第十八章　环与域

- 环的定义及其性质
  - 环的定义
  - 环的性质
  - 特殊的环
  - 有限域
- 子环、理想、商环、环同态
  - 子环定义及判别
  - 理想、商环、环同态

环的定义

定义 设$<R, +, \cdot>$是代数系统，+和·是二元运算。

如果满足以下条件:

（1）$<R, +>$构成交换群

（2）$<R, \cdot>$构成半群

（3）运算·关于运算+满足分配律

则称$<R, +, \cdot>$是一个环。

环中的术语

- 通常称+运算为环中的加法， ·运算为环中的乘法.
- 环中加法单位元记作 **0**.
- 乘法单位元（如果存在）记作 **1**.
- 环中加法单位元0恰好是乘法的零元.
- 对任何元素 x，称 x 的加法逆元为负元，记作$-x$.
- 若 x 存在乘法逆元的话，则称之为逆元，记作x^{-1}.
- 符号：$0, 1, -x, x^{-1}, nx, x^n, x-y$

环的实例

(1) 整数集、有理数集、实数集和复数集关于普通的加法和乘法构成环，分别称为整数环Z，有理数环Q，实数环R和复数环C.

(2) n ($n\geq 2$)阶实矩阵的集合$M_n(R)$关于矩阵的加法和乘法构成环，称为n阶实矩阵环。

(3) 设$Z_n=\{0, 1, \ldots, n-1\}$，$\oplus$和$\otimes$分别表示模$n$的加法和乘法，则$<Z_n, \oplus, \otimes>$构成环，称为模$n$的整数环。

(4) 集合的幂集 $P(B)$关于集合的对称差运算和交运算构成环。

环的性质

1) $a0 = 0a = 0$

2) $(-a)b = a(-b) = -(ab)$

3) $(-a)(-b) = ab$

4) $a(b-c) = ab - ac,$

$(b-c)a = ba - ca$

5) $(\sum_{i=1}^{n} a_i)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$

6) $(na)b = a(nb) = n(ab)$

环中的运算

环中加法的交换律、结合律；

乘法的结合律；

乘法对加法的分配律.

例 在环中计算 $(a+b)^3$, $(a-b)^2$

解 $(a+b)^3 = (a+b)(a+b)(a+b)$

$= (a^2+ba+ab+b^2)(a+b)$

$= a^3+ba^2+aba+b^2a+a^2b+bab+ab^2+b^3$

$(a-b)^2 = (a-b)(a-b)=a^2-ba-ab+b^2$

注：在初等代数中的加法和乘法运算都是在实数域中进行，乘法可交换

特殊的环

- 交换环、含幺环
- 无零因子环 $ab=0 \Rightarrow a=0$或$b=0$
  - 实例：数环, Z_p为无零因子环当且仅当 p为素数.
  - 定理：R是环，R为无零因子环 $\Leftrightarrow$ R中乘法有消去律.
- 整环：无零因子、含幺、交换环
- 除环：$|R|>1$, $<R^*, \cdot>$ 构成群(R^*中每个元素都可逆)
- 域：$|R|>1$, 交换的除环或者R^*中每个元素都有逆元的整环
  - 实例：$H=\left\{\begin{pmatrix}\alpha & \beta \\ -\bar{\beta} & \bar{\alpha}\end{pmatrix} \middle| \alpha,\beta\in C\right\}$是除环，不是域。
  - p为素数时，Z_p是域

特殊的环

(1) 整数环Z、有理数环Q、实数环R、复数环C都是交换环、含幺环、无零因子环和整环，其中除Z之外都是域。

(2) 令$2Z=\{2n \mid n\in Z\}$，则$<2Z, +, \cdot>$构成交换环和无零因子环. 但不是含幺环和整环。

(3) 设$n\in Z$, $n\geq 2$, 则n阶实矩阵的集合$M_n(R)$关于矩阵加法和乘法构成环，它是含幺环，但不是交换环和无零因子环，也不是整环。

