信息安全数学基础

韩　琦

计算机科学与技术学院

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

作业

- 证明$(S_n, \cdot, 1)$为群。
- 设$(Z_2^m, \oplus, 0)$中$Z_2^m = \{(a_1 a_2 \cdots a_m) | a_i \in \{0, 1\}\}$，$Z_2^m$中运算$\oplus$为两向量逐位在$Z_2$中作运算$\oplus_2$(也称作逐位异或)，0 为$m$维全零向量。证明$(Z_2^m, \oplus, 0)$为群。
- 设$\sigma = \begin{pmatrix} 12345678 \\ 73154682 \end{pmatrix}$，求$\sigma$在$S_8$中的逆$\sigma^{-1}$。

Detailed overview

环的定义

定义（环）

设五元组$(R,+,\cdot,0,1)$中，R为集合，$+$与$\cdot$为集R上二元运算，0与1为R中元。若$(R,+,\cdot,0,1)$满足：

- $R1$(加法交换群)：$(R,+,0)$是交换群
- $R2$(乘法半群)：$(R,\cdot,1)$是有单位元的半群
- $R3$(乘法对加法的分配律)：

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

则称$(R,+,\cdot,0,1)$为**环**，简称环R。

环的定义

定义（环）

设五元组$(R,+,\cdot,0,1)$中，R为集合，$+$与$\cdot$为集R上二元运算，0与1为R中元。若$(R,+,\cdot,0,1)$满足：

- $R1$(加法交换群)：$(R,+,0)$是交换群
- $R2$(乘法半群)：$(R,\cdot,1)$是有单位元的半群
- $R3$(乘法对加法的分配律)：

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

则称$(R,+,\cdot,0,1)$为**环**，简称环R。

环的定义

定义（环）

设五元组$(R,+,\cdot,0,1)$中，R为集合，$+$与$\cdot$为集R上二元运算，0与1为R中元。若$(R,+,\cdot,0,1)$满足：

- $R1$(加法交换群)：$(R,+,0)$是交换群
- $R2$(乘法半群)：$(R,\cdot,1)$是有单位元的半群
- $R3$(乘法对加法的分配律)：

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

则称$(R,+,\cdot,0,1)$为**环**，简称环R。

环的定义

定义（环）

设五元组$(R,+,\cdot,0,1)$中，R为集合，$+$与$\cdot$为集R上二元运算，0与1为R中元。若$(R,+,\cdot,0,1)$满足：

- $R1$(加法交换群)：$(R,+,0)$是交换群
- $R2$(乘法半群)：$(R,\cdot,1)$是有单位元的半群
- $R3$(乘法对加法的分配律)：

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

则称$(R,+,\cdot,0,1)$为**环**，简称环R。

环的定义(续)

- $+$与$\cdot$称为环R的**加法与乘法**；
- 1称为环的**单位元**；
- 0称为环的**零元**；
- 若$a'' \in R$使$a'' \cdot a = 1$，则称a''为a的**逆元**，写为a^{-1}；
- 若$a' \in R$使$a' + a = 0$，则称a'为a的**负元**，写为$-a$；
- $(R, +, 0)$称为环R的**加法群**；
- $(R, \cdot, 1)$称为环R的**乘法半群**。

环的定义(续)

- $+$与$\cdot$称为环R的**加法与乘法**；
- 1称为环的**单位元**；
- 0称为环的**零元**；
- 若$a'' \in R$使$a'' \cdot a = 1$，则称a”为a的**逆元**，写为a^{-1}；
- 若$a' \in R$使$a' + a = 0$，则称a'为a的**负元**，写为$-a$；
- $(R, +, 0)$称为环R的**加法群**；
- $(R, \cdot, 1)$称为环R的**乘法半群**。

环的定义(续)

- $+$与$\cdot$称为环R的**加法与乘法**；
- 1称为环的**单位元**；
- 0称为环的**零元**；
- 若$a'' \in R$使$a'' \cdot a = 1$，则称a''为a的**逆元**，写为a^{-1}；
- 若$a' \in R$使$a' + a = 0$，则称a'为a的**负元**，写为$-a$；
- $(R, +, 0)$称为环R的**加法群**；
- $(R, \cdot, 1)$称为环R的**乘法半群**。

环的定义(续)

- $+$与$\cdot$称为环R的**加法与乘法**；
- 1称为环的**单位元**；
- 0称为环的**零元**；
- 若$a'' \in R$使$a'' \cdot a = 1$，则称a"为a的**逆元**，写为a^{-1}；
- 若$a' \in R$使$a' + a = 0$，则称a'为a的**负元**，写为$-a$；
- $(R, +, 0)$称为环R的**加法群**；
- $(R, \cdot, 1)$称为环R的**乘法半群**。

