§ 10.4 环与域

定义 设 $<R,+,\cdot>$ 是一个代数系统，+, · 是两个二元运算，若

（1）$<R,+>$ 构成交换群

（2）$<R,\cdot>$ 构成半群

（3）运算 ·对+满足分配律

则称 $<R,+,\cdot>$ 构成**环**。

例 $<\mathbb{Z},+,\cdot>$，$<\mathbb{R},+,\cdot>$，$<M_n(\mathbb{R}),+,\cdot>$，$<P(B),\oplus,\cap>$，$<\mathbb{Z}_n,\oplus_n,\otimes_n>$ 都是环。

注

① 对环$<R,+,\cdot>$，称$+$为加法，称$\cdot$为乘法（$a\cdot b$可简记为ab）；环$<R,+,\cdot>$可简记为R；

② 群$<R,+>$的单位元称为R的零元，记为0；

③ 若半群$<R,\cdot>$有单位元，则称之为R的单位元，记为1；

以后，用R^*表示$R-\{0\}$。

④ 在群$<R,+>$中，记$a^{-1}\triangleq -a$，$a-b\triangleq a+(-b)$；

⑤ 设R是一个环，$a\in R$，$n\in\mathbb{Z}$，规定

$$na=\begin{cases} 0, & n=0 \\ \underbrace{a+\cdots+a}_{n\text{个}}, & n>0 \\ \underbrace{(-a)+\cdots+(-a)}_{-n\text{个}}, & n<0 \end{cases}$$

$$a^n=\underbrace{aa\cdots a}_{n\text{个}},\quad n>0$$

定理 设R是一个环，则

（1）$\forall a\in R,\ a0=0a=0$

（2）$\forall a,b\in R,\ (-a)b=a(-b)=-(ab)$

（3）$\forall a,b,c\in R,\ a(b-c)=ab-ac,\ (b-c)a=ba-ca$

例 在环R中计算 $(a-b)^2$。

解 由环R的减法定义以及上述定理，

$$
\begin{aligned}
(a-b)^2 &= (a-b)(a-b)\\
&= (a-b)a-(a-b)b\\
&= a^2-ba-(ab-b^2)=a^2-ba-ab+b^2
\end{aligned}
$$

▌

定义 设$<R,+,\cdot>$是一个环

（1）若$<R,\cdot>$是交换半群，则称R是**交换环**；

（2）若$<R,\cdot>$是含幺半群，则称R是**含幺环**；

（3）若$\forall a,b\in R$，$ab=0 \Rightarrow a=0$或$b=0$，则称R是**无零因子环**；

（4）若R可交换、含单位元，也是无零因子环，则称R是**整环**；

（5）若R是整环，至少包含2个元素，且$\forall a\in R^*$，均有$a^{-1}\in R$，则称R是**域**；

例 $<\mathbb{Z},+,\cdot>$是整环

$<Z_6,\oplus_6,\otimes_6>$有零因子 $\Rightarrow$ 不是整环

$<M_n(R),+,\cdot>$有零因子 $\Rightarrow$ 不是整环

$<2\mathbb{Z},+,\cdot>$不含单位元 $\Rightarrow$ 不是整环

$<Z_5,\oplus_5,\otimes_5>$是域

例 三个数域：

有理数域 $<\mathbb{Q},+,\cdot>$

实数域 $<\mathbb{R},+,\cdot>$

复数域 $<\mathbb{C},+,\cdot>$

例 至少包含两个元素的代数系统$<F,+,\cdot>$是域当且仅当:

（1）$<F,+>$是交换群

（2）$<F^*,\cdot>$是交换群

（3）$\cdot$对$+$满足分配律

定义 设F是一个域。若$|F|=n$，则称F是**有限域**，记为F_n或$GF(n)$。

例 $<Z_p,\oplus_p,\otimes_p>$是域$\Leftrightarrow$ p是素数。

定义 设R_1与R_2是两个环，φ：$R_1 \to R_2$。若对$\forall x, y \in R_1$，

$$\varphi(x+y) = \varphi(x) + \varphi(y)$$

$$\varphi(xy) = \varphi(x)\varphi(y)$$

则称φ是R_1到R_2的**同态映射**，简称**环同态**。

类似有**满同态**，**同构**等概念。

例 令φ：$\mathbb{Z} \to Z_n$，$\varphi(k) = k(\bmod n)$, $k \in \mathbb{Z}$，则φ是环 $<\mathbb{Z}, +, \cdot>$ 到环 $<Z_n, \oplus_n, \otimes_n>$ 的满同态。

全同态加密技术 设M, S分别表示明文空间与密文空间，M中的元素为二进制符号串(可视为数)，M中有数的加法+与乘法·两种运算。设E：$M\rightarrow S$是加密函数。若存在S上的运算Add与$Multi$，使得

$$Add(E(x), E(y))=E(x+y)$$

$$Multi(E(x), E(y))=E(x\cdot y)$$

则称加密函数E是**全同态加密函数**。

通过对密文的运算实现对明文的运算

小结：

1. 掌握群的基本概念

   半群、独异点、群、元素的阶、群的阶、同态(构)

2. 掌握子群的概念及性质

   子群的判别、生成子群、拉格朗日定理

3. 掌握循环群与置换群的概念

   有限与无限循环群，置换、轮换、对换

4. 了解环与域的概念

   环、零元、单位元、整环、域、有限域