信息安全数学基础

（内部教材）

院系：计算机科学与技术学院

教师：韩 琦

版本：2023秋_v_20230910

目 录

第一部分

近世代数

前 言

近世代数也叫抽象代数。代数是数学的其中一门分支，可大致分为初等代数学和近视代数（抽象代数）学两部分。初等代数学是指19世纪上半叶以前发展的代数方程理论，主要研究某一代数方程（组）是否可解，如何求出代数方程所有的根〔包括近似根〕，以及代数方程的根有何性质等问题。

法国数学家伽罗瓦〔1811-1832〕在1832年运用「群」的思想彻底解决了用根式求解多项式方程的可能性问题。他是第一个提出「群」的思想的数学家，一般称他为近世代数创始人。他使代数学由作为解代数方程的科学转变为研究代数运算结构的科学，把代数学由初等代数时期推向近世代数时期。

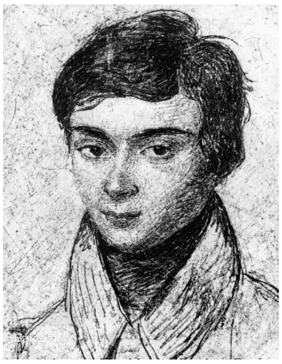

图 0-1 法国数学家伽罗瓦〔1811-1832〕

他是一个天才少年, 15岁学习数学, 短短5年就创造出对后世影响深远的“群论”, 带来数学的革命。他也是一个悲情少年, 两次升学未成, 三次论文发表被拒, 两次被捕入狱, 20岁时就因与情敌对决而黯然离世......

本章，我们就一起来了解一下近世代数都有哪些精彩的概念和方法，以及能够为信息技术和信息安全带来哪些理论上的支撑。

第 1 章　群

1.1 集合和代数运算

在介绍代数结构之前，我们先来了解一下构成代数结构的基本要素。

首先，要了解的概念是**集合**。近世代数中群、环、域的定义都是基于集合的，通过对集合上运算的约束，将集合构造成具有不同特性的新对象。

若干个(有限或无限多个)固定事物的全体称作一个**集合**，简称集。组成一个集合的事物称作这个集合的**元素**，简称元。

不包含任何元素的集合称作空集合，记为$\varnothing$。

集合常用大写字母$A, B, C, \cdots$表示，元素常用小写字母$a, b, c, \cdots$表示。一个集合若是由元素$a, b, c, \cdots$组成的，用符号表示为

$$A = \{a, b, c, \cdots\}$$

若a是集合A的一个元素，就说a属于A或A包含a，用符号表示为

$$a \in A \quad 或 \quad A \ni a$$

定义 1.1 (映射) 设X与Y是两个集合，如果有一个法则η，它对X中每个元素x，在Y中都有一个唯一确定的元素y与它对应，则称η为集合X到集合Y的一个**映射**。这种关系表示为

$$\eta : x \longrightarrow y \quad 或 \quad y = \eta(x)$$

并且把y称作x在映射η之下的**象**，而把x称作y在映射η之下的**原象**或**逆象**。

例 1.1 设$A = \{a, b, c, d\}$，$B = \{1, 2, 3\}$，令

$$\begin{aligned} \eta_1 :\ & a \longrightarrow 1 \\ & b \longrightarrow 2 \\ & c \longrightarrow 3 \\ & d \longrightarrow 3 \end{aligned}$$

易知η_1是A到B的一个映射。再令

$$\begin{aligned}\eta_2:\quad & a \longrightarrow 1\\ & b \longrightarrow 2\\ & d \longrightarrow 3\end{aligned}$$

由于A中元素c在η_2之下没有象，故η_2不是A到B的一个映射。若令

$$\begin{aligned}\eta_3:\quad & a \longrightarrow 1\\ & b \longrightarrow 2\\ & c \longrightarrow 1\\ & d \longrightarrow 1\end{aligned}$$

η_3是A到B的一个映射。

例 1.2 设X为有理数集，Y为实数集，则法则

$$\eta : x \longrightarrow \frac{1}{x-1}$$

不是X到Y的映射，因为有理数1没有确定的象。

例 1.3 设X和Y都是有理数集，法则

$$\eta : \frac{a}{b} \longrightarrow a + b$$

不是X到Y的映射。因为，例如对于$\frac{1}{2} = \frac{2}{4}$，却有

$$\eta(\frac{1}{2}) = 1 + 2 = 3, \quad \eta(\frac{2}{4}) = 2 + 4 = 6$$

即X中相等的元素在Y中的象不唯一。

例 1.4 设$X = \{1, 2, 3\}, Y = \{2, 4, 8, 10\}$，则法则

$$\eta : x \longrightarrow 2x$$

不是X到Y的映射。虽然η对X中每个元素都有一个唯一确定的象，但3的象6却不属于Y。

这就是说，集合X到集合Y的一个法则η，在满足一下三个条件是才是一个映射：

(1)η对于X中每个元素都必须有象；

(2)X中每个元素的象是唯一的；

(3)X中每个元素的象必须属于Y。

下面来看一下什么是**集合上的代数运算**：

定义 1.2 (**集合上的代数运算**) 设S为集合，映射

$$\eta : \begin{cases} S \times S & \to & S \\ (x, y) & \mapsto & z \end{cases}$$

称为集合S上的代数运算。

例 1.5 普通加法、减法与乘法都是整数集、有理数集、实数集合复数集的代数运算。

例 1.6 普通的减法不是正整数集的代数运算，例如正整数1减2得-1，但-1不是正整数。

例 1.7 法则

$$a \circ b = ab + 1 \quad \text{或} \quad a \circ b = a + b - 10$$

都是整数集的代数运算，而且前者还是自然数集的一个代数运算。

例 1.8 法则

$$A \circ B = |A| B$$

是数域F上全体n阶方阵的集合的一个代数运算。

1.2 群的定义

定义 1.3 (**群**) 设三元组$(G, \cdot, 1)$中G为集合，$\cdot$为集G上的代数运算，1为G中一个元。若$(G, \cdot, 1)$满足：

- $G1$(乘法结合律)：$a \cdot (b \cdot c) = (a \cdot b) \cdot c$，$a, b, c \in G$；
- $G2$(单位元)：$1 \cdot a = a \cdot 1 = a$，$a \in G$；

