) a) b)

(7) a) c)

(6) 选作