2022-2023学年秋季学期

课程名称：信息安全数学基础

英文名称：*Mathematical Foundations for Information Security*

授课团队：胡磊、许军、王丽萍

助　　教：郭一

信息安全数学基础

Mathematical Foundations for Information Security

[第 10 次课] 环和域

授课教师：许军

授课时间：2022年11月16日

概　要

- 环的定义
- 零因子、乘法群、特征
- 整环、除环和域
- 子环、理想和商环
- 极大理想、素理想
- 整环的分式化

环的定义

定义：设 R 是一个非空集合，R 上定义有两个代数运算：加法（记为“＋”）和乘法（记为“.”），假如

（1）$(R,+)$是一个**交换群**。

（2）R 关于**乘法满足结合律**。即对于任意 $a,b,c \in R$，有

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

（3）**乘法对加法满足左、右分配律**，即对于任意 $a,b,c\in R$，有

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

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

则称 R 为环。

环的定义（续）

如果，R 还满足

（4）乘法交换，即对于任意$a,b\in R$，有$a\cdot b=b\cdot a$。

则称 R 为交换环。

如果 R 中存在元素1_R，使得

（5）对于任意$a\in R$，有$1_R\cdot a=a\cdot 1_R=a$。

则称 R 为有单位元环。元素1_R（或简记为 1）称为 R 中的单位元。

R 的加法群中的单位元素记为 0，称为环 R 的零元素。R 中的元素$a\in R$加法逆元称为负元，记为$-a$。与第三章中的群的乘法一样，R 中两个元素的乘法$a\cdot b$可简记为ab。

例

- （1）全体整数关于数的普通加法和乘法构成一个环，称为整数环 。

  （２）全体有理数（实数、复数）关于数的普通加法和乘（法构成一个环。

  （3）模 m 的所有剩余类构成一个环，称为模 m 的剩余类环，记为 Z_m 或 Z/mZ。

- 上面的例子都是有乘法单位元的交换环，其乘法单位元都为整数1。
- 事实上有很多环并没有单位元，也可能不满足交换律。

例 4.1.3 设 n 是偶数，$n\mathbb{Z}$ 对于数的普通加法和乘法来说作成一个环. 但 $n\mathbb{Z}$ 没有单位元。

例 4.1.4 数域 F 上的 n 阶方阵的全体关于矩阵的加法和乘法构成一个环，称为 F 上的 n 阶方阵环，记为 $M_n(F)$。这个环的单位元为 n 阶单位矩阵。因为矩阵的乘法不满足交换律，所以 $M_n(F)$ 不是交换环。

例 4.1.5 $R=\{0,a,b,c\}$。加法和乘法由以下两个表给定：

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

×	0	a	b	c
0	0	0	0	0
a	0	0	0	0
b	0	a	b	c
c	0	a	b	c

则 R 对于上述两种运算构成一个环.

证明：首先证明 R 对于加法构成加法交换群。根据其运算表可以看出：

（1）加法封闭。

（2）满足结合律。因为 $a+(b+c)=a+a=0,(a+b)+c=c+c=0$，所以 $a+(b+c)=(a+b)+c$。其余可一一验证。

（3）有零元为 0，0 加上任何 R 中的元素都等于该元素。

（4）有负元。任何 R 中的元素的负元为其本身。

（5）满足交换律。R 的加法运算表是对称的，所以加法满足交换律。

其次，要证明乘法封闭且满足结合律。根据乘法运算表，乘法封闭显然。又 $a(bc)=ac=0,(ab)c=0c=0$，所以 $a(bc)=(ab)c$。其余的结合律可一一验证。