(4) $<Z_6, \oplus, \otimes>$构成环，它是交换环、含幺环，但不是无零因子环和整环。

例题

整环：无零因子、含幺、交换环

除环：$|R|>1$, $<R^*,\cdot>$ 构成群

域 $|R|>1$, 交换的除环或者R^*中每个元素都有逆元的整环

例 设p为素数，证明Z_p是域。

证(I): p为素数，$p\geq 2$，所以$|Z_p|\geq 2$。

易见Z_p关于模p乘法可交换，单位元是1，且对于任意的$i, j, k\in Z_p$，$i\neq 0$有

$$i\otimes j = i\otimes k \Rightarrow i\otimes(j-k)=0 \Rightarrow p|i(j-k) \Rightarrow p|j-k \Rightarrow j=k,$$

因此Z_p^*中消去律成立。

又Z_p^*关于乘法$\otimes$构成有限半群，且不含零元，故Z_p^*关于乘法$\otimes$构成群，从而Z_p是域。

定理6 设G是有限半群，且不含零元. 若G中消去律成立，则G是群.

例题

整环：无零因子、含幺、交换环

除环：$|R|>1$, $<R^*,\cdot>$ 构成群

域 $|R|>1$, 交换的除环或者R^*中每个元素都有逆元的整环

例 设p为素数，证明Z_p是域。

证(II): p为素数，$p\geq 2$，所以$|Z_p|\geq 2$。

易见Z_p关于模 p乘法可交换，单位元是1，且对于任意的$i, j\in Z_p$，$i\neq 0$有$i\otimes j=0 \Rightarrow p|ij \Rightarrow p|j \Rightarrow j=0$，所以$Z_p$中无零因子，$Z_p$为整环。

下面证明每个非零元素都有逆元。任取$i\in Z_p$, $i\neq 0$，令$i\otimes Z_p=\{i\otimes j|j\in Z_p\}$, 则 $i\otimes Z_p=Z_p$，否则必存在 $j, k\in Z_p$，使得$i\otimes j=i\otimes k$，于是$i\otimes(j-k)=0 \Rightarrow p|i(j-k) \Rightarrow p|j-k \Rightarrow j=k$，矛盾。由于$1\in Z_p$，故存在 $j\in Z_p$，使得 $i\otimes j=1$。由于$\otimes$运算的交换性可知 j 就是i的逆元。从而证明了Z_p是域。

例题

Chapter17.6:

例5 G为Abel群，$|G| = n$, 素数$p|n$, 则G中有p阶元.

推论 pq (p, q为互异素数) 阶Abel群必为循环群。

例 p, q为不等的素数，证明无pq阶的整环。

证：假设R为pq阶的整环，则$\langle R, +\rangle$为pq阶的Abel群。

存在p阶元a，q阶元b. 所以$|a+b|=pq$,

$$|a| = n, |b| = m, ab = ba \Rightarrow |ab| \mid [n, m],$$

若$(n, m) = 1$, $|ab| = nm$

于是$\langle R, +\rangle$为循环群,

令$c=a+b$为生成元,

于是$R=\{0, c, 2c, \ldots, (pq-1)c\}$

取$x=pc$, $y=qc$, 则$xy=(pc)(qc) = pqc^2 = 0$

故x, y为零因子。矛盾！

有限域

- 定义：F为域，$|F|$有限
- 实例：Z_p，p为素数

  Z_p为整环

  $<Z_p-\{0\}, \cdot>$有限半群，无零元，适合消去律

  $<Z_p-\{0\}, \cdot>$构成Abel群
- 结论：有限的整环都是域
- 有限域的特征
  - F为有限域，1在$<F, +>$中的阶为域F的特征.
  - 有限域的特征为素数；Z_p的特征为p.