- $G3$(逆元)：对$a \in G$，有$a' \in G$使得$a \cdot a' = a' \cdot a = 1$。

则称$(G, \cdot, 1)$为**群**，简称群G，1称为群G的**单位元**，a'称为a的**逆元**。

若$(G, \cdot, 1)$还满足

- $G4$(交换律)：$a \cdot b = b \cdot a$，$a, b \in G$

则称G为**交换群**。

若$(G, \cdot, 1)$仅满足$G1, G2$，则称G为**有单位元的半群**。

若$(G, \cdot, 1)$ 满足$G1, G2, G4$，则称G为**有单位元的交换半群**。

例 1.9 设$(Q^*, \cdot, 1)$中Q^*为零以外的所有有理数的集合，$\cdot$为有理数乘法，1为整数1，则$(Q^*, \cdot, 1)$满足$G1, G2, G3$和$G4$。故$(Q^*, \cdot, 1)$为交换群。

例 1.10 设$(Z, +, 0)$中Z为整数集，$+$为整数的加法，0为整数零，易验证$(Z, +, 0)$中有$a + (b + c) = (a + b) + c$，故$G1$成立；又有$a + 0 = 0 + a$，故$G2$成立；最后有$a + (-a) = (-a) + a = 0$，这里$(-a)$表示与$a$对应的负整数，因而$G3$成立；再$a + b = b + a$，故$G4$成立。从而$(Z, +, 0)$为交换群。

例 1.11 设$GL_n(\mathbf{R})$为n阶实数可逆方阵的集合，$\cdot$为两矩阵的乘法，$\mathbf{I}$为单位阵，则$(GL_n(R), \cdot, \mathbf{I})$为群。$GL_n(R)$称为实数域$R$上$n$阶一般线性群。

例 1.12 (希尔密码) 在希尔密码(Hill Cipher)中加密变换为

$$(y_1 y_2 \cdots y_m) = (x_1 x_2 \cdots x_m)\mathbf{M}(\text{mod } 26)$$ □

这里密钥$\mathbf{M} \in GL_m(Z_{26}), x_i, y_i \in Z_{26}, Z_{26} = \{0, 1, \cdots, 25\}$，$x_i$为明文，$y_i$为密文。(上式右边的行向量$(x_1, x_2, \cdots, x_m)$与矩阵$\mathbf{M}$乘是先进行通常的实数行向量与实数矩阵乘再对所得行向量的每一分量取模26。)

加密过程：字母$AB \cdots Z$分别对应$0, 1, \cdots, 25$，加密前先将明文字母串变换为Z_{26}上的数字串，然后再按上述表达式每次m个数字的将明文数字串变换为密文数字串，最后将密文数字串变换为密文字母串。

关于如何求逆矩阵，可以参考如下的定理：

定理 1.1 设$\mathbf{A} = (a_{ij})$为一个定义在$\mathbf{Z}_{26}$上的$n \times n$矩阵，若$\mathbf{A}$在mod 26上可逆，则有：

$$\mathbf{A}^{-1} = (det\mathbf{A})^{-1}\mathbf{A}^*(\text{mod } 26)$$

这里，$\mathbf{A}^*$是$\mathbf{A}$的伴随矩阵。

例 1.13 (IDEA密码的群运算) IDEA(International Data Encryption Algorithm)用到结构$(Z_2^{16}, \oplus, \boxplus, \odot, 0)$，其中$Z_2^{16} = a = a_0a_1\cdots a_{15}|a_i \in Z_2$，0表示全零向量，约定$a \in Z_2^{16}$在需要时等同为二进制表示为$a$的整数或反过来一整数等同为其16位的二进制表示。对$a, b \in Z_2^{16}$，定义$a \oplus b$为按位异或；定义$a \boxplus b$为$a + b \ mod \ 2^{16}$；定义$a \odot b$为$(a \cdot b \ mod \ 65537) \ mod \ 65536$，此时需约定$a \neq 0, b \neq 0$。这里$(Z_2^{16}, \oplus, 0), (Z_2^{16}, \boxplus, 0), (Z_2^{16}, \odot, 0)$都为群。IDEA密码反复在$Z_2^{16}$上施行不同群运算$\oplus, \boxplus, \odot$以获得一个好的密码体制所需的扩散与混淆效应。

定义 1.4 (子群) 设$(G, \cdot, 1)$为群，A为G的子集合。若$1 \in A$且$(A, \cdot, 1)$构成群，则称A为G的**子群**，并记为$A \leq G$。

例 1.14 证明$nZ = \{0, \pm n, \pm 2n \cdots\}$为整数群$(Z, +, 0)$的子群。

证:

- $nZ \subseteq Z$
- $0 \in A$
- $(nZ, +, 0)$为群

1.3 置换与对称群

定义 1.5 (置换) $S = \{1, 2, \cdots, n\}$，映射$\sigma : S \to S$是可逆的，则称σ为S上的**置换**。

定义 1.6 (对称群) 全体S上的置换所成的集合记为S_n，命1表示恒等置换，在S_n中以$\sigma(i)$表示i在置换σ下的像，定义S_n中两元素σ与η的乘积为

$$[\sigma \cdot \eta](i) = \sigma(\eta(i))$$

则$(S_n, \cdot, 1)$成群，群S_n称为n次**对称群**。

可见，对称群是一个以置换为集合中元素的群。

下面，我们从对称群的角度来重新描述一下置换和代换两种古典密码方法：

例 1.15 (置换密码) 在置换密码(Permutation Cipher)中加密变换为：
$(y_1\ \ y_2\ \ \cdots\ \ y_m) = (\sigma(x_1)\ \ \sigma(x_2)\ \ \cdots\ \ \sigma(x_m))$，
这里$x_i, y_i \in S = \{1, 2, \cdots, m\}$，$x_i$为明文，$y_i$为密文，$\sigma \in S_m$，$S_m$为$\{1, 2, \cdots, m\}$上$m$次对称群。加密时按上述表达式每次$m$个字符的将明文串变换为密文串。

设置换密码中$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \in S_4$，则对应明文MAGAZINE的密文为AMAGEZIN。

例 1.16 (代换密码) 在代换密码(Substitution Cipher)中加密变换为$y = \sigma(x)$，这里$x, y \in \Sigma = \{A, B, \cdots, Z\}$，$x$为明文，$yi$为密文，$\sigma \in S_{ym\Sigma}$，
$S_{ym\Sigma}$为Σ上的对称群。加密时按上述表达式逐字符的将明文串变换为密文串。