最后，可验证乘法对加法满足结合律。因为，$c(a+b)=cc=c,ca+cb=a+b=c$，所以 $c(a+b)=ca+cb$。其余情形可一一验证。

综上所述，R 是环。

这个环没有乘法单位元，也没有乘法结合律。

环的简单性质

设 R 是一个环，$a,b\in R$，m,n 是正整数，ma 表示 m 个 a 相加，a^m 表示 m 个 a 相乘，则

（1）$a\cdot 0=0\cdot a=0$；

（2）$a(-b)=(-a)b=-(ab)$；

（3）$n(a+b)=na+nb$；

（4）$m(ab)=(ma)b=a(mb)$；

（5）$a^m a^n=a^{m+n}$；

（6）$(a^m)^n=a^{mn}$。

零因子

- 定义： 设R是一个环，如果存在非零元素a和b，满足ab=0，则称环R为有零因子环，称a为R的左零因子，称b为R的右零因子。否则称R为无零因子环。

- 例： Z_m 是无零因子环，当且仅当 m 是素数。
- 例： 设 n≥2，域上 n 阶方阵的集合是有零因子环。

- 无零因子环中消去率成立。
- 在交换环中，左零因子、右零因子的概念是统一的。在非交换环中，左零因子不一定是右零因子，如特殊矩阵环

环中乘法群

- 定义：　设 R 是一个有单位元环，a 是其中一个元素。若存在元素 b，使得 ab=ba=1 ，则称 a 是一个可逆元。
- 环中非零元并不一定有逆元
  - 整数环 Z 中，仅有 1 和-1 两个元素存在逆元
  - 多项式环中，非零常数项存在逆元
  - 域上 n 阶方阵环中，行列式非零的方阵存在逆元
- 乘法可逆元一定不是左、右零因子。
- （有单位元）环中所有可逆元的集合组成一个乘法群，称为环的乘法群

环的特征

- **定理：** 设 R 是一个无零因子环。若 R 中存在一个非零元的加法阶是有限数，则所有非零元的加法阶都是有限数，并且相等，且是某个素数。
- **证明：** 设a、b 是非零元，a的加法阶是整数 n。由na=0，

  0=0b=(a+…+a)b=ab+…+ab=a(b+…+b)　　（n个相加）
- 因为无零因子，a不为0，所以 b+…+b=0，b的加法阶是有限数，且为整数 n 的某个因子 m。反过来，同理可证 a的加法阶是整数 m 的某个因子。因此，n=m。即所有非零元的加法阶相等。
- 设所有非零元的加法阶为n。若n不是素数，设 n=rs，正整数r和s 都小于 n。则 (ra)(sa)=rsa2=(na)a=0

又R是无零因子环，所以 ra=0 或 sa=0，这与n是a的加法阶矛盾。因此，n是素数。

环特征的定义

定义 4.1.4 设 R 是一个无零因子环，称 R 中非零元的加法阶为环 R 的特征，记为 $\mathrm{Char}R$。当 R 中非零元的加法阶为无穷大时，称 R 的特征为零，记 $\mathrm{Char}R=0$；当 R 中非零元的加法阶为某个素数 p 时，称 R 的特征为 p，记 $\mathrm{Char}R=p$。

例 4.1.9 设 R 是特征为 p 的交换环，$a,b\in R$，有 $(a\pm b)^p=a^p\pm b^p$。

证明：$(a+b)^p=a^p+\binom{p}{1}a^{p-1}b+\cdots+\binom{p}{p-1}ab^{p-1}+b^p$。

因为，对于 $1\le k\le p-1$，$\binom{p}{k}=\dfrac{p!}{k!(p-k)!}=\dfrac{p\cdot(p-1)!}{k!(p-k)!}$。