域上的多项式环

- 设F是域，令
  $F[x]=\{a_0+a_1x+a_2x^2+\ldots+a_nx^n \mid a_i \in F, n \in N\}$,
  则$F[x]$关于 F 上多项式的加法和乘法构成一个环，称为域 F 上的多项式环。若F为有限域，则称
  $F[x]$ 为有限域 F 上的多项式环。

  习题十七第60题：设f 是群G的满自同态，若G只有有限个子群，证明 f 是G的自同构。一般地，群的自同态满射不一定是自同构。

  例如，取$G=R[x]$，$R[x]$是实数域上的多项式环。G关于多项式的加法构成一个Abel群。映射 f 将每个多项式$g(x)$映成它的导数 $g'(x)$ ，如$2x$映成2，2映成0. 易证 f 是自同态满射，但不是一一映射，所以不是同构。

有限域的性质

设F为有限域，则存在素数p使得$|F|=p^n$.

证明思想:

$A=\langle 1\rangle=\{0, 1, \ldots, p-1\}$

$Ax_1=\{0, x_1, 2x_1, \ldots, (p-1)x_1\}$，$x_1\in F^*$，$|Ax_1|=p$

若$F=Ax_1$则结束;

否则$\exists x_2\in F-Ax_1, x_2\neq 0, Ax_1+Ax_2=\{a_1x_1+a_2x_2 \mid a_1,a_2\in A\}$

可以证明Ax_1+Ax_2中的元素两两不同，因此

$|Ax_1+Ax_2|=p^2$;

照此处理，$|Ax_1+Ax_2+Ax_3|=p^3$, 直到穷尽所有的元素。

二元域与纠错码

- $\boldsymbol{F}=\{\mathbf{0},\mathbf{1}\}$是一个域，称为二元域，记为$\boldsymbol{F}_{2}$.

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

- 域$\boldsymbol{F}_{2}$上的矩阵运算和多项式运算，如:

$$\begin{pmatrix}\mathbf{1} & \mathbf{1}\\ \mathbf{1} & \mathbf{1}\end{pmatrix}\begin{pmatrix}\mathbf{1} & \mathbf{1}\\ \mathbf{1} & \mathbf{0}\end{pmatrix}=\begin{pmatrix}\mathbf{0} & \mathbf{1}\\ \mathbf{0} & \mathbf{1}\end{pmatrix}$$

$$(\boldsymbol{x}^{2}+\mathbf{1})(\boldsymbol{x}^{3}+\boldsymbol{x}+\mathbf{1})=\boldsymbol{x}^{5}+\boldsymbol{x}^{2}+\boldsymbol{x}+\mathbf{1}$$

纠错举例

信息传输，常用一组$0,1$信号来代表一个信息，每一个$0,1$序列就是F_2上的向量——称为码字。

一个简单的纠错方案：有纠一个错的能力

作F_2上4×15矩阵

$$H=\begin{bmatrix}0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\end{bmatrix}$$

将十进制数$1,2,\ldots,15$变成四位二进制数后，把它们看成 F_2 上的4元向量，依次排在第1列，第2列，…，第15列，就得到上面的矩阵$\boldsymbol{H}$。

纠错举例

以$\boldsymbol{H}$为系数矩阵作$\boldsymbol{F_2}$上的齐次线性方程组

$$\boldsymbol{H_{4\times 15}X_{15\times 1}=0} \qquad (*)$$

取方程组$(*)$的解集合，它是$\boldsymbol{F_2}$上$\mathbf{15}$元向量的一个集合，用以作为承载各个信息的$\mathbf{0,1}$向量的集合，其中的每一个向量都是一个码字。任一个码字

$$\boldsymbol{\alpha}=\begin{pmatrix}\boldsymbol{a_1}\\ \boldsymbol{a_2}\\ \vdots\\ \boldsymbol{a_{15}}\end{pmatrix},\ \boldsymbol{a_i}\in\boldsymbol{F_2}$$

是$(*)$的解，即$\boldsymbol{H\alpha=0}$.