设代换密码中$\sigma = \begin{pmatrix} ABCDEFGHIJKLMNOPQRSTUVWXYZ \\ DCABIJHGFEZYXWVUTSRQPONMLK \end{pmatrix}$，则对应密文ESJCACDVVZ的明文为IREADABOOK。

1.4 循环群与生成元

定义 1.7 (循环群) 若群G的每一个元都能表成一个元素a的方幂，则G称为由a生成的**循环群**，记作$G =< a >$，a称为循环群G的**生成元**。

根据元素的阶的性质，循环群$G =< a >$共有两种类型：

1. 当生成元a是无限阶元素时，则G称为无限阶循环群。
2. 如果a的阶为n，即$a^n = 1$，那么这时$G =< a >=< 1, a, a^2, \cdots, a^{n-1} >$，则$G$称为由$a$所生成的$n$阶循环群，注意此时$1, a, a^2, \cdots, a^{n-1}$两两不同。

例 1.17 (群上的离散对数) 对$a, b \in G$(G为交换群)，求整数x使得$b = a^x$。

p阶循环群G上的离散对数问题迄今无快速算法。据此，p阶循环群G上的离散对数问题可用于公开钥密码体制的设计。注意，群上的离散对数问题中G为交换群，G的运算写成+，则群上的离散对数问题表示为：

对$a, b \in G$(G为交换群，运算写成+)，求整数x使得$b = xa$。

例 1.18 (希尔密码) ：在希尔密码(Hill Cipher)中加密变换为

$$(y_1 y_2 \cdots y_m) = (x_1 x_2 \cdots x_m) M mod\, 26 \tag{1-1}$$

这里密钥$M \in GL_m(Z_{26}), x_i, y_i \in Z_{26}, Z_{26} = 0, 1, \cdots, 25$，$x_i$为明文，$y_i$为密文，式1-1右边的行向量$(x_1, x_2, \cdots, x_m)$与矩阵$M$乘是先进行通常的实数行向量与实数矩阵乘再对所得行向量的每一分量取模26。

1.5 群上的离散对数

不同代数系统中都有各自的对数(离散对数)问题，有的可以找到快速算法，有的则尚未找到快速算法。尚未找到快速算法的离散对数问题，可以看作一个数学上的“难题”，能够用来构造密码学算法或协议。

例 1.19 ($(Z_n^*, \otimes_n, 1)$) 设$\otimes_n$为模n乘，三元组$(Z_n, \otimes_n, 1)$满足G1、G2和G4，为有单位元的交换半群，但其一般不为群，因为当n为合数时，Z_n中某些元不存在逆元。
当n为素数时，对$a \in Z_n^* = \{1, 2, \cdots, n-1\}$有$a' \in Z_n^*$使得$a \otimes_n a' = 1$，即$Z_n^*$中每个元都有逆元，故$(Z_n^*, \otimes_n, 1)$为群。

例 1.20 (**$(Z_n^*, \otimes_n, 1)$上的离散对数**) 设n为素数，在$(Z_n^*, \otimes_n, 1)$中可定义
$a^m = a \otimes_n a \otimes_n \cdots \otimes_n a$（$m$个$a$，$m$为整数）
对已知的$a, b \in Z_n^*$，求整数x，使得 $a^x = b$的问题称为Z_n^*上的离散对数问题。该问题迄今无快速算法，被应用于Diffie-Hellman密钥交换协议中。

例 1.21 (**群上的离散对数**) 对$a, b \in G$（G为交换群），求整数x使得$b = a^x$。
群上离散对数问题中G为交换群，G的运算写成$+$，则群上的离散对数问题表示为：求整数x使得$b = xa$。
此种形式的离散对数问题应用于椭圆曲线密码体制（ECC）中。

第 2 章　环

2.1 环的定义

定义 2.1 (环) 设五元组$(R,+,\cdot,0,1)$中，R为集合，$+$与$\cdot$为集R上代数运算，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。$+$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$a'+a=0$，则称a'为a的**负元**，写为$-a$。若$a"\in R$使$a"\cdot a=1$，则称$a"$为a的a^{-1}。$(R,+,0)$称为环R的**加法群**。$(R,\cdot,1)$称为环R的**乘法半群**。

定义 2.2 (交换环) 若环$(R,+,\cdot,0,1)$满足

- $R4$(乘法半群交换)：$(R,\cdot,1)$为交换的半群。

则称R为**交换环**。

定义 2.3 (体，域) 若环$(R,+,\cdot,0,1)$满足

- $R5$：$(R^*,\cdot,1)$为群，这里$R^*=R-\{0\}$；或
- $R6$：$(R^*,\cdot,1)$为交换群。

则称R为**体或域**。

例 2.1 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：

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

例 2.2 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

例 2.3 ：设$Z_n=\{0,1,\cdots,n-1\}$，$\oplus_n,\otimes_n$分别是模n加和模n乘，则五元组$(Z_n,\oplus_n,\otimes_n,0,1)$为环，称为剩余类环，简记为环$(Z_n,+,\cdot,0,1)$或$Z_n$。

例 2.4 ：设p为素数，剩余类环$(Z_p,\oplus_n,\otimes_n,0,1)$为域，该域称为有限域，写为$GF(p)$。在$GF(17)$中$14+15=12, 5\cdot 8=6, 5^{-1}=7$。

2.2 整环

下面介绍零因子和整环的概念：

定义 2.4 (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 2.5 (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 2.5 在环Z_{26}中13和2是零因子。

2.3 理想

定义 2.6 (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 2.7 (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 2.6 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$nZ=(n)$。

2.4 环上多项式

设x为文字，R为交换环，$x \notin R$。定义R上多项式集

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

其中，$f(x) = \sum_{i=0}^{n} a_i x^i$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，$a_i$称为$f(x)$的第$i$次项系数；约定$a_0 x^0$简写为$a_0$。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$n$，$n + (-\infty) = -\infty$。

下面定义$R[x]$中的$+$与$\cdot$：

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

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

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

定义 2.8 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。

例 2.7 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 2.8 令$f(x) = 2x^2 + 1, g(x) = 13x^3 + 24x^2 + 1 \in Z_{26}[x]$，则

$$f(x)g(x) = 22x^4 + 13x^3 + 24x^2 + 1$$

注意，$f(x)g(x)$的次数为4，因Z_{26}有零因子所致。

定理 2.1 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. $\partial(f(x)+g(x)) \leq \max(\partial f(x), \partial g(x))$

