第二章 代数基础

第三部分 有限域

2.7 有限域

2.7.1 域的定义与基本性质
2.7.2 域上的多项式
2.7.3 有限域的构造

第四部分 代数基础应用

2.8 代数在信息安全中的应用

第二章 代数基础

第三部分 有限域

2.7 有限域

2.7.1 域的定义与基本性质

2.7.2 域上的多项式

2.7.3 有限域的构造

第四部分 代数基础应用

2.8 代数在信息安全中的应用

本节学习目标

能描述域的概念

熟悉常见的域

域的性质、子域

2.7.1 域的概念

定义2.1 环$(F,+,\cdot)$的所有非零元关于乘法构成一个交换群，则称$(F,+,\cdot)$为域，简称 F 为域。

域的另一种描述：

1. F 关于加法构成交换群；
2. $F^* = F \setminus \{0\}$ 关于乘法构成交换群；
3. 乘法对加法的分配律成立。

定义2.2

- 若域 F 有无限个元素，则称F为无限域；
- 否则称 F 为有限域（Galois 域），并把 F 的元素个数称为 F 的阶。若 F 的阶为 q，记 F 为 GF(q)。

2.7.1 域的概念

问题1： $(Z_2, \oplus, \otimes)$是不是域?

问题2：模9环Z_9={0,1,2,3,4,5,6,7,8}，是不是域？

问题3：模7环Z_7={0,1,2,3,4,5,6}，是不是域？

问题4：全体有理数关于加法和乘法是不是域?

问题5 实数域R 上n阶方阵环 $(R^{n\times n}, +, \times)$是不是域?

2.7.1 域的概念

例1：全体实数关于加法和乘法是域。

例2：全体有理数关于加法和乘法是域

例3：全体复数关于加法和乘法是域

例4：全体整数关于加法和乘法不是域。

例5：$(Z_p, \oplus, \otimes)$ 是域，这里p是素数。

例6：当n为合数时，$(Z_n, \oplus, \otimes)$ 不是域。

2.7.1 域的性质

定理2.3 如果 $(F,+,\times)$ 为域, 则F具有如下性质：

(1) $a+c=b+c \Rightarrow a=b;$

(2) $c\neq 0, a\times c=b\times c \Rightarrow a=b;$

(3) $-(a+b)=(-a)+(-b);\ (-a)\times(-b)=a\times b$

(4) $-(-a)=a;\ (a^{-1})^{-1}=a;\ (-a)^{-1}=-a^{-1}$

2.7.1 域的性质

定义2.4 若域 $(F,+,\times)$ 的子环 F_0 关于加法与乘法构成域，则称 F_0 为 F 的**子域**，F 称为 F_0 的**扩域**。

定理2.5 任何域 F 和它子域 F_0 有相同的零元和单位元，且 F_0 是 F 加法子群，$F_0 \setminus \{0\}$ 是 $F \setminus \{0\}$ 的乘法子群。

例：

- 有理数域 Q 是实数域 R 的子域；
  实数域 R 是有理数域 Q 的扩域。
- 实数域 R 是复数域 C 的子域；
  复数域 C 是实数域 R 的扩域。

2.7.1 域的性质

注意：

有理数域 $\mathbf{Q}$ 和整数环 Z 模素数 p 的剩余类域 $Z_p = \{0, 1, 2, \ldots, p-1\}$ 是两类最基本的域。

一切域可以看做这两类域的扩域！

2.7.1 域的性质

定义2.6 设 F 是一个域，则 F 的所有子域的交集仍是 F 的子域，这个子域称为 F 的**素域**。显然，素域是 F 的最小子域。

定理2.7 设 F 是一个域，则 F 的素域

- 或者同构于有理数域 Q，
- 或者同构于整数环 Z 模素数 p 的剩余类域 Z_p。

小节

- 域的概念
- 常见的域
- 域性质
- 子域

第二章 代数基础

第三部分 有限域

2.7 有限域

2.7.1 域的定义与基本性质

2.7.2 域上的多项式

2.7.3 有限域的构造

第四部分 代数基础应用

2.8 代数在信息安全中的应用

2.7.2 域上的多项式除法

- 对于$F[x]$中的任意两个多项式

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0, \quad a_i \in F,$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0, \quad b_j \in F,$$