纠错举例

假设它在传输时受到干扰，有一位发生改变，设在第i位发生改变，即第i位由$\mathbf{0}$变$\mathbf{1}$或由$\mathbf{1}$变$\mathbf{0}$. 由F_2的运算，这相当于第i位加上$\mathbf{1}$. 令

$$\boldsymbol{e}_i = \begin{pmatrix} \mathbf{0} \\ \vdots \\ \mathbf{0} \\ \mathbf{1} \\ \mathbf{0} \\ \vdots \\ \mathbf{0} \end{pmatrix} \begin{matrix} \\ \\ \\ \dots\text{第}i\text{位} \\ \\ \\ \\ \end{matrix}$$

纠错举例

则接收到的向量为$\boldsymbol{\beta}=\boldsymbol{\alpha}+\boldsymbol{e}_i$，用$\boldsymbol{H}$乘它，

$\boldsymbol{H\beta}=\boldsymbol{H\alpha}+\boldsymbol{He}_i=\boldsymbol{0}+\boldsymbol{He}_i=\boldsymbol{H}$的第$\boldsymbol{i}$列的列向量。

因此，对接收到的向量$\boldsymbol{\beta}$，若$\boldsymbol{\beta}$是$\boldsymbol{H}$的第$\boldsymbol{i}$列的列向量，则$\boldsymbol{\beta}$出错在第$\boldsymbol{i}$位，只要将$\boldsymbol{\beta}$再加上$\boldsymbol{e}_i$就恢复了发出和码字。

纠错举例

例如：解方程组$\boldsymbol{H}_{4\times15}\boldsymbol{X}_{15\times1}=\mathbf{0}$得一般解

$$\begin{cases} x_1 = x_3 + x_5 + x_7 + x_9 + x_{11} + x_{13} + x_{15} \\ x_2 = x_3 + x_6 + x_7 + x_{10} + x_{11} + x_{14} + x_{15} \\ x_4 = x_5 + x_6 + x_7 + x_{12} + x_{13} + x_{14} + x_{15} \\ x_8 = x_9 + x_{10} + x_{11} + x_{12} + x_{13} + x_{14} + x_{15} \end{cases}$$

$\boldsymbol{X}=(1,1,1,1,1,1,1,1,1,1,1,1,1,1,1)^T$是其中一个解。

纠错举例

若将$\boldsymbol{X}$的第6位变为0得

$\boldsymbol{Y} = (\mathbf{1,1,1,1,1,0,1,1,1,1,1,1,1,1,1})^{\boldsymbol{T}}.$

假设我们并不知道它是由$\boldsymbol{X}$改变第6位而得，但我们只知道它与方程组$\boldsymbol{H}_{\mathbf{4\times15}}\boldsymbol{X}_{\mathbf{15\times1}} = \mathbf{0}$的一个解最多有一位不同。

因$\boldsymbol{HY} = \begin{pmatrix} \mathbf{0} \\ \mathbf{1} \\ \mathbf{1} \\ \mathbf{0} \end{pmatrix}$与$\boldsymbol{H}$的第6列相同，故$\boldsymbol{Y}$与原解在第6位差了1，将$\boldsymbol{Y}$在第6位加1就得原解了。

18.2 子环、理想、商环、环同态

- 子环

  子环定义

  子环判别
- 理想
- 商环
- 环同态及其性质

子环定义及其判别

- 定义：非空子集关于环中运算+, · 构成环
- 实例：$n\mathbf{Z}$是<Z, +, ·>的子环
- 子环就是子代数，平凡子环存在
- 判别：子加群判别+半群判别
- 子整环、子除环、子域