两个多项式相加，最高次项有可能相加后为0，因此上述第2个结论，是小于等于。

例：多项式环的主理想 设$f(x) = \sum_{i=0}^{n} a_i x^i \in Z[x]$，则$(f(x) = f(x)z(x)|z(x) \in Z[x])$为$Z[x]$的主理想。

例：纠错码之—循环码 设F为域，环$(F[x]_{x^n-1}$，$+$，$\cdot$，0，$1)$中$F[x]_{x^n-1}$为域F上次数小于n的多项式集合，$+$与$\cdot$分别为两多项式的模x^n-1加与乘，该环称为剩余类多项式环。该环的由x^n-1的因式，$n-k$次多项式$g(x)$生成的理想$I = \{f(x) = v_0 + v_1 x + \cdots + v_{n-1}x^{n-1}|$有次数小于$k$的多项式$h(x)$使$f(x) = h(x)g(x)\}$具有如下性质：
若$v_0 + v_1 x + \cdots + v_{n-1}x^{n-1} \in I$，则$v_{n-1} + v_1 x + \cdots + v_{n-2}x^{n-1} \in I$。$I$为循环纠错码。

第 3 章　域

3.1 域的定义

定义 3.1 (**域**) 设五元组$(F, +, \cdot, 0, 1)$中，F为集合，$+$和$\cdot$为集合F上的代数运算，0和1为F中元。若$(F, +, \cdot, 0, 1)$满足

- $F1$(加法交换群)：$(F, +, 0)$是交换群
- $F2$(乘法交换群)：$(F^*, \cdot, 1)$是交换群，这里$F^* = F - 0$
- $F3$(乘法对加法的分配律)：$a \cdot (b + c) = a \cdot b + a \cdot c$，$a, b, c \in F$

则称$(F, +, \cdot, 0, 1)$为**域**，简称域F。$+$和$\cdot$称为域F的加法和乘法。1称为F的单位元，0称为域的零元。若$a' \in F$使$a' + a = 0$，则称a'为a的负元，写为$-a$。若$a" \in F$使$a" \cdot a = 1$，则称$a"$为a的逆元，写为a^{-1}。$(F, +, 0)$称为域F的加法群。$(F^*, \cdot, 1)$称为域F的乘法群。

例 3.1 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。

例 3.2 实数集R在实数加法$+$与实数乘法$\cdot$下为域，称为实数域$(R, +, \cdot, 0, 1)$，简记为域R。

例 3.3 五元组$(Q, +, \cdot, 0, 1)$中，Q为有理数集合，0和1为有理数0和1，$+$和$\cdot$称为有理数$+$和$\cdot$。$(Q, +, \cdot, 0, 1)$满足域的定义，称为有理数域Q。类似地有实数域R和复数域C。

定义 3.2 设F是一个域，如果F含有无限多个元素，则称F为无限域。相反，如果F含有有限个元素，则称为**有限域**或**Galois域**，并把F中元素的个数称为F的**阶**。若F含有q个元素，可简记为$GF(q)$。

例 3.4 在域$GF(2)$中仅有两个元0和1，故称二元域。元0和1可又电信号的低和高实现，模2加$\oplus_2$可由数字信号的异或实现，模2乘$\otimes_2$可由数字信号的与实现，所以二元域$GF(2)$就成为信息科学技术领域及信息安全领域应用最多的域之一。

3.2 扩域

定理 3.1 **(带余除法)** 设$f(x)$和$g(x)$为$F[x]$中的多项式，且$g(x)\neq 0$，则存在惟一的两个多项式$q(x)$和$r(x)$，使得

$$f(x)=q(x)g(x)+r(x),\quad \partial r(x)<\partial g(x) \tag{3-1}$$

称$f(x)$为被除式，$g(x)$为除式，$q(x)$为商式，$r(x)$为余式。

式3-2中，若$r(x)=0$，则称$g(x)$是$f(x)$的**因式**，或称$f(x)$是$g(x)$的**倍式**，还称$f(x)$能被$g(x)$整除，记作$g(x)|f(x)$。

设$f(x),g(x),q(x)$是$F[x]$中的多项式，且$q(x)\neq 0$。如果$q(x)$既是$f(x)$的因式，又是$g(x)$的因式，则称$q(x)$为$f(x)$和$g(x)$的**公因式**。如果$f(x)$和$g(x)$不全为0，则$f(x)$和$g(x)$的公因式中次数最高的首1多项式称为$f(x)$和$g(x)$的最高公因式，记作$(f(x),g(x))$。如果$(f(x),g(x))=1$，则称$f(x)$与$g(x)$互素。

设$f(x),g(x),q(x)$是$F[x]$中的多项式，且$q(x)\neq 0$。如果$q(x)$既是$f(x)$的倍式，又是$g(x)$的倍式，则称$q(x)$为$f(x)$和$g(x)$的**公倍式**。如果$f(x)$和$g(x)$不全为0，则$f(x)$和$g(x)$的公因式中次数最低的首1多项式称为$f(x)$和$g(x)$的最低公倍式，记作$[f(x),g(x)]$。

定理 3.2 设$f(x)$和$g(x)$为$F[x]$中不等于0的多项式，则必存在$F[x]$中的两个多项式$a(x)$和$b(x)$，使得

$$(f(x),g(x))=a(x)f(x)+b(x)g(x) \tag{3-2}$$

例 3.5 设$f(x)=x^6+x^4+x+1$，$g(x)=x^4+x+1$为$GF(2)$上的多项式，用Eulid算法求出$(f(x),g(x))$。

$$\begin{aligned}
&x^6+x^4+x+1=(x^2+1)(x^4+x+1)+(x^3+x^2)\\
&x^4+x+1=(x+1)(x^3+x^2)+(x^2+x+1)\\
&x^3+x^2=x(x^2+x+1)+x\\
&x^2+x+1=(x+1)x+1\\
&x=1x+0
\end{aligned}$$

所以$(f(x),g(x))=1$。进一步把上述各式改写如下(在$GF(2)$上+等于−):

$$\begin{aligned}
&x^3+x^2=x^6+x^4+x+1+(x^2+1)(x^4+x+1)\\
&x^2+x+1=x^4+x+1+(x+1)(x^3+x^2)\\
&x=x^3+x^2+x(x^2+x+1)\\
&1=x^2+x+1+(x+1)x\\
&x=1x+0
\end{aligned}$$