由上式可知 $k!(p-k)!\mid p\cdot(p-1)!$，而 $k!(p-k)!$ 与素数 p 互素，所以 $k!(p-k)!\mid(p-1)!$，因此 $\binom{p}{k}$ 是 p 的倍数，进而有 $\binom{p}{k}a^{p-k}b^{k}=0$，由此可得

$$(a+b)^p=a^p+b^p$$

$(a-b)^p=a^p-b^p$ 的证明留给读者。

例：Z_p的特征为p。 Z_p上多项式环的特征为p。

整环、除环和域

定义： 一个有单位元的无零因子的交换环叫做一个整环。

定义： 一个至少包含两个元素的、有单位元的、每个非零元均有逆元的环R叫做一个除环。

注意到，除环的概念中，并没有要求它满足乘法交换律。

性质：一个有单位元的环的全部非零元构成群，当且仅当这个环是除环。

定义：交换的除环叫做域。

例

- Z_p是整环、除环、域。对m是合数，Z_m不是整环、除环、域。
- 整数环、域上多项式环是整环，不是除环、域。

非交换除环的例子

例 4.2.2 设 $H=\{a_0+a_1i+a_2j+a_3k \mid a_0,a_1,a_2,a_3\in\mathbb{R}\}$ 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：

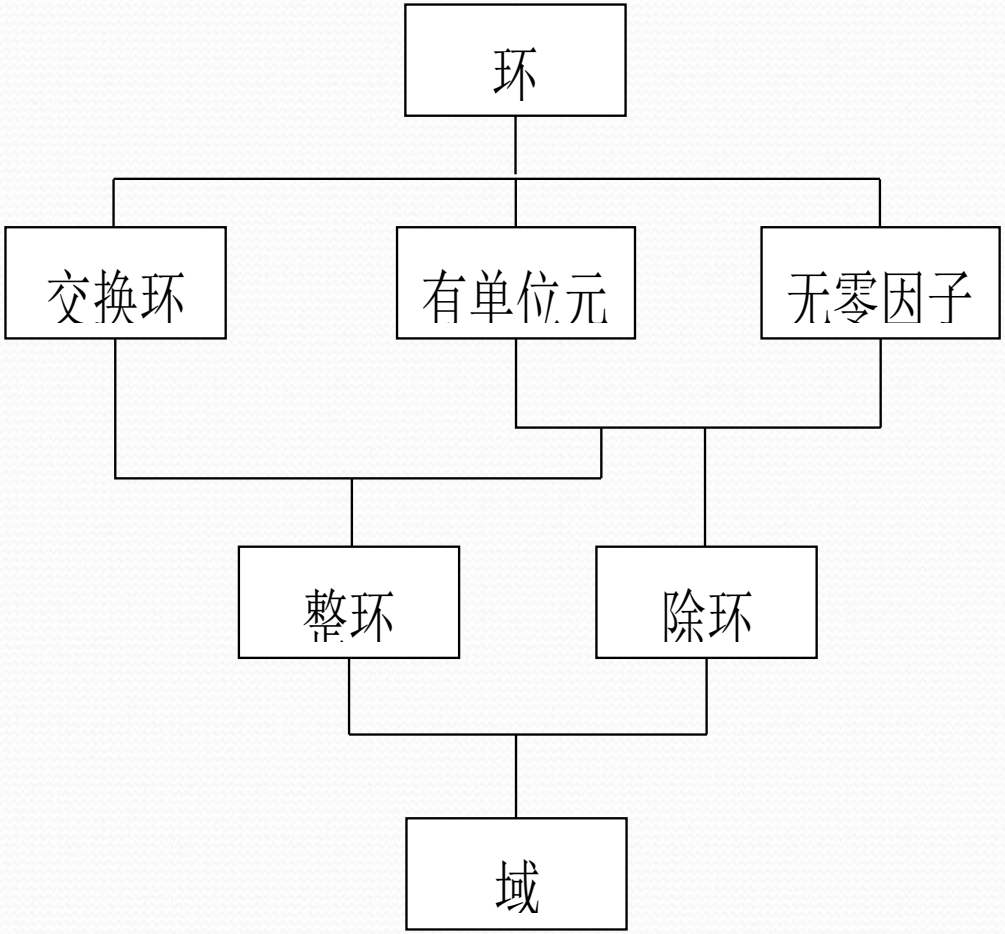
（1）$i^2=j^2=k^2=-1$；　　（2）$ij=k, jk=i, ki=j$。