环的定义(续)

- $+$与$\cdot$称为环R的**加法与乘法**；
- 1称为环的**单位元**；
- 0称为环的**零元**；
- 若$a'' \in R$使$a'' \cdot a = 1$，则称a"为a的**逆元**，写为a^{-1}；
- 若$a' \in R$使$a' + a = 0$，则称a'为a的**负元**，写为$-a$；
- $(R, +, 0)$称为环R的**加法群**；
- $(R, \cdot, 1)$称为环R的**乘法半群**。

环的定义(续)

- $+$与$\cdot$称为环R的**加法与乘法**；
- 1称为环的**单位元**；
- 0称为环的**零元**；
- 若$a'' \in R$使$a'' \cdot a = 1$，则称a"为a的**逆元**，写为a^{-1}；
- 若$a' \in R$使$a' + a = 0$，则称a'为a的**负元**，写为$-a$；
- $(R, +, 0)$称为环R的**加法群**；
- $(R, \cdot, 1)$称为环R的**乘法半群**。

环的定义(续)

- $+$与$\cdot$称为环R的**加法与乘法**；
- 1称为环的**单位元**；
- 0称为环的**零元**；
- 若$a'' \in R$使$a'' \cdot a = 1$，则称a”为a的**逆元**，写为a^{-1}；
- 若$a' \in R$使$a' + a = 0$，则称a'为a的**负元**，写为$-a$；
- $(R, +, 0)$称为环R的**加法群**；
- $(R, \cdot, 1)$称为环R的**乘法半群**。

交换环、体、域

定义（交换环）

若环$(R, +, \cdot, 0, 1)$满足

- *R4(乘法半群交换)：$(R, \cdot, 1)$为交换半群。*

则称R为交换环。

定义（体，域）

若环$(R, +, \cdot, 0, 1)$满足

- *R5：$(R^*, \cdot, 1)$为群，这里$R^* = R - \{0\}$，则称R为体*
- *R6：$(R^*, \cdot, 1)$为交换群，则称R为域*

交换环、体、域

定义（交换环）

若环$(R, +, \cdot, 0, 1)$满足

- *R4(乘法半群交换)：$(R, \cdot, 1)$为交换半群。*

*则称R为**交换环**。*

定义（体，域）

若环$(R, +, \cdot, 0, 1)$满足

- *R5：$(R^*, \cdot, 1)$为群，这里$R^* = R - \{0\}$，则称R为**体***
- *R6：$(R^*, \cdot, 1)$为交换群，则称R为**域***

交换环、体、域

定义（交换环）

若环$(R,+,\cdot,0,1)$满足

- *R4(乘法半群交换)：$(R,\cdot,1)$为交换半群。*

*则称R为**交换环**。*

定义（体，域）

若环$(R,+,\cdot,0,1)$满足

- *R5：$(R^*,\cdot,1)$为群，这里$R^*=R-\{0\}$，则称R为体*
- *R6：$(R^*,\cdot,1)$为交换群，则称R为域*

交换环、体、域

定义（交换环）

若环$(R, +, \cdot, 0, 1)$满足

- *R4(乘法半群交换)：$(R, \cdot, 1)$为交换半群。*

*则称R为**交换环**。*

定义（体，域）

若环$(R, +, \cdot, 0, 1)$满足

- *R5：$(R^*, \cdot, 1)$为群，这里$R^* = R - \{0\}$，则称R为**体***
- *R6：$(R^*, \cdot, 1)$为交换群，则称R为域*

交换环、体、域

定义（交换环）

若环$(R, +, \cdot, 0, 1)$满足

- *R4(乘法半群交换)：$(R, \cdot, 1)$为交换半群。*

*则称R为**交换环**。*

定义（体，域）

若环$(R, +, \cdot, 0, 1)$满足

- *R5：$(R^*, \cdot, 1)$为群，这里$R^* = R - \{0\}$，则称R为**体***
- *R6：$(R^*, \cdot, 1)$为交换群，则称R为**域***

举例

例

整数集Z在整数$+$与整数$\cdot$下为交换环，称为整数环$(Z,+,\cdot,0,1)$，简记为环Z。

证明

- $(Z,+,0)$是交换群
- $(Z,\cdot,1)$是有单位元的交换半群
- 乘法对加法的分配律：

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

举例

例

整数集Z在整数$+$与整数$\cdot$下为交换环，称为整数环$(Z,+,\cdot,0,1)$，简记为环Z。

证明

- $(Z,+,0)$是交换群
- $(Z,\cdot,1)$是有单位元的交换半群
- 乘法对加法的分配律：

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

举例

例

有理数集Q在有理数加法$+$与有理数乘法$\cdot$下为域，称为有理数域$(Q,+,\cdot,0,1)$，简记为域Q。

证明

- $(Q,+,0)$是交换群
- $(Q,\cdot,1)$是有单位元的半群
- 乘法对加法的分配律：

  $a\cdot(b+c)=a\cdot b+a\cdot c,\ (b+c)\cdot a=b\cdot a+c\cdot a$
- $(Q^*,\cdot,1)$是交换群