把x,x^2+x+1,x^3+x^2依次代入表达式$1=x^2+x+1+(x+1)x$中：

$$\begin{aligned}
1 &= (x^2+x+1)+(x+1)[(x^3+x^2)+x(x^2+x+1)]\\
&= (x+1)(x^3+x^2)+(x^2+x+1)(x^2+x+1)\\
&= (x+1)(x^3+x^2)+(x^2+x+1)[(x^4+x+1)+(x+1)(x^3+x^2)]\\
&= (x^3+x)(x^3+x^2)+(x^2+x+1)(x^4+x+1)\\
&= (x^3+x)[(x^6+x^4+x+1)+(x^2+1)(x^4+x+1)]+(x^2+x+1)(x^4+x+1)\\
&= (x^3+x)(x^6+x^4+x+1)+(x^5+x^2+1)(x^4+x+1)
\end{aligned}$$

最后得到

$$(f(x),g(x))=(x^3+x)f(x)+(x^5+x^2+1)g(x)$$

设$f(x)$是$F[x]$中的一个多项式，且$\partial f(x)\ \geq\ 1$。如果$f(x)$的因式只有常数$c(c\neq 0)$或$cf(x)$，则称$f(x)$为域F上的**不可约多项式或既约多项式**。否则，称$f(x)$为域F上的可约多项式。

定理 3.3 域F上的次数≥ 1的多项式都可以分解成一些域F上的既约多项式的乘积。如果不计这些既约多项式在乘积中的先后顺序，那么这些分解还是惟一的。

定理 3.4 设$p(x)$是域F上的一个n次既约多项式，记$F[x]_{p(x)}$为模$p(x)$的全体余式集合，即

$$F[x]_{p(x)}=\{a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots a_1x+a_0,a_i\in F\}$$

并对于任意的$f(x)$和$g(x) \in F[x]_{p(x)}$，定义以下的按模加和按模乘运算：

$$f(x) + g(x) = (f(x) + g(x))_{p(x)}$$
$$f(x) \cdot g(x) = (f(x) \cdot g(x))_{p(x)}$$

则$F[x]_{p(x)}$关于所定义的加法和乘法运算构成域。如果F包含q个元素，则$F[x]_{p(x)}$是一个包含q^n个元素的有限域$GF(q^n)$，而且F是这个$GF(q^n)$的子域。

根据定理3.4，F是$F[x]_{p(x)}$的子域，$F[x]_{p(x)}$是F的扩域。从F到$F[x]_{p(x)}$是经过$p(x)$实现的，所以又称$F[x]_{p(x)}$是又$p(x)$扩成的域。

例 3.6 由$GF(2)$上的4次既约多项式$p(x) = x^4 + x + 1$扩成的$GF(2^4)$如下表所示

4位向量形式	多项式形式
0000	0
0001	1
0010	x
0100	x^2
1100	x^3
0011	$x+1$
0110	x^2+x
1100	x^3+x^2
1011	x^3+x+1
0101	x^2+1
1010	x^3+x
0111	x^2+x+1
1000	x^3+x^2+x
1111	x^3+x^2+x+1
1101	x^3+x^2+1
1001	x^3+1

定义 3.3 设$f(x)$为$GF(2)$上的$n-1$次多项式，A为$GF(2)$上的n位数据组，

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0, \quad a_i \in GF(2)$$
$$A = (a_{n-1}, a_{n-2}, \cdots, a_1, a_0), \quad a_i \in GF(2)$$

定义映射如下：

$$f(x) \leftrightarrow A$$

显然，这种映射关系是一对一的映射，该映射将一个多项式转换成一个数据组，反过来，也可将一个数据组转换成一个多项式。

3.3 有限域

定义 3.4 设F是一个域，如果F含有无限多个元素，则称F为**无限域**。相反，如果F含有有限个元素，则称为**有限域**或**Galois域**，并把F中元素的个数称为F的**阶**。若F含有q个元素，可简记为$GF(q)$。

例 3.7 在域$GF(2)$中仅有两个元0和1，故称二元域。元0和1可由电信号的低和高实现，$\oplus_2$可由数字信号的异或实现，$\otimes_2$可由数字信号的与实现，所以二元域$GF(2)$就成为信息科学技术领域及信息安全领域应用最多的域之一。

3.3.1 有限域的加法特性

在有理数域Q、实数域R和复数域C中，任意多个1相加都不等于0。而在有限域中，因为元素的个数有限，所以下面的元素序列中不可能没有相同的元素：

$$1, 1+1 = 2 \cdot 1, 1+1+1 = 3 \cdot 1, 1+1+1+1 = 4 \cdot 1, \cdots$$

设在此序列中有$i \cdot 1 = j \cdot 1, 1 \leq i < j$，则有$(j-i) \cdot 1 = 0$。令$p = j - i$，则有$p \cdot 1 = 0$

定义 3.5 **(域的特征)** 设F是一个域，而1是其乘法单位元。如果对应任意的正整数m，都有$m \cdot 1 \neq 0$，则称域F的特征是0。如果有一个正整数m，使得$m \cdot 1 = 0$，而且适合此条件的最小正整数为p，则称域F的特征是p。

定理 3.5 设F是一个域，F的特征要么是0，要么是一个素数p。

证明：假设F的特征是0，则定理成立。假设F的特征不是0，则必存在一个正整数m，使得$m \cdot 1 = 0$。设满足此条件的最小正整数p，证明p一定是素数。假设p不是素数，则p可分解成$p = p_1 p_2, 1 < p_1, p_2 < p$。于是

$$p \cdot 1 = p_1 p_2 \cdot 1 = (p_1 \cdot 1)(p_2 \cdot 1) = 0$$

因此有$p_1 \cdot 1 = 0$ 或$p_2 \cdot 1 = 0$
这与p的最小性相矛盾，所以p一定是素数。

例 3.8 只有0和1两个元素的二元域$GF(2)$和由$GF(2)$上的n次既约多项式扩成的有限域$GF(2^n)$的特征都是2。

根据前定理，特征为0的域一定是无限域，而有限域的特征一定是一个素数。

注意：此论断的逆命题不成立。例如，系数取自$GF(p)$的全体有理数函数的集合

$$S = \{\frac{f(x)}{g(x)} | f(x), g(x) \text{ 是}GF(p)\text{上的多项式}\} \qquad \square$$