子环判定定理

定理 设R是环，S是R的非空子集，若

(1) $\forall a, b \in S$，$a-b \in S$

(2) $\forall a, b \in S$，$ab \in S$

则S是R的子环。

证：由(1)知S关于环R中的加法构成群。

由(2)知S关于环R中的乘法构成半群。

显然R中关于加法的交换律，以及乘法对加法的分配律在S中也是成立的。因此S是R的子环。

注：根据子群和子半群的判定定理可以直接得到子环的判定定理。

实例

(1) 考虑整数环<Z, +, ·>，对于任意给定的自然数n,

$nZ=\{nk|k\in Z\}$是Z的非空子集，且$\forall nk_1, nk_2\in nZ$有

$$nk_1-nk_2=n(k_1-k_2)\in nZ$$

$$nk_1 \cdot nk_2=n(k_1nk_2)\in nZ$$

根据判定定理, nZ是整数环Z的子环。

(2) 考虑模6整数环<Z_6, $\oplus$, $\otimes$>，不难验证：

{0}, {0,3}, {0,2,4}, Z_6是它的子环。

其中{0}和Z_6是平凡的，其余的是非平凡的真子环。

理想

- 理想：D是环$<R, +, \cdot>$的非空子集，满足

  (1) $<D, +>$ 是$<R, +>$的子群

  (2) $\forall r\in R, rD\subseteq D, Dr\subseteq D$

- 例：$F[x]$为数域F上的多项式环，

  $I=\{a_1x+a_2x^2+\cdots+a_nx^n | a_i\in F, n\in N\}$,

  即I是由所有常数项为0的多项式构成的集合，则I是$F[x]$的理想。

理想

- 说明：
  - 左理想 (只满足$rD \subseteq D$) 与右理想

    $D = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} | a, b \in R \right\}$为$M_2(R)$的左理想，但不是右理想。

  - 理想是R的子环，但是子环不一定是理想。

    <Z, +, ·>是<R, +, ·>的子环，但不是理想。

- 平凡理想：{0}, R自身。

例题

域: $|R|>1$, 交换的除环(即$<R^*, \cdot>$ 构成群)或者R^*中每个元素都有逆元的整环

例1 R为交换环，$1\in R$, 且$1\neq 0$, 则R为域当且仅当R只含有平凡理想。

证 $(\Rightarrow)$ 设D为理想，$D\neq\{0\}$，$\exists x\in D$, $x\neq 0 \Rightarrow x^{-1}\in R \Rightarrow$
$1= x^{-1}x\in D \Rightarrow \forall r\in R$, $r= r\cdot 1\in D$, 故$R=D$.

$(\Leftarrow)$ $\forall x\neq 0$, $x\in R$, 令$Rx=\{rx|r\in R\}$. 下证Rx为理想.

$\forall r_1x, r_2x \in Rx$，有$r_1x-r_2x = (r_1-r_2)x\in Rx$，因此$<Rx, +>$构成$<R, +>$的子群。

$\forall r_1x\in Rx, r_2\in R$，有$(r_1x)r_2=(r_1r_2)x\in Rx$, $r_2(r_1x)=(r_2r_1)x \in Rx$，故$Rx$是理想。