- $F[x]$上的加法和乘法分别如下：

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

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

2.7.2 域上的多项式除法

定理2.7 设 F 为一个域，$F[x]$ 关于**x**的多项式全体

$$F[x]=\{\,a_0+a_1x+\ldots+a_nx^n\,|\,n\geq 0,\ a_i\in F\,\}$$

关于多项式加法和乘法为有单位元的交换整环。

2.7.2 域上的多项式除法

例1： 设 $f(x)=x^6+x^4+x+1,\ g(x)=x^4+x+1,$ 为$\mathbf{Z}_2$上两个多项式，则

$$f(x)=(x^2+1)\cdot g(x)+(x^3+x^2).$$

注：$(x^2+1)g(x)+(x^3+x^2)=(x^2+1)(x^4+x+1)+(x^3+x^2)=x^6+x^3+x^2+x^4+x+1+x^3+x^2=f(x)$

例2：如果上例中f与g是$\mathbf{Z}_5$上两个多项式，则

$$f(x)=(x^2+1)\cdot g(x)+(4x^3+4x^2).$$

注：$(x^2+1)g(x)+(4x^3+4x^2)=(x^2+1)(x^4+x+1)+(4x^3+4x^2)=x^6+x^3+x^2+x^4+x+1+4x^3+4x^2=f(x)$

2.7.2 域上的多项式除法

定理2.8 设 $f(x), g(x) \in F[x]$，$g(x) \neq 0$，则存在唯一两个多项式 $q(x)$，$r(x)$，使得

$$f(x) = q(x)g(x) + r(x)$$

其中 $r(x) = 0$ 或 $\deg\big(r(x)\big) < \deg\big(g(x)\big)$。

- $q(x)$ 称为$g(x)$ 除$f(x)$ 的**商式**；
- $r(x)$称为$g(x)$ 除 $f(x)$的**余式**；
- 上述定理中性质称为**带余除法**。
- 对于一般多项式环上述定理不成立。

2.7.2 多项式因式

定义2.8 设 $f(x)$，$g(x)\in F[x]$，如果$g(x)$除 $f(x)$ 的余式 $r(x)=0$ ，则称 $g(x)$ 整除 $f(x)$，记为 $g(x)\mid f(x)$，这时称 $g(x)$为 $f(x)$的因式. 否则称 $g(x)$ 不整除 $f(x)$，记为 $g(x)\nmid f(x)$.

2.7.2 多项式因式

- 零次多项式是任意多项式的因式；任意多项式都是零多项式的因式；
- 如果 $f(x)|g(x), g(x)|f(x)$ ，则

$$f(x)=c\cdot g(x) \quad c\in F\setminus\{0\}$$

- 如果 $f(x)|g(x), g(x)|h(x)$ ，则 $f(x)|h(x)$.

2.7.2 多项式因式

定义2.9 设 $d(x)$，$f(x)$，$g(x)\in F[x]$. 如果

(1) $d(x)\mid f(x)$，$d(x)\mid g(x)$

(2) 对 $f(x)$和 $g(x)$的任意共同的因式(公因子) $d_1(x)$，均有 $d_1(x)\mid d(x)$

则称$d(x)$ 为$f(x)$ 和 $g(x)$的**最大公因式**, 记为

$$d(x)=\big(f(x),g(x)\big)$$

2.7.2 域上的多项式-最大公因式

- 当 $f(x)=g(x)=0$ 时，规定 $(f(x),g(x))=0$

- 当 $q(x)$是$f(x)$与 $g(x)$ 的最大公因式，则 $cq(x)$ 也是$f(x)$与$g(x)$的最大公因式，一般用 $(\boldsymbol{f}(\boldsymbol{x}),\boldsymbol{g}(\boldsymbol{x}))_1$ 表示最高项系数为1的最大公因式；

- 当 $f(x)$与$g(x)$不全为 0 时，$d(x)$为$f(x)$与$g(x)$的最大公因式 $\Leftrightarrow$ $d(x)$ 为$f(x)$与 $g(x)$的次数最高的公因式.

