信息安全数学基础

4.3 子环、理想和商环

信息与软件工程学院

子环的定义

定义 4.3.1 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。

例 4.3.1 例 **4.1.1** 当中，$\mathbb{Z}$是$\mathbb{Q}$的子环，$\mathbb{Q}$是$\mathbb{R}$的子环，$\mathbb{R}$是$\mathbb{C}$的子环。$n\mathbb{Z}$是$\mathbb{Z}$的子环。

类似的，可以定义子整环，子除环，子域的概念。

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。易知，子环的交仍为子环。

子环的判定定理

定理4.3.1（1）设**R**是环，**S**是**R**的一个非空子集，**S**是**R**的子环当且仅当

$$a-b\in S, ab\in S, \forall a,b\in S。$$

（2）设**R**是除环，**S**是**R**的一个非空子集，**S**是**R**的子除环当且仅当

$$a-b\in S, ab^{-1}\in S, \forall a,b(\neq 0)\in S。$$

证明：根据子群的充要条件很容易验证定理中的两个充要条件。

例4.3.2 假设**R**是环，记集合$C(R)=\{a\in R|ab=ba,\forall b\in R\}$（同每一个元交换的元之集），称为环**R**的中心，则$C(R)$是R的子环。

证明：根据定理**4.3.1**可以直接验证。

子环的例子

- 例4.3.3 求模12的剩余类环$\mathbb{Z}_{12}$的所有子环。

解：由于$\mathbb{Z}_{12}$的加法群是一个循环群，故剩余类环$\mathbb{Z}_{12}$的子环关于加法是（$\mathbb{Z}_{12}$，＋）的子循环群，共有下面 6 个：

$$S_1 = \langle [1] \rangle = R;$$

$$S_2 = \langle [2] \rangle = \{[0],[2],[4],[6],[8],[10]\};$$

无单位元

$$S_3 = \langle [3] \rangle = \{[0],[3],[6],[9]\};$$

$$S_4 = \langle [4] \rangle = \{[0],[4],[8]\};$$

有单位元

无零因子

$$S_5 = \langle [6] \rangle = \{[0],[6]\};$$

$$S_6 = \langle [0] \rangle = \{[0]\}。$$

经检验，它们都是$\mathbb{Z}_{12}$的子环，从而$\mathbb{Z}_{12}$有上面的 6 个子环。

子环的性质

设S是R的子环，S与R的可以有不同的性质。

1. 对于交换律

（1）若**R**是交换环，则**S**也是交换环；

（2）若**S**是交换环，则**R**未必是交换环。

2. 对于零因子

（1）若**R**无零因子，则**S**也是无零因子；

（2）若**S**无零因子，则**R**未必无零因子。

3. 对于单位元

（1）若**R**有单位元，则**S**未必有单位元；

（2）若**S**有单位元，则**R**未必有单位元。

环同态

定义4.3.2 设$(R,+,\cdot)$和$(R',\oplus,\circ)$是环，$f:R\to R'$为映射。若f保持运算，即对任意$a,b\in R$有

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

则称f是环**R**到**R'**的一个同态。类似群中的定义，可定义环的单同态、满同态、同构的概念。

环同态性质

定理4.3.2 设$f:R\to R'$为环的满同态.

（1）若**0**是**R**中的零元，则**f(0)**是**R** ' 中的零元；

（2）$f(-a)=-f(a),\forall a\in R$;

（3）若R有单位元且**1**是R的单位元，则$f(1)$是R'的单位元；

（4）若S是R的子环，则$f(S)$是R'的子环；

（5）若S'是R'的子环，则$f^{-1}(S')=\{a\in R|f(a)\in S'\}$是$R$的子环。

证明： （1）对于任意元素$a\in R$，有

$$f(a)=f(a+0)=f(a)+f(0)=f(0)+f(a)$$

所以$f(0)$是**R** ' 中的零元。

定理 4.3.2 证明（续）

（2）对于任意元素$a \in R$，有

$$f(0) = f(a - a) = f(a + (-a)) = f(a) + f(-a)$$

所以$f(-a) = -f(a), \forall a \in R$。

（3）对于任意元素$a \in R$，有

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

所以$f(1)$是R'的单位元。

（4）和（5）可根据同态的定义和定理**4.3.1**进行验证。

同态的例子

例4.3.4 设$f:\mathbb{Z}\to\mathbb{Z}_n$为$f(x)=x(mod\ n)$，$x\in\mathbb{Z}_n$。证明：$f:\mathbb{Z}\to\mathbb{Z}_n$为满同态。

