第八章　群和环

第十七节 环与域(1)


一个运算
半群
独异点
群
特殊代数系统
布尔代数
三个运算
环
域
两个运算

一. 环(Ring)

定义：给定代数系统 <A,+,·>，+ 和 · 是 A 上二元 运算，若满足以下条件：

(1) <A,+> 是交换群。

(2) <A, ·> 是半群。

(3) · 对 + 可分配。即对任何 $a,b,c \in A$，有

$$a\cdot(b+c)=(a\cdot b)+(a\cdot c) \text{ 及 } (a+b)\cdot c=(a\cdot c)+(b\cdot c)$$

则称 <A,+,·> 是个环。

思考

$<R, +, \cdot>$、$<\mathcal{P}(E), \oplus, \cap>$是否是环？

$<\mathcal{P}(E), \cap, \cup>$、$<\mathcal{P}(E), \oplus, \cup>$是否是环？

因为 $<\mathcal{P}(E), \cap>$ 不是群，所以 $<\mathcal{P}(E), \cap, \cup>$ 不是环。

因为 $\cup$ 对 $\oplus$ 不可分配，所以 $<\mathcal{P}(E), \oplus, \cup>$ 不是环。

并且 $\cdot$ 对 $+$ 可分配，所以 $<R, +, \cdot>$ 是环。

$<\mathcal{P}(E), \oplus, \cap>$是环，因为 $<\mathcal{P}(E), \oplus>$ 是交换群；

$<\mathcal{P}(E), \cap>$是半群；并且 $\cap$ 对 $\oplus$ 可分配，

所以 $<\mathcal{P}(E), \oplus, \cap>$ 是环。

二. 环的运算法则

设<A, + ,· >是环，任意 $a,b,c\in A$,

符号约定：

对 +：幺元用 0 表示，a 的逆元用 $-a$ 表示；

对 · ：幺元用 1 表示，a 的逆元用 a^{-1} 表示。

将 $a+(-b)$ 记为 $a-b$。

定理1

设<A, + ,· >是环，任意 $a,b,c \in A$,

(1) $a \cdot 0 = 0 \cdot a = 0$

(+ 的幺元，恰是 · 的零元)

(1) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b) = -a \cdot b$

(2) $(-a) \cdot (-b) = a \cdot b$

(3) $a \cdot (b-c) = (a \cdot b) - (a \cdot c) = a \cdot b - a \cdot c$

(4) $(a-b) \cdot c = a \cdot c - b \cdot c$

定理1

设<A, + ,· >是环，任意 $a,b,c \in A$,

(1) $a\cdot 0=0\cdot a=0$ （+ 的幺元，恰是 · 的零元）

证明： 因为 $a\cdot 0+a\cdot 0=a\cdot(0+0)=a\cdot 0=a\cdot 0+0$,

由<A, + >是交换群，满足消去律，所以

$a\cdot 0=0$。 类似可证 $0\cdot a=0$

(2) $(-a)\cdot b= a\cdot(-b)= -(a\cdot b)$

证明： 因为 $a\cdot b+a\cdot(-b)=a\cdot(b+(-b))=a\cdot 0=0$,

即 $a\cdot(-b)$ 是 $a\cdot b$ 的 + 运算逆元，于是

$$a\cdot(-b)= -(a\cdot b)$$

类似可证 $(-a)\cdot b= -(a\cdot b)$

(3) $(-a)\cdot(-b)=a\cdot b$

证明：根据(2)

$$(-a)\cdot(-b)=-(a\cdot(-b))=-(-(a\cdot b))=a\cdot b$$

(4) $a\cdot(b-c)=a\cdot b-a\cdot c$

证明：

$$a\cdot(b-c)=a\cdot(b+(-c))=a\cdot b+a\cdot(-c)$$
$$=a\cdot b+(-(a\cdot c))=a\cdot b-a\cdot c$$

(5) $(a-b)\cdot c=a\cdot c-b\cdot c$

证明：

$$(a-b)\cdot c=(a+(-b))\cdot c=a\cdot c+(-b)\cdot c$$
$$=a\cdot c+(-(b\cdot c))=a\cdot c-b\cdot c$$

例： 在环中计算 $(a+b)^3$, $(a-b)^2$

解：
$$(a+b)^3 = (a+b)\cdot(a+b)\cdot(a+b)$$
$$= (a^2+b\cdot a+a\cdot b+b^2)\cdot(a+b)$$
$$= a^3+b\cdot a^2+a\cdot b\cdot a$$
$$+b^2\cdot a+a^2\cdot b+b\cdot a\cdot b+a\cdot b^2+b^3$$

$$(a-b)^2 = (a-b)\cdot(a-b) = a^2-b\cdot a-a\cdot b+b^2$$

第十七节 结束