2.7.2 多项式的辗转相除法

定理2.8 (最大公因式的计算方法：**辗转相除法)**

设 $f(x), g(x), r(x) \in F[x]$，如果 $f(x) = q(x)g(x) + r(x)$

则 $(f(x), g(x))_1 = (g(x), r(x))_1$

例　设 $f(x) = x^6 + x^4 + x + 1$

$g(x) = x^4 + x + 1 \in F[x],\ F = Z_2$

求 $(f(x), g(x))_1$.

2.7.2 多项式的辗转相除法

定理2.9（欧几里得算法） 设 $f(x), g(x) \in F[x]$，则 $f(x)$ 与 $g(x)$ 的最大公因式一定存在，并且可以表示为 $f(x)$ 与 $g(x)$ 的一个组合，

$$\big(f(x), g(x)\big) = u(x)f(x) + v(x)g(x)$$

其中 $u(x), v(x) \in F[x]$。

例　设 $f(x) = x^6 + x^4 + x + 1$

$g(x) = x^4 + x + 1 \in F[x],\ F = Z_2$

求$u(x), v(x)$, 使得

$$u(x)f(x) + v(x)g(x) = (f, g)_1$$

2.7.2 多项式的辗转相除法

定义2.10 设 $f(x)$，$g(x)\in F[x]$. 如果

$$(f(x),g(x))_1=1$$

则称 $f(x)$与$g(x)$ 互素。

- 互素具有如下性质：

(1) $(f(x),g(x))_1=1\Leftrightarrow$

$$\exists u(x),\ v(x)\in F[x],\ u(x)f(x)+v(x)g(x)=1$$

(2) 若 $(f(x),g(x))_1=1$，$f(x)\mid g(x)h(x)$ ，则 $f(x)\mid h(x)$

(3) 若 $f(x)\mid h(x)$，$g(x)\mid h(x)$，$(f(x),g(x))_1=1$ 则

$$f(x)g(x)\mid h(x)$$

2.7.2 域上不可约多项式

定义2.11 设$p(x)\in F[x]$，$\deg\big(p(x)\big)\geq 1$，如果 $p(x)$的因式只有非零常数以及自身的非零常数倍，则称 $p(x)$ 为不可约多项式或既约多项式，否则称 $p(x)$ 为可约多项式.

注：AES算法的S盒采用了Z_2上不可约多项式

$$f(x)=x^8+x^4+x^3+x+1$$

2.7.2 域上不可约多项式

定理2.12 关于不可约多项式，有如下结论：

- 一次多项式总是不可约
- 多项式的可约性与其所在的域密切相关
- $p(x)$为不可约多项式 $\Leftrightarrow$ $p(x)$不能分解成两个次数更低的多项式的乘积。对于任意 $f(x)$