证明： 不难证明：f是$\mathbb{Z}$到$\mathbb{Z}_n$的满射。对于任意$x,y\in\mathbb{Z}$，有

$$f(x+y)=(x+y)(mod\ n)=x(mod\ n)+y(mod\ n)=f(x)+f(y)$$

$$f(xy)=(xy)(mod\ n)=x(mod\ n)y(mod\ n)=f(x)f(y)$$

所以$f:\mathbb{Z}\to\mathbb{Z}_n$为满同态。

例 4.3.5 设$R=\mathbb{Z}\times\mathbb{Z}=\{(a,b)|a,b\in\mathbb{Z}\}$，定义 **R** 的代数运算如下：

$$(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_2)，(a_1,b_1)(a_2,b_2)=(a_1a_2,b_1b_2)$$

则 **R** 显然作成一个环，称之为$\mathbb{Z}$与$\mathbb{Z}$的直积，记为$\mathbb{Z}^{(2)}$. 易知映射

$$\pi:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z};(a,b)\mapsto a,\forall a,b\in\mathbb{Z}$$

为满同态，但$\mathbb{Z}^{(2)}$中有零因子，而$\mathbb{Z}$无零因子。

商环

设R是一个环，A关于R中的加法构成R的一个子加群，则有商加群

$$R/A=\{x+A|x\in R\}$$

其加法为$(x+A)+(y+A)=(x+y)+A$。为了让R/A成为一个环，引入乘法：

$$(x+A)(y+A)=xy+A,\forall x,y\in R.$$

乘法是否有意义?

即若$\boldsymbol{x_1+A=x_2+A,y_1+A=y_2+A}$，是否有$\boldsymbol{x_1y_1+A=x_2y_2+A}$?

理想

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4.3.5 整数n的所有倍数之集$\langle n\rangle=\{nk|k\in \mathbb{Z}\}$构成整数环Z的一个理想。

商环（剩余类环）

设R是环，I是R的理想，在商群$R/I=\{x+I|x\in R\}$中定义乘法为：

$$(x+I)(y+I)=xy+I,\forall x,y\in R。$$

由于I是一个理想，所以上述定义的乘法有意义。

定理4.3.5 设R是环，I是R的理想，则R/I构成一个环，称为R关于理想I的商环（或称剩余类环）．其中元素$x+I$通常也记为$[x]$，称之为x所在的等价类或x模I的剩余类。

例4.3.6 任意$n\in$Z，$\langle n\rangle=\{nk|k\in \text{Z}\}$是整数环Z的一个理想，则有商环

$$\text{Z}/\langle n\rangle=\{k+<n>|\ k\in \text{Z}\}=\{[0],[1],\cdots,[n-1]\}$$

其中$[i]=\{i+kn|\ k\in \text{Z}\}$，$i=0,1,\ldots,n-1$。称之为模n的剩余类环，一般记为Z/nZ或$\text{Z}_n$

同态基本定理

定理 4.3.6 设R是环，对于R中的任意理想I，都存在自然的满同态

$$\pi: R \to R/I，\ a \to [a]，\forall a \in R.$$

证明：利用定义可以直接验证。

定理4.3.7 （同态基本定理）设φ是环R到R'的一个同态映射，则

（1）$ker\varphi = \{x \in R | \varphi(x) = 0\}$是R的理想，称$ker\varphi$为同态$\varphi$的核；

（2）$R/ker\varphi \cong \varphi(R)$。

证明：类似于群同态基本定理可以证明。

感 谢 聆 听！

xynie@uestc.edu.cn