信息安全数学基础

4.2 整环、除环和域

信息与软件工程学院

整环的定义

- 定义4.2.1 一个有单位元、无零因子的交换环叫做一个整环。
- 例如，Z、Q、R、C都是整环，而2Z、Z_n(n是合数)、$M_n(F)$不是整环。
- 整环中并不是所有的元素都存在乘法逆元。
- 例4.2.1 Q、R、C中任意一个非零数a都有一个逆元$\frac{1}{a}$，且$a\left(\frac{1}{a}\right)=\left(\frac{1}{a}\right)a=1$．而Z中仅有±1是可逆元。

除环和域

定义4.2.2 一个环R称为除环，假如

- ➢R中至少包含一个不等于零的元 (即R中至少有两个元素);
- ➢R有单位元;
- ➢R的每一个不等于零的元有一个逆元。

注意到，除环的概念中，并没有要求它满足乘法交换律。

定义4.2.3 交换除环称为域。

例如，Q、R、C都是域。

除环的性质

定理 4.2.1 （1）除环是无零因子环。

（2）设R是一个非零环，记$R^* = \{a \in R | a \neq 0\} = R\backslash\{0\}$，则R是除环当且仅当$R^*$对于R的乘法构成一个群，称这个群为除环R的乘法群。

证明： （1）设R是除环，$a, b \in R$

$$a \neq 0, ab = 0 \Rightarrow a^{-1}ab = b = 0。$$

（2）R^*对于R的乘法构成一个群，显然R可满足除环定义中的三个条件。

反之，设R是除环。由于R是无零因子环，所以R^*对于乘法封闭；由环的定义，乘法满足结合律；由除环的定义，R^*中有单位元，即R的单位元，而且R^*中每一个元素均有逆元。因此，R^*是群。

非交换除环的例子

例4.2.2 设$H=\{a_0+a_1i+a_2j+a_3k|a_0,a_1,a_2,a_3\in\mathbb{R}\}$是实数域$\mathbb{R}$上的四维向量空间，$1,i,j,k$为其一组基，规定基元素之间的乘法为：

（1）$i^2=j^2=k^2=-1$；（2）$ij=k,jk=i,ki=j$。

将其线性扩张为H中的元素之间的乘法。则H关于向量的加法和上面定义的乘法构成一个除环，称之为（**Hamilton)**四元数除环。

证明：只需证明H^*对于H的乘法构成一个群，为此只需证明H中的每个非零元均可逆：事实上，设$0\neq\alpha=a_0+a_1i+a_2j+a_3k\in H$，则$\Delta={a_0}^2+{a_1}^2+{a_2}^2+{a_3}^2\neq 0$，令$\beta=\frac{a_0}{\Delta}-\frac{a_1}{\Delta}i-\frac{a_2}{\Delta}j-\frac{a_3}{\Delta}k\in H$，则$\alpha\beta=\beta\alpha=1$，即$\alpha$可逆，从而$H$为除环。

有限环与除环

定理4.2.2 一个至少含有两个元素的无零因子的有限环是除环。

证明：设$R=\{0,a_1,\cdots,a_n\}$是一个无零因子环，**n**是正整数，$a_i\neq 0$，$1\leq i\leq n$。要证明R^*对于**R**的乘法构成一个群。

因为**R**无零因子，所以R^*对于**R**中的乘法封闭。任选$a(\neq 0)\in R$，考察$aa_1,aa_2,\cdots,aa_n$。若$aa_i=aa_j$，则$a(a_i-a_j)=0$，又$a\neq 0$，所以$a_i=a_j$。因此，$\{aa_1,aa_2,\cdots,aa_n\}=\{a_1,a_2,\cdots,a_n\}$。同理可得$\{a_1a,a_2a,\cdots,a_na\}=\{a_1,a_2,\cdots,a_n\}$。故对于任意$a,b\in R^*$，方程