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 α 可逆，从而 H 为除环。

整环、除环和域

本节中介绍的几种最常见的环之间有如下的关系图：



子环、理想和商环

定义：设 S 是环 R 的一个非空子集合。如果 S 对 R 的两个运算也构成一个环，则称 S 为 R 的一个子环，称 R 为 S 的扩环。

任意环 R 都至少有两个子环：0 和 R，称之为 R 的平凡子环。设$S \le R$且$S \ne R$，则称 S 是 R 的一个真子环。

例： 整数环 Z 是有理数环 Q 的子环，mZ 是 Z 的子环。

例：求模 12 的剩余类环 Z/12Z 的所有子环。

解：由于这个环的加法群是一个循环群，故剩余类环的子环关于加法是加法群的子循环群，共有下面 6 个：

$$S_1=([1])=R;\quad S_2=([2])=\{[0],[2],[4],[6],[8],[10]\};\quad S_3=([3])=\{[0],[3],[6],[9]\};$$

$$S_4=([4])=\{[0],[4],[8]\};\quad S_5=([6])=\{[0],[6]\};\quad S_6=([0])=\{[0]\}=0。$$

商环

- 设R是环，S是 R 的子环， S是 R 的加法子群，R可以写成S的陪集之并。 $a+S=a'+S$ 当且仅当 $a'-a \in S$
- 那么在陪集集合 中定义两个陪集的加法：

$$(a+S)+(b+S)=(a+b)+S$$

这个定义是良的。（交换群的任意子群是正规子群）

- 定义两个陪集的乘法为：

$$(a+S)(b+S)=(ab)+S$$

这个定义有没有问题？

即若 $a+S=a'+S$, $b+S=b'+S$ ，是否有 $(ab)+S=(a'b')+S$，也就是$a'b'-ab \in S$。已知 $a'-a \in S$ 和 $b'-b \in S$。注意到

$$a'b'-ab = a'(b'-b) + (a'-a)b$$

- 分别取$a'-a=0$ 和 $b'-b=0$，看看S要满足什么要求？

理想

为此，引入理想的概念：

定义 4.3.3 设 R 是一个环，I 是 R 的一个非空子集，若满足

（1）$a-b\in I,\forall a,b\in I$ ；

（2）$ar\in I$，且 $ra\in I$，$\forall a\in I$，$\forall r\in R$；

则称 I 为环 R 的一个理想，记为 $I\lhd R$.

理想一定是子环，反之未必。对于任意环 R，{0}和 R 都是理想，分别称之为零理想和单位理想。

例 4.3.6 整数 n 的所有倍数之集 $(n)=\{nk\,|\,k\in\mathbb{Z}\}$ 构成整数环 $\mathbb{Z}$ 的一个理想。

理想的例子

- Z的全部理想为mZ，m为非负整数
- 域K上多项式环K[x]的全部理想为(f)={f(x)全部倍式}，其中f(x)为首一多项式

- 包含乘法可逆元的理想只能是环本身
- 域的理想只能是集合{0}和域本身

商环何时是域？

- 设 R 是有单位元的交换环，I是 R 的理想，R/I 何时是域？
- 即任给 $a \in R \setminus I$, 存在$b \in R$，使得

$$(a+I)(b+I) = 1+I \quad 即\ 1-ab \in I$$

- 若理想J真包含I，取 在J 中但不在 I 中的元素 a，则$ab \in J$，$1=(1-ab)+ab \in J$，必须有 J=R。所以， I是极大理想（没有真包含 I 的真理想）
- 反过来，若 I是极大理想，取 $a \in R \setminus I$, 可验证

$$\{ab+u: b \in R, u \in I\}$$

是 R 的真包含 I 的理想，则这个理想只能是R，1必须属于其中，$1=ab+u$，$(a+I)(b+I) = 1+I$，R/I 的每个非零元有逆。

- 定理：设 R 是有单位元的交换环，I是 R 的理想，R/I 是域当且仅当I是极大理想

素理想

- 定义：设 R 是有单位元的交换环，I是 R 的理想，若任给 a,b∈R，ab ∈I时必有 a ∈I 或 b ∈I，则称I是素理想
- 定理：设 R 是有单位元的交换环，I是 R 的理想，R/I无零因子当且仅当I是素理想