$$p(x) \mid f(x) \text{或} (f(x), p(x)) = 1$$

2.7.2 域上不可约多项式

例3：x^4+2 是有理数域上、实数域、复数域、域$\mathbf{Z}_3$不可约多项式吗？不是给出分解。

解：在实数域中与域$\mathbf{Z}_3$中分别分解如下：

$$x^4+2=(x^2+\sqrt{2}+x\sqrt[4]{8})(x^2+\sqrt{2}-x\sqrt[4]{8})$$

$$x^4+2=(x^2-1)(x^2+1)=(x-1)(x+1)(x^2+1)$$

2.7.2 域上不可约多项式

定理2.13 关于一般域上多项式，有如下进一步结论

1) 复数域上不可约多项式只有一次多项式。

2) 实数域不可约多项式只有一次多项式与某些二次多项式，并且 ax^2+bx+c 不可约 $\Leftrightarrow b^2-4ac<0$ 。

3) 有理数域上存在任意次不可约多项式，并且 x^n+2 是不可约多项式。

4) 有限域F上总存在任意次不可约多项式。

2.7.2 域上不可约多项式

定理2.14 $F[x]$ 中每一个次数 ≥ 1 的首一多项式均可唯一表示成 $F[x]$ 中首一的不可约多项式的乘积。这里的唯一是指，若

$$f(x)=p_1(x)p_2(x)\dots p_s(x)=q_1(x)q_2(x)\dots q_t(x)，$$

则 $s=t$，并且适当交换因式的秩序，有

$$p_i(x)=q_i(x),\qquad i=1,2,\dots,s\ .$$

第二章 代数基础

第三部分 有限域

2.7 有限域

2.7.1 域的定义与基本性质

2.7.2 域上的多项式

2.7.3 有限域的构造

第四部分 代数基础应用

2.8 代数在信息安全中的应用

2.7.3 多项式模运算

定义2.15 若域F上多项式$f(x)$与$g(x)$被$m(x)$除有相同的余式，则$f(x)$与$g(x)$关于模$m(x)$同余，简记为

$$f(x)=g(x) \bmod m(x)$$

例1：$f(x)=x^2+x+1,\ g(x)=x^4+x+1, m(x)=x^2+1$是$Z_2$上的多项式，则

$$f(x)=g(x)=x \bmod m(x)$$

2. 7. 3 多项式模运算

定理2.16 $f(x)=g(x) \bmod m(x)$，当且仅当$m(x) \mid f(x)-g(x)$.

例1：$f(x)=x^2+x+1,\ g(x)=x^4+x+1, m(x)=x^2+1$ 是Z_2上的多项式，则

$$f(x)=g(x)=x \bmod m(x)$$

2.7.3 多项式模运算

定理2.17 给定域上多项式 $f(x), g(x), q(x), r(x), m(x)$,则有

1) $f(x)=g(x) \bmod m(x)$, $q(x)=r(x) \bmod m(x)$, $k \in F$, 则

$f(x)+q(x)=g(x)+ r(x) \bmod m(x)$

$k f(x)=kg(x) \bmod m(x)$

2) $f(x)=g(x) \bmod m(x)$, $q(x)=r(x) \bmod m(x)$, $k \in Z$, 则

$f(x)q(x)=g(x)r(x) \bmod m(x)$

$f(x)^k=g(x)^k \bmod m(x)$

3) $q(x)f(x)= q(x)g(x) \bmod m(x)$, $(q(x) , m(x))=1$, 则

$f(x)=g(x) \bmod m(x)$

2.7.3 剩余类域的构造

例1 设 $f(x)=x^3+1$ 为$\mathbf{Z}_2$上的多项式，则$\mathbf{Z}_2$上的多项式全体被 $f(x)$ 除后的余式有**8**个：

$$0,\ 1,\ x,\ x+1,\ x^2, x^2+1,\ x^2+x, x^2+x+1$$

例2 设 $f(x)=x^2+1$ 为$\mathbf{Z}_3$上的多项式，则$\mathbf{Z}_3$上的多项式全体被 $f(x)$ 除后的余式有**9**个：

$$0,\ 1,\ 2,\ x,\ x+1,\ x+2, 2x, 2x+1,\ 2x+2$$

2.7.3 剩余类域的构造

- 设 $p(x)$ 为 $F[x]$ 的**n**次多项式，$F[x]$中所有多项式除以 $p(x)$ 的全体余式为

$$\{ a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \mid a_i \in F \}$$

该集合记为 $\boldsymbol{F[x]/\langle p(x) \rangle}$ 。

定义加法 $f(x) \oplus g(x) = f(x) + g(x) \bmod p(x)$

定义乘法 $f(x) \otimes g(x) = f(x) \cdot g(x) \bmod p(x)$

2.7.3 剩余类域的构造

定理2.18 $F[x]/\langle p(x)\rangle$ 的阶为 p^n, 且 $F[x]/\langle f(x)\rangle$ 关于模 $p(x)$ 的加法与乘法构成环，称之为模 $p(x)$ 的剩余类环.