因此$Rx=R$, 存在y使得$yx=1$，因为乘法可交换，故x有逆元。$<R^*, \cdot>$构成群，因此R是域。

期中考试情况说明

- 参考人数：**315**
- **85**分以上**: 111, 35.2%**
- 均分：**76.93**
- 不及格**: 36, 11.4%**

期中考试情况说明

一　（每空3分，共66分）填空题。

1. 设$*$为有理数域$\mathbb{Q}$上的二元运算：对任意$x, y \in \mathbb{Q}$有$x * y = x + y + xy$. 则关于$*$运算的单位元是____，零元是___，可逆元存在的条件及逆元是________。
2. 群$\langle \mathbb{Z}_4, \oplus \rangle$上的自同态$f: x \longmapsto 2x \pmod 4$导出的同余关系是______.
3. 设$V_1 = \langle M_2(\mathbb{R}), + \rangle$，$V_2 = \langle M_2(\mathbb{R}), \cdot \rangle$，其中$M_2(\mathbb{R})$为2阶实矩阵集，$+$，$\cdot$分别为矩阵加法和乘法。若$V_1 \times V_2$中的运算记为$\odot$，则$\left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle \odot \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle =$__________.
4. 写出半群$\langle \mathbb{Z}_4, \otimes \rangle$的所有子半群（写出载体即可）：___________.
5. 关于普通乘法$\cdot$，半群$\langle \mathbb{Z}, \cdot \rangle$中由$\{4, 8\}$生成的子半群的载体是_$\{4,8,16,32,\ldots\}$___.
6. 考虑群$\langle M_2(\mathbb{R}), + \rangle$中的下列子集：（1）全体对称矩阵；（2）全体上三角矩阵；（3）全体行列式非负的矩阵；（4）全体行列式为0的矩阵。其中_____________构成子群。
7. 设$G = \langle a \rangle$是14阶循环群，则G的全部生成元是____，全部子群是___.
8. 设$\langle a^2 \rangle$是无限循环群，则其全部生成元是________，全部子群是__$\langle a^{2i} \rangle, i = 0,1,2,\ldots$

期中考试情况说明

9. 在S_7中，阶为15的元素个数为______.

10. 设H是S_3中由(23)生成的子群，则H在S_3中的全部右陪集为__，S_3的全部共轭类为___.

11. 令$GL_2(\mathbb{Z})$表示2阶整数矩阵中行列式等于1或−1的所有矩阵组成的集合，$GL_2(\mathbb{Z})$关于矩阵乘法构成群。该群的中心为_______，$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$的正规化子为_____.

12. 群$\langle \mathbb{Z}, + \rangle$的自同构群为_2阶循环群或$\mathbb{Z}_2$或者2个元素的群（写出与其同构的群也可）。

13. 设变换群$G = \{f_{(a,b)} | f_{(a,b)}(x) = ax + b, a, b \in \mathbb{Q}, a \neq 0, \forall x \in \mathbb{Q}\}$，易知$N = \{f_{(1,b)} | b \in \mathbb{Q}\}$是其正规子群。则商群$G/N$的载体为_$\{Nf_{(a,0)} | a \in \mathbb{Q}, a \neq 0\}$_.

14. 设a是含幺环R的幂零元，即存在某个正整数n使得$a^n = 0$，则$(1-a)^{-1} =$_____.

15. 设F是由4个元素构成的域，则F的特征可能是___.

16. 模14的剩余类环$\mathbb{Z}_{14}$中的全部零因子为______.

期中考试情况说明

二、（17分）设f是群G到群H的同态，证明：

(1) $\mathrm{ker}f \trianglelefteq G$;　非空1分，子群1分，正规性3分

(2) $G/\mathrm{ker}f \cong f(G)$.　映射+良定义，单，满，同态，各3分

三、（17分）**定义**：设R是交换环，$a,b \in R$，若存在$c \in R$，使得$b = ac$，则称**a<u>整除</u>b**，记作$a|b$.若对任意$x \in R$，均有$a|x$，则称a为R的一个<u>单位</u>。

（1）请根据上述定义，求高斯整环$\mathbb{Z}[i] = \{a + bi|a,b \in \mathbb{Z}\}$的所有单位。

（2）设R是含幺交换环，$a \in R$.求证：a是单位当且仅当a在R中可逆。

（1）$\mathbb{Z}[i]$有单位元1，设$a + bi \in \mathbb{Z}[i]$是单位，则存在$c + di \in \mathbb{Z}[i]$使得$(a + bi)(c + di) = 1$. (3分)

于是$ac - bd = 1,\ ad + bc = 0$. (2分)讨论知，$1,-1,i,-i$是$\mathbb{Z}[i]$的所有单位。(4分)