- Z_m=Z/mZ 无零因子（是域）当且仅当 m为素数
- K[x]/(f)无零因子（是域）当且仅当 f(x)是不可约多项式

- GF(p)=Z_p=Z/pZ 和 GF(p^n)=Z_p [x]/(f) 是信息安全里常常工作的两类有限域，其中 f(x)是Z_p上n次首一不可约多项式

整环的分式化

- 相对于**由整数定义分数**，在一个**更大的范围**里就可以做**除法**了
- **条件：有单位元、无零因子、交换**

定理 4.4.2 对于每一个整环 R，一定存在一个域 Q，使得 R 是 Q 的子环。

证明：设 R 是整环。当 R 只包含零元时，定理显然成立。考虑至少含有两个元素的整环。记集合 $Q=\left\{\frac{b}{a}\mid a,b\in R,b\neq 0\right\}$。约定

（1）$a=\frac{a}{1}$，$\forall a\in R$，1 是 R 的单位元。

（2）$\frac{0}{a}=0$，$\forall a\in R$，0 是 R 的零元。

（3）$\frac{bc}{ac}=\frac{b}{a}$，$\forall a,b,c\in R,a\neq 0,c\neq 0$。

定义如下运算：

定理 4.4.2 证明（续）

（1）加法：$\frac{b}{a}+\frac{d}{c}=\frac{bc+ad}{ac}$，$a,b,c,d\in R,a\neq 0,c\neq 0$；

（2）乘法：$\frac{b}{a}\cdot\frac{d}{c}=\frac{bd}{ac}$，$a,b,c,d\in R,a\neq 0,c\neq 0$。

首先证明集合Q关于上面定义的加法构成加法交换群。由于 R 是有单位元的交换群，所以有：

（1）封闭性：显然。

（2）结合律：

$$\frac{b}{a}+\left(\frac{d}{c}+\frac{f}{e}\right)=\frac{b}{a}+\frac{ed+cf}{ce}=\frac{bce+aed+acf}{ace};$$

$$\left(\frac{b}{a}+\frac{d}{c}\right)+\frac{f}{e}=\frac{bc+ad}{ac}+\frac{f}{e}=\frac{bce+aed+acf}{ace}。$$

定理 4.4.2 证明（续）

（3）零元：为 R 中的零元。

$$\frac{b}{a}+0=\frac{b}{a}+\frac{0}{a}=\frac{b}{a};$$

$$0+\frac{b}{a}=\frac{0}{a}+\frac{b}{a}=\frac{b}{a}。$$

（4）负元：$\frac{b}{a}$的负元为$\frac{-b}{a}$

$$\frac{b}{a}+\frac{-b}{a}=\frac{0}{a}=0。$$

（5）交换律：

$$\frac{b}{a}+\frac{d}{c}=\frac{d}{c}+\frac{b}{a}。$$

因此，Q是加法交换群。

定理 4.4.2 证明（续）

对于乘法，显然满足封闭性、结合律及交换律。1 是Q的乘法单位元。对于Q中的非零元$\frac{b}{a}$，有

$$\frac{b}{a}\cdot\frac{a}{b}=1,$$

即$\frac{a}{b}$是$\frac{b}{a}$的乘法逆元。因此，Q对于乘法是乘法交换群。

乘法对加法的分配率也显然成立。

综上所述，Q是域，称为 R 的分式域。

容易验证R中的加法与乘法与Q中定义的加法和乘法一致。因此，R是Q的子环。