定理2.19 如果 $p(x)$ 是不可约多项式, 则 $F[x]/\langle f(x)\rangle$ 关于模 $p(x)$的加法与乘法构成域，称之为模 $p(x)$ 的剩余类域。

2.7.3 剩余类域的构造

问题：对于素数 p, 如何构造 p^n 元有限域？

1. 取 F 为 p 阶有限域，p 为素数；
2. 取 $f(x)$ 为 $F[x]$ 中一个n次不可约多项式；
3. $F[x]/\langle p(x)\rangle$ 为一个 p^n 元域。

注：由于任意次不可约多项式存在，故对于任意素数 p 和任意正整数 n，一定存在 p^n 元有限域。

2.7.3 域的特征

定义2.20 设 $(F,+,\times)$ 为一个域，1 为其单位元。

- 如果对任意正整数 m，均有 $m\times 1\neq 0$，则称 F 的特征为 0。
- 如果有一个正整数 m，记使得 $m\times 1=0$ 的最小正整数为 p（可证 p 为素数），则称 F 的特征为 p。

定理 2.21 设 $(F,+,\times)$ 为一个域，

- 若 F 的素域同构于有理数域 Q，则 F 的特征为 0。
- 若 F 的素域同构于模素数 p 的剩余类域 Z_p，则 F 的特征为 p。

2.7.3 域的特征

定理 2.22 如果域 F 特征为 p，则 F 的任何子域都包含 F 的零元和单位元，从而包含素域

$$F_0 = \{0, 1, 2, \ldots, p-1\}$$

定理 2.23 设 F 是有限域，则 F 中元素的个数必为素数的方幂，即 $|F| = p^n, n \in Z^+$。

定理 2.24 对每个素数 p 和正整数 n，都存在一个 p^n 元有限域。

2.7.3 有限域加法特性

定理 2.25 如果域 F 特征为 p，有如下结论成立

- 对 $\forall a, b \in F$，均有

$$p \cdot a = 0, \qquad (a+b)^p = a^p + b^p$$

- $m \in Z,\ m \cdot a = 0 \Leftrightarrow p \mid m$

2.7.3 域的特征

定理 2.26 设 F_q 是有限域，其中 $q = p^n, n \geq 1, p$ 是素数，则乘法群 $(F_q^*, \cdot)$ 是循环群。

定义 2.27 有限域 F_q 的乘法群 F_q^* 中的生成元称为 F_q 的本原元。

2.7.3 剩余类域的构造

例3 令 $F = Z_2$，在 $F[x]$ 中取 $f(x) = x^2 + x + 1$，$f(x)$ 为 $F[x]$ 中 2 次不可约多项式。

$$F[x]/\langle f(x)\rangle = \{a_0 + a_1 x \mid a_i \in Z_2\}$$

为 $2^2 = 4$ 元域。

例4 令 $F = Z_3$，在 $F[x]$ 中取 $f(x) = x^5 + x^2 + x + 1$，$f(x)$ 为 $F[x]$ 中 5 次可约多项式。$f(x) = x^5 + x^2 + x + 1 = (x+1)(x^4 + 2x^3 + x^2 + 1)$

$$F[x]/\langle f(x)\rangle = \{a_0 + a_1 x + \cdots + a_4 x^4 \mid a_i \in Z_3\}$$

为 3^5 元环但不是域。

2.7.3 域的特征

例5 已知 x^2+1为 Z_3 上不可约多项式，有限域 F_9 构造如下：

$$F_9 = F_3[x]/\langle x^2+1\rangle$$

$$= \{0, 1, 2, x, 1+x, 2+x, 2x, 1+2x, 2+2x\}$$

可验证 $F_9^* = \langle 1+x\rangle$，即

$$F_9 = \{0, (1+x)^0 = 1, (1+x)^1 = 1+x,$$

$$(1+x)^2 = 2x, (1+x)^3 = 1+2x,$$

$$(1+x)^4 = 2, (1+x)^5 = 2+2x,$$

$$(1+x)^6 = x, (1+x)^7 = 2+x\}$$

2.7.3 有限域乘法特性

例6 已知 x^3+x+1为 F_2上不可约多项式，写出 $F_2[x]$模(x^3+x+1)的剩余类域 $F_2[x]/\langle x^3+x+1\rangle$

多项式	本原元的幂元
0	0
1	x^0
x	x^1
$x+1$	x^3
x^2	x^2
x^2+1	x^6
x^2+x	x^4
x^2+x+1	x^5