举例

例

有理数集Q在有理数加法$+$与有理数乘法$\cdot$下为域，称为有理数域$(Q,+,\cdot,0,1)$，简记为域Q。

证明

- $(Q,+,0)$是交换群
- $(Q,\cdot,1)$是有单位元的半群
- 乘法对加法的分配律：

  $a\cdot(b+c)=a\cdot b+a\cdot c$，$(b+c)\cdot a=b\cdot a+c\cdot a$
- $(Q^*,\cdot,1)$是交换群

整环

定义（零因子）

设$a, b \in R$，且$a \neq 0, b \neq 0$，若$a \cdot b = 0$，则称a与b为环R中的**零因子**。

定义（整环）

环R若无零因子，则称R为无零因子环。交换的无零因子环称为**整环**。

例

在环Z_{26}中13和2是零因子。

整环

定义（零因子）

设$a, b \in R$，且$a \neq 0, b \neq 0$，若$a \cdot b = 0$，则称a与b为环R中的**零因子**。

定义（整环）

环R若无零因子，则称R为无零因子环。交换的无零因子环称为**整环**。

例

在环Z_{26}中13和2是零因子。

整环

定义（零因子）

设$a, b \in R$，且$a \neq 0, b \neq 0$，若$a \cdot b = 0$，则称a与b为环R中的**零因子**。

定义（整环）

环R若无零因子，则称R为无零因子环。交换的无零因子环称为**整环**。

例

在环Z_{26}中13和2是零因子。

理想、主理想

定义（理想）

*若I为环R的加法群的子群，且对任$a \in I$和任$r \in R$有$ar \in I$和$ra \in I$，则称I为环R的**理想**。*

定义（主理想）

*若I为交换环R的理想。若$I = \{ra | r \in R\}$，则称I为环R的**主理想**，并记为$I = (a)$。*

例

在整数环$(Z, +, \cdot, 0, 1)$中，令$nZ = \{0, \pm n, \pm 2n, \cdots\}$，则$nZ$为环$Z$的理想，且$nZ$为环$Z$的主理想，此时$nZ = (n)$。

理想、主理想

定义（理想）

*若I为环R的加法群的子群，且对任$a \in I$和任$r \in R$有$ar \in I$和$ra \in I$，则称I为环R的**理想**。*

定义（主理想）

*若I为交换环R的理想。若$I = \{ra | r \in R\}$，则称I为环R的**主理想**，并记为$I = (a)$。*

例

在整数环$(Z, +, \cdot, 0, 1)$中，令$nZ = \{0, \pm n, \pm 2n, \cdots\}$，则$nZ$为环$Z$的理想，且$nZ$为环$Z$的主理想，此时$nZ = (n)$。

理想、主理想

定义（理想）

*若I为环R的加法群的子群，且对任$a \in I$和任$r \in R$有$ar \in I$和$ra \in I$，则称I为环R的**理想**。*

定义（主理想）

*若I为交换环R的理想。若$I = \{ra | r \in R\}$，则称I为环R的**主理想**，并记为$I = (a)$。*

例

在整数环$(Z, +, \cdot, 0, 1)$中，令$nZ = \{0, \pm n, \pm 2n, \cdots\}$，则$nZ$为环$Z$的理想，且$nZ$为环$Z$的主理想，此时$nZ = (n)$。

多项式环

定义（环上的多项式）

设x为文字，R为交换环，$x \notin R$。定义R上多项式集

$$R[x] = \{f(x) = \sum_{i=0}^{n} a_i x^i | n \in Z, a_i \in R\}$$

- $f(x) = \sum_{i=0}^{n} a_i x^i$称为交换环$R$上关于文字$x$的多项式；
- $a_i x^i$称为$f(x)$的第i次项，a_i为$f(x)$的第i次项系数；$a_0 x^0$ 写为a_0。
- 当$a_n \neq 0$时，$a_n x^n$称为$f(x)$的首项，n称为$f(x)$的次数，记为$\partial f(x) = n$；特别当$a_n = 1$时，称$f(x)$为首1多项式；
- 称$0 \in R$为$R[x]$中的零多项式，并约定$\partial(0) = -\infty$(负无穷大)，并约定任意非负整数n，$n + (-\infty) = -\infty$。