便构成一个特征为p的无限域。之所以是无限域，是因为对$f(x)$和$g(x)$的次数没有限制。

定理 3.6 设F是特征为p的一个有限域，对于任意$a, b \in F$都有

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

证明： 根据牛顿二项式定理，$(a+b)^p = \sum_{k=0}^{p} C_p^k a^k b^{p-k}$ 注意到其中$C_p^0 = C_p^p = 1$，而对于$1 \le k \le p-1, C_p^k = \frac{p(p-1)\cdots(p-k+1)}{1\cdot 2\cdot 3\cdots k}$。因为$C_p^k$是正整数，$p$是素数，所以$\frac{(p-1)\cdots(p-k+1)}{1\cdot 2\cdot 3\cdots k}$一定是整数，也就是说$p|C_p^k$，因此$C_p^k = 0 \; mod \; p$。

例 3.9 设$f(x) = x^4 + x + 1$是$GF(2)$上的多项式，则
$(f(x))^2 = (x^4 + x + 1)^2 = x^8 + x^2 + 1$ $\square$

3.3.2 有限域的乘法特性

引理 3.6 设G是一个有限交换群，a是G的一个n阶元素，k是任意正整数，则a^k是$\frac{n}{(n,k)}$阶元素。特别a^k是n阶元素，当且仅当$(n, k) = 1$。

引理 3.7 设G是一个有限交换群，a是G的一个m阶元素，b是G的一个n阶元素，并假设$(n, m) = 1$，则ab是一个mn阶元素。

引理 3.8 设G是一个有限交换群。假定G中元素的阶最大为n，则G中任何元素的阶都是n的因子。

定理 3.7 任一有限域的乘法群都是循环群。

定理 3.8 (**Fermat定理**) $GF(p^n)$中的任一元素a都满足等式 $a^{p^n}=a$
或者说都是方程 $x^{p^n}-x=0$
的根。还可以说 $x^{p^n}-x=\prod_{a\in F}(x-a)$

该定理说明方程$x^{p^n}-x=0$没有重根，而且$GF(p^n)$的全部元素就是它的全部根。

定义 3.9 (**本原元**) 有限域$GF(q)$乘法群的生成元(即阶为$q-1$的元素)为$GF(q)$的本原元。

一个有限域往往不只有一个本原元。根据前面引理可以算出有限域本原元的个数。考虑有q个元素的有限域$GF(q)$，根据定理，$GF(q)$的乘法群是循环群，这就是说，$GF(q)$至少有一个本原元a使得

$$a^0=1,a,a^2,\cdots,a^{q-2}$$

就是$GF(q)$的乘法群的全体元素。根据引理，元素$a^i(i=1,2,\cdots,q-2)$的阶为$q-1$，当且仅当$(i,q-1)=1$。因此，$GF(q)$的本原元个数为$\phi(q-1)$。($\phi(x)$为欧拉函数，表示在小于x且与x互素的正整数的个数。例如$\phi(5)=4,\phi(6)=2$)。

考查由$GF(2)$上的既约多项式x^4+x+1扩成的有限域$GF(2^4)$，其全体非零元素构成循环群。设a是一个本原元，则$GF(2^4)$的循环群共有$\phi(2^4-1)=\phi(15)=8$个本原元：

$$a,a^2,a^4,a^7,a^8,a^{11},a^{13},a^{14}$$

4个5阶元素

$$a^3,a^6,a^9,a^{12}$$

两个3阶元素

$$a^5,a^{10}$$

Fermat定理说明，$GF(p^n)$上的每一个元素都满足$x^{p^n}-x=0$，其中$x^{p^n}-x$是$GF(p)$上的首1多项式。但是$GF(p^n)$的元素除了满足这一多项式外，还可能满足其他次数更低的多项式。由此导出最小多项式和本原多项式的概念。

定义 3.10 $GF(p^n)$的任一元素a的最小多项式是以a为根的次数最低的$GF(p)$上的首1多项式，记作$M(x)$。本原元的最小多项式称为本原多项式。

考查由$GF(2)$上的既约多项式x^4+x+1扩成的有限域$GF(2^4)$。设a是一个本原元，$GF(2^4)$的部分元素的最小多项式如下：

$$\begin{array}{ccccc} 0 & \leftrightarrow & 0 & \leftrightarrow & M(x)=x \\ 1 & \leftrightarrow & 1 & \leftrightarrow & M(x)=x+1 \\ x & \leftrightarrow & a & \leftrightarrow & M(x)=x^4+x+1 \\ x^3 & \leftrightarrow & a^3 & \leftrightarrow & M(x)=x^4+x^3+x^2+x+1 \\ x^2+x & \leftrightarrow & a^5 & \leftrightarrow & M(x)=x^2+x+1 \end{array}$$

3.3.3 有限域上的多项式在高级数据加密标准(AES)中的应用

AES进行加解密数据处理的数据单位主要为字节和字(4个字节)。为了能够进行字节和字的加法、乘法等运算，AES采用有限域的多项式表示法来表示字节和字。具体地，AES采用$GF(2)$上的既约多项式

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

作为运算模，用其余式构成$GF(2^8)$。这样，一个字节就可视为一个多项式，并视为$GF(2^8)$中的一个元素。字节的相加定义为$GF(2)$上多项式的相加。字节的相乘定义为$GF(2)$上多项式的相乘，并取模$m(x)$。

例如，字节$9BH+6FH$就可表示为如下的多项式加

$$(x^7+x^4+x^3+x+1)+(x^6+x^5+x^3+x^2+x+1)=x^7+x^6+x^5+x^4+x^2$$

上述多项式系数相加

$$(10011011)\oplus(01101111)=(11110100)=F4H$$

又如

$$(x^6+x^4+x^2+x+1)+(x^7+x+1)=x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1$$

而

$$x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1 \quad mod \quad x^8+x^4+x^3+x+1 = x^7+x^6+1$$

这恰好完成了字节$57H \times 83H = C1H$的运算。

AES定义了$GF(2^8)$上的一个倍乘函数$xtime(x)$，用以实现字节的按模移位：

$$xtime(x) = x \cdot f(x) \quad mod \quad x^8+x^4+x^3+x+1$$

例如，设字节为$57H$，则

$$\begin{aligned} xtime(57) &= x(x^6+x^4+x^2+x+1) \\ &= (x^7+x^5+x^3+x^2+x) \quad mod \quad (x^8+x^4+x^3+x+1) \\ &= x^7+x^5+x^3+x^2+x = AEH \end{aligned}$$