（2） 4分x2

商环

定义 D为R的理想，$\forall x\in R$, 定义

$$\overline{x} = D + x = \{d + x \mid d \in D\}$$

$$R/D = \{\overline{x} \mid x \in R\}$$

$$\overline{x} + \overline{y} = \overline{x + y}, \overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

<R/D, +, ·> 构成环，称为R关于D的商环。

注：良定义验证

$$\overline{x} = \overline{x'}, \overline{y} = \overline{y'} \Rightarrow x' = d_1 + x, y' = d_2 + y$$

$$\overline{x'} \cdot \overline{y'} = \overline{x' \cdot y'} = \overline{(d_1 + x)(d_2 + y)}$$

$$= \overline{d_1 d_2 + x d_2 + d_1 y + xy} = \overline{d + xy} = \overline{xy} = \overline{x} \cdot \overline{y}$$

商环的实例

实例：$<Z_6, \oplus, \otimes>$

理想 $\{0\}, \{0, 2, 4\}, \{0, 3\}, Z_6$

商环 $Z_6/\{0\}=\{\{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}\}$,

$Z_6/Z_6=\{Z_6\}$

$Z_6/\{0, 3\}=\{\{0,3\}, \{1,4\}, \{2,5\}\}$,

$Z_6/\{0, 2, 4\}=\{\{0,2,4\}, \{1,3,5\}\}$

环同态

- 环同态 $f: R_1 \to R_2$

  $$f(x+y)=f(x)+f(y)$$

  $$f(xy)=f(x)f(y)$$

- 同态核：$\mathrm{ker}f = \{x \in R_1 \mid f(x)=0\}$
- 实例
  - f_c: Z→Z, $f_c(x)=cx$，c=0, 1

    $\mathrm{ker}f_0$=Z; $\mathrm{ker}f_c$={0}，$c \neq 0$
  - φ: Z→$\mathrm{Z_n}$，φ(x)=x (mod n)

    kerφ=nZ

环同态的性质

1. $f(0)=0$, $f(-x)=-f(x)$, $f(x^{-1}) = f(x)^{-1}$
2. (1) S是R_1的子环，则$f(S)$是R_2的子环

   (2) f 满，T是R_2的子环，则$f^{-1}(T)$是R_1的子环

   (3) D是R_1的理想，则$f(D)$是$f(R_1)$的理想

   (4) f 满，I是R_2的理想，则$f^{-1}(I)$是R_1的理想
3. $\mathrm{ker}f=\{x\in R_1 | f(x)=0\}$; $\mathrm{ker}f$是R_1的理想
4. 同态基本定理

   环R的任何商环R/D是R的同态像

   若$R \sim R'$, 则 $R' \cong R/\mathrm{ker}f$

性质的证明

证：2. (2) 证 $f^{-1}(T)$是 R_1的子环.

$f^{-1}(T)$非空，$\forall x, y\in f^{-1}(T)$，由 f 满知，$\exists a, b\in T$ 使得 $f(x)=a, f(y)=b$, 于是

$$f(x-y)=f(x)-f(y)=a-b\in T,\ x-y\in f^{-1}(T)$$

$$f(xy)=f(x)f(y)=ab\in T,\ xy\in f^{-1}(T)$$

(3) 证 $f(D)$是理想.

$f(D)$是$f(R_1)$的子加群。

$\forall x\in f(D),\ r\in f(R_1), \exists a\in D$, 使得$f(a)=x$, $\exists b\in R_1$, $f(b)=r$, 使得$xr=f(a)f(b)=f(ab)\in f(D)$. 同理，$rx\in f(D)$.

性质证明(续)

3． $\ker f = \{x \mid x \in R_1, f(x) = 0\}$

证明：$\ker f$是R_1的理想

证 $\ker f$ 是$\langle R_1, +\rangle$的正规子群.

$\forall x \in \ker f,\ r \in R_1$, 有

$f(xr) = f(x)f(r) = 0f(r) = 0$

故 $xr \in \ker f$.

同理，$rx \in \ker f$.