加法与乘法

下面定义$R[x]$中的$+$与$\cdot$：
设$f(x)=\sum_{i=0}^{n}a_ix^i$，$g(x)=\sum_{j=0}^{m}b_jx^j$，定义

$$f(x)+g(x)=\sum_{i=0}^{max\{m,n\}}(a_i+b_i)x^i$$

$$f(x)\cdot g(x)=\sum_{k=0}^{m+n}(\sum_{i+j=k}a_ib_j)x^k$$

定义

设R为交换环，五元组$(R[x],+,\cdot,0,1)$称为R上的多项式环，其中$+$与$\cdot$如上述定义。

加法与乘法

下面定义$R[x]$中的$+$与$\cdot$：
设$f(x)=\sum_{i=0}^{n}a_ix^i$，$g(x)=\sum_{j=0}^{m}b_jx^j$，定义

$$f(x)+g(x)=\sum_{i=0}^{max\{m,n\}}(a_i+b_i)x^i$$

$$f(x)\cdot g(x)=\sum_{k=0}^{m+n}(\sum_{i+j=k}a_ib_j)x^k$$

定义

设R为交换环，五元组$(R[x],+,\cdot,0,1)$称为R上的多项式环，其中$+$与$\cdot$如上述定义。

加法与乘法

下面定义$R[x]$中的$+$与$\cdot$：
设$f(x)=\sum_{i=0}^{n}a_ix^i$，$g(x)=\sum_{j=0}^{m}b_jx^j$，定义

$$f(x)+g(x)=\sum_{i=0}^{max\{m,n\}}(a_i+b_i)x^i$$

$$f(x)\cdot g(x)=\sum_{k=0}^{m+n}(\sum_{i+j=k}a_ib_j)x^k$$

定义

设R为交换环，五元组$(R[x],+,\cdot,0,1)$称为R上的多项式环，其中$+$与$\cdot$如上述定义。

加法与乘法

下面定义$R[x]$中的$+$与$\cdot$:
设$f(x)=\sum_{i=0}^{n}a_ix^i$，$g(x)=\sum_{j=0}^{m}b_jx^j$，定义

$$f(x)+g(x)=\sum_{i=0}^{max\{m,n\}}(a_i+b_i)x^i$$

$$f(x)\cdot g(x)=\sum_{k=0}^{m+n}(\sum_{i+j=k}a_ib_j)x^k$$

定义

设R为交换环，五元组$(R[x],+,\cdot,0,1)$称为R上的多项式环，其中$+$与$\cdot$如上述定义。

举例

例

设Q与R分别为有理数域与实数域，$Q[x]$与$R[x]$为有理多项式环与实多项式环。

例

令$f(x)=2x^2+1, g(x)=13x^3+24x^2+1 \in Z_{26}[x]$，

求$f(x)+g(x)$和$f(x)g(x)$

定理

设R为整环，$f(x), g(x) \in R[x]$，则：

1. $\partial(f(x)g(x)) = \partial f(x) + \partial g(x)$
2. $\partial(f(x)+g(x)) = \max(\partial f(x), \partial g(x))$

举例

例

设Q与R分别为有理数域与实数域，$Q[x]$与$R[x]$为有理多项式环与实多项式环。

例

令$f(x)=2x^2+1, g(x)=13x^3+24x^2+1 \in Z_{26}[x]$，

求$f(x)+g(x)$和$f(x)g(x)$

定理

设R为整环，$f(x), g(x) \in R[x]$，则：

1. $\partial(f(x)g(x)) = \partial f(x) + \partial g(x)$
2. $\partial(f(x)+g(x)) = \max(\partial f(x), \partial g(x))$

举例

例

设Q与R分别为有理数域与实数域，$Q[x]$与$R[x]$为有理多项式环与实多项式环。

例

令$f(x) = 2x^2 + 1, g(x) = 13x^3 + 24x^2 + 1 \in Z_{26}[x]$，

求$f(x) + g(x)$和$f(x)g(x)$

定理

设R为整环，$f(x), g(x) \in R[x]$，则：

1. $\partial(f(x)g(x)) = \partial f(x) + \partial g(x)$
2. $\partial(f(x) + g(x)) = \max(\partial f(x), \partial g(x))$

作业

- 设$Z_n = \{0, 1, \cdots, n-1\}$，$\oplus_n, \otimes_n$分别是模$n$加和模$n$乘，五元组$(Z_n, \oplus_n, \otimes_n, 0, 1)$为环，称为剩余类环，简记为环$(Z_n, +, \cdot, 0, 1)$或$Z_n$。证明该结论
- 证明Z_p为域，这里p为素数
- 证明有零因子的环不为域