这就实现了把字节$57H$循环左移一位。用向量表示为$xtime(01010111) = (10101110)$。

在AES中4个字节定义为一个字，若要实现按字节操作的字处理，需要引入$GF(2^8)$上的多项式，即系数取自有限域$GF(2^8)$元素的多项式为$GF(2^8)$上的多项式。这样，一个4字节的字便与一个次数小于4的$GF(2^8)$上的多项式相对应。为了进行字处理，AES定义了字的相加和相乘。

设$a(x) = a_3x^3+a_2x^2+a_1x+a_0, b(x) = b_3x^3+b_2x^2+b_1x+b_0$是$GF(2^8)$上的多项式，定义$a(x)$与$b(x)$相乘模$x^4+1$的积为$c(x) = c_3x^3+c_2x^2+c_1x+c_0$：

$$c(x) = a(x) \cdot b(x) \quad mod \quad x^4+1$$

其中，$c(x)$的系数由下面4个式子得到：

$$\left.\begin{aligned} c_0 &= a_0 \cdot b_0 \oplus a_3 \cdot b_1 \oplus a_2 \cdot b_2 \oplus a_1 \cdot b_3 \\ c_1 &= a_1 \cdot b_0 \oplus a_0 \cdot b_1 \oplus a_3 \cdot b_2 \oplus a_2 \cdot b_3 \\ c_2 &= a_2 \cdot b_0 \oplus a_1 \cdot b_1 \oplus a_0 \cdot b_2 \oplus a_3 \cdot b_3 \\ c_4 &= a_3 \cdot b_0 \oplus a_2 \cdot b_1 \oplus a_1 \cdot b_2 \oplus a_0 \cdot b_3 \end{aligned}\right\}$$

注意，由于是模x^4+1，所以取模后获得循环移位。

在AES中要对4个字节的字进行列混淆变换，列混淆变换把4个字节的字看作$GF(2^8)$上的多项式$b(x) = b_3x^3 + b_2x^2 + b_1x + b_0$，然后与一固定多项式$c(x)$相乘并模多项式$x^4 + 1$：

$$b(x)c(x) \quad mod \quad x^4 + 1$$

其中$c(x)$为

$$c(x) = 03x^3 + 01x^2 + 01x + 02$$

例如，$xc(x) \quad mod \quad x^4 + 1 = 01x^3 + 01x^2 + 02x + 03$，系数进行了循环移位。

因为$c(x)$与x^4+1是互素的，从而保证$c(x)$存在逆多项式$d(x)$，而$c(x)d(x) = 1 \quad mod \quad x^4 + 1$。只有逆多项式$d(x)$存在，才能正确进行解密。

第二部分

部分习题答案

3.4 群

1. 证明$(S_n, \cdot, 1)$为群。

证：设α, β, η为S_n中任意三个元素，i是S中的任一元素，则有

- $G1$：$[\alpha \cdot \beta] \cdot \eta(i) = \alpha \cdot [\beta \cdot \eta](i) = \alpha(\beta(\eta(i)))$
- $G2$：$[1 \cdot \alpha](i) = [\alpha \cdot 1](i) = \alpha(i)$
- $G3$：$[\alpha \cdot \alpha^{-1}](i) = [\alpha^{-1} \cdot \alpha](i) = i$，其中$\alpha^{-1}$为$\alpha$的逆映射

2. 证明例1-7中的$(Z_2^m, \oplus, 0)$为群。

证：设$\alpha = \{\alpha_1, \alpha_2, \cdots, \alpha_m\}, \beta = \{\beta_1, \beta_2, \cdots, \beta_m\}, \eta = \{\eta_1, \eta_2, \cdots, \eta_m\}$为$Z_2^m$中任意三个元素，则有

- $G1$：$(\alpha \oplus \beta) \oplus \eta = \alpha \oplus (\beta \oplus \eta) = \{\alpha_1 \oplus \beta_1 \oplus \eta_1, \cdots, \alpha_m \oplus \beta_m \oplus \eta_m\}$
- $G2$：$\alpha \oplus 0 = 0 \oplus \alpha = \alpha$
- $G3$：$\alpha \oplus \alpha = \{\alpha_1 \oplus \alpha_1, \cdots, \alpha_m \oplus \alpha_m\} = \{0, 0, \cdots, 0\} = 0$，即$\alpha$的逆即为本身

3. 设$\sigma = \begin{pmatrix} 12345678 \\ 73154682 \end{pmatrix}$，求$\sigma$在$S_8$中的逆$\sigma^{-1}$。

解：$\sigma^{-1}(7) = 1$，$\sigma^{-1}(3) = 2$，$\sigma^{-1}(1) = 3$，$\sigma^{-1}(5) = 4$，
$\sigma^{-1}(4) = 5$，$\sigma^{-1}(6) = 6$，$\sigma^{-1}(8) = 7$，$\sigma^{-1}(2) = 8$，
即$\sigma = \begin{pmatrix} 12345678 \\ 38254617 \end{pmatrix}$

3.5 环

1. 证明$(Z_n, \oplus_n, \otimes, 0, 1)$为环。

证：设$a \neq 0, b \neq 0, c \neq 0$为$Z_n$中任意三个元素，则有

- $R1$：$(Z_n, \oplus_n, 0)$是交换群
  - $G1 : (a \oplus_n b) \oplus_n c = a \oplus_n (b \oplus_n c)$
  - $G2 : 0 \oplus_n a = a \oplus_n 0 = a$
  - $G3 : a \oplus_n (-a) = (-a) \oplus_n a = 0$，即$a$的逆即为$a$的相反数
  - $G4 : a \oplus_n b = b \oplus_n a$
- $R2$：$(Z_n, \otimes_n, 1)$是半群
  - $G1 : (a \otimes_n b) \otimes_n c = a \otimes_n (b \otimes_n c)$

– $G2 : 1 \otimes_n a = a \otimes_n 1 = a$

- $R3$：$a \otimes_n (b \oplus_n c) = a \otimes_n b \oplus_n a \otimes_n c, (b \oplus_n c) \otimes_n a = b \otimes_n a \oplus_n c \otimes_n a$