$$ax=b\text{和}xa=b$$

在R^*中有解。因此R^*是群。 □

有限整环与除环

推论4.2.1 有限整环是域。

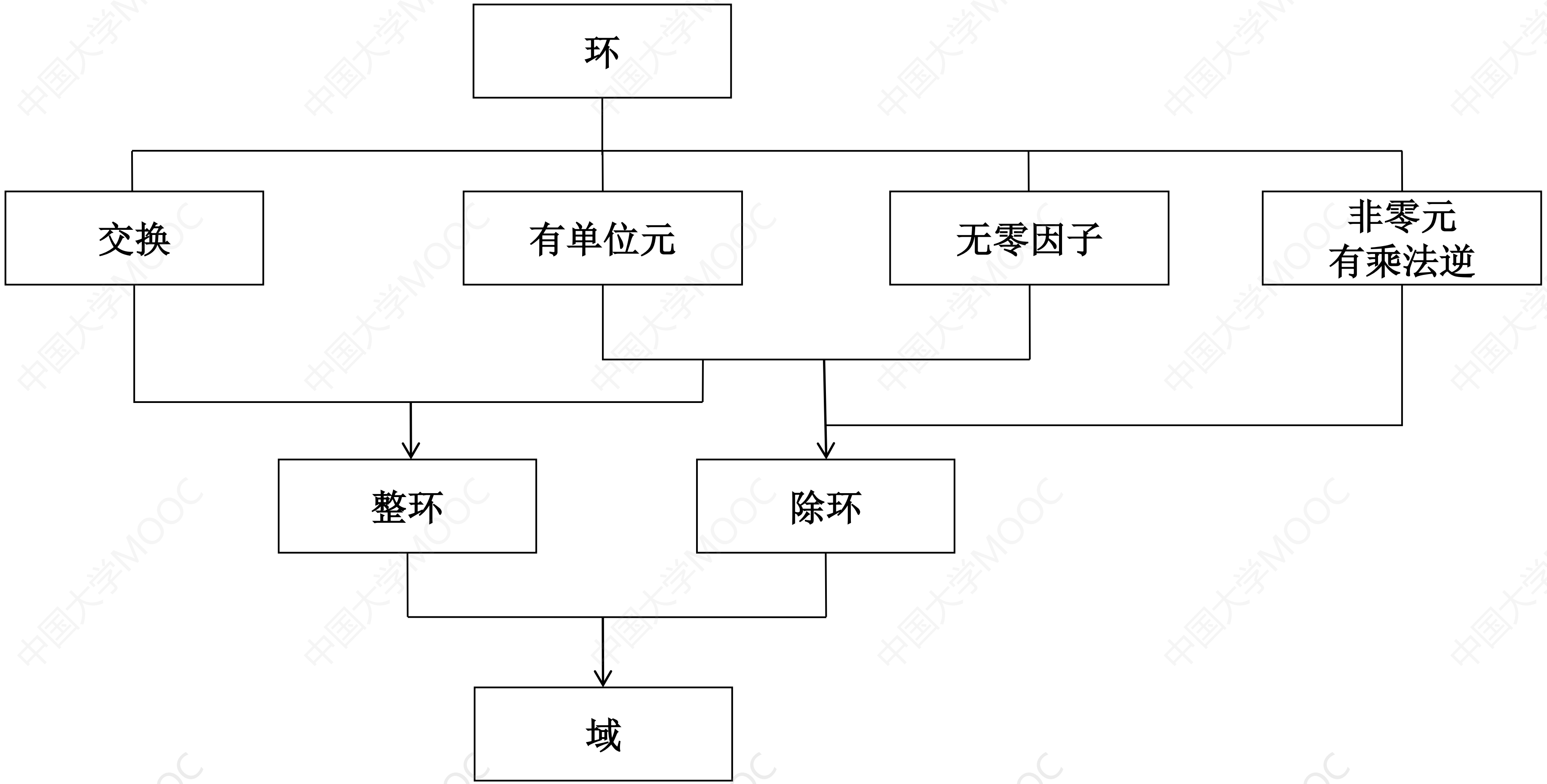
证明：根据定理4.2.2，有限整环是除环，又整环满足乘法交换律，根据域的定义，有限整环是域。

例 4.2.3 模p的剩余类环$\mathbb{Z}_p$是域当且仅当p是素数。

证明：(⇒)：易知$p \neq 0,1$．若p为合数，则$p = ab, a, b \neq \pm 1$．于是$a \neq 0(mod\ p)$，$b \neq 0(mod\ p)$，但$ab \equiv 0(mod\ p)$，即$\mathbb{Z}_p$中有零因子，此与$\mathbb{Z}_p$是域矛盾，故p是素数。

(⇐)：设p是素数．若$ab \equiv 0(mod\ p)$，则$p|ab$，从而$p|a$或$p|b$，即有$a \equiv 0(mod\ p)$或$b \equiv 0(mod\ p)$，故$\mathbb{Z}_p$为一个无零因子环，于是$\mathbb{Z}_p$是一个有限整环，根据推论 4.2.1，$\mathbb{Z}_p$是域。

整环、除环和域



感 谢 聆 听!

xynie@uestc.edu.cn