2. 证明$(Z_p, \oplus_p, \otimes_p, 0, 1)$为域，这里$p$为素数

证：设$a \neq 0, b \neq 0, c \neq 0$为$Z_p$中任意三个元素，则有

- $R1$：$(Z_p, \oplus_p, 0)$是交换群

– $G1 : (a \oplus_p b) \oplus_p c = a \oplus_p (b \oplus_p c)$

– $G2 : 0 \oplus_p a = a \oplus_p 0 = a$

– $G3$ 因为$a \in Z_p$，则$a < p$，那么存在$x \in Z_p$使得$a + x = p$，即$a \oplus_p x = 0$，即a的逆存在

– $G4 : a \oplus_p b = b \oplus_p a$

- $R2$：$(Z_p^*, \otimes_p, 1)$是交换群

– $G1 : (a \otimes_n b) \otimes_n c = a \otimes_n (b \otimes_n c)$

– $G2 : 1 \otimes_n a = a \otimes_n 1 = a$

– $G3$: 因为p是素数，则$(a, p) = 1$，即存在两个元素x, y使得$ax + py = 1$，则有$ax = 1 - py$，即有$a \otimes_p x = 1$，即a的逆存在

– $G4 : a \otimes_p b = b \otimes_p a$

- $R3$：$a \otimes_p (b \oplus_p c) = a \otimes_p b \oplus_p a \otimes_p c, (b \oplus_p c) \otimes_p a = b \otimes_p a \oplus_p c \otimes_p a$

3. 证明有零因子的环不为域

证明：假设有零因子的环为域，设该有零因子的环为R，则有$a \neq 0, b \neq 0 \in R$使得$a \cdot b = 0$。

又因为R为域，则a存在逆，记作a^{-1}，使得$1 = a^{-1} \cdot a$。由于$b \neq 0$，两边同乘以b，有$b = a^{-1} \cdot a \cdot b = a^{-1} \cdot (a \cdot b) = 0$，这与$b \neq 0$矛盾。因此，假设不成立。则有零因子的环不为域。

3.6 域

1. 求下列各组$GF(2)$上的多项式组的最高公因式

- $f(x) = x^5 + x^4 + x^3 + x^2 + x + 1, g(x) = x^4 + x^2 + x + 1$
- $f(x) = x^5 + x^4 + x^2 + 1, g(x) = x^3 + x + 1$

解：

- $f(x) = g(x)(x + 1) + x^2 + x$

$g(x) = (x^2 + x)(x^2 + x) + x + 1$

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

因此$(f(x),g(x))=x+1$

- $f(x)=g(x)(x^2+x+1)+x^2$

$g(x)=x^2x+x+1$

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

$x+1=x+1$

$x=1\cdot x$

因此$(f(x),g(x))=1$

2. 写出$GF(2)$上多项式x^4+1为模的所有剩余类

解：共有16个剩余类：$0,1,x,x+1,x^2,x^2+1,x^2+x,x^2+x+1,x^3,x^3+1,x^3+x,x^3+x^2,x^3+x+1,x^3+x^2+1,x^3+x^3+x^2+x,x^3+x^2+x+1$

3. $p(x)=x^2+x+1$是$GF(2)$上的既约多项式，由$p(x)$扩成域$GF(2^2)$，写出其加法和乘法表

解：$GF(2^2)$中元素有$0,1,x,x+1$，则其加法表为

	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+ 1	x+1	x	1	0

其乘法表为

	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+ 1
x	0	x	x+1	1
x+ 1	0	x+1	1	x

4. * 设F是特征为p的域，a和b是F的任意两个元素，而n是非负整数，证明$(a+b)^{p^n}=a^{p^n}+b^{p^n}$。

证明：根据牛顿二项式定理，$(a+b)^{p^n}=\sum_{k=0}^{p^n}C_{p^n}^k a^k b^{p^n-k}$ 注意到其中$C_{p^n}^0=C_{p^n}^{p^n}=1$，而对于$1\le k\le p^n-1, C_{p^n}^k=\frac{p^n(p^n-1)\cdots(p^n-k+1)}{1\cdot2\cdot3\cdots k}$。因为$C_{p^n}^k$是正整数，$p$是素数，所以$\frac{p^{n-1}(p^n-1)\cdots(p^n-k+1)}{1\cdot2\cdot3\cdots k}$一定是整数，也就是说$p|C_{p^n}^k$，因此$C_{p^n}^k=0\ mod\ p$。

3.7 数论

1. 求(a,b)、$[a,b]$及使得$au+bv=(a,b)$的整数u,v：

(a) $a=72,\ b=-60$

(b) $a=168,\ b=-180$

解：

(a)

$$\begin{aligned}72 &= -60\times(-1)+12\\ -60 &= 12\times(-5)\end{aligned}$$

因此$(72,-60)=12$，$[72,-60]=\frac{|72\times(-60)|)}{(72,-60)}=360$

又$12=70\times 1+(-60)\times 1$，因此$u=1,v=1$

(b)

$$\begin{aligned}-180 &= 168\times(-1)-12\\ 168 &= 12\times 14\end{aligned}$$

因此$(168,-180)=12$，$[168,-180]=\frac{|168\times(-180)|)}{(168,-180)}=2520$

又$12=168\times(-1)+(-180)\times(-1)$，因此$u=-1,v=-1$

2. 解一次不定方程：

(a) $3x+92y=17$

(b) $42x+70y+105z=56$

解：

(a) 先计算$(3,92)$：

$$\begin{aligned}92 &= 3\times 30+2\\ 3 &= 2\times 1+1\\ 2 &= 2\times 1\end{aligned}$$

因此$(3,92)=1$，而$(3,92)|17$，所以方程有解。

又

$$\begin{aligned}1 &= 3-2=3-(92-3\times 30)\\ &= 3\times 31+92\times(-1)\end{aligned}$$

所以$x_0=31\times 17=527,y_0=(-1)\times 17=-17$，所以方程的解为$x=527+92t,y=-17-3t$，其中$t$为任意整数。

(b) 第一步：

- 计算$(42,70)$：

$$\begin{aligned}70 &= 42\times 1+28\\42 &= 28\times 1+14\\28 &= 14\times 2\end{aligned}$$

因此$(42,70)=14$，所以设$42x+70y=14w$，即$3x+5y=w$
又$(3,5)=1$，且$1=3\times 2+5\times(-1)$，所以$x_0=2w, y_0=-w$，则$x=2w+5t, y=-w-3t$，其中t为任意常数。

- 将$42x+70y=14w$代入原始方程得$14w+105z=56$，化简得$2w+15z=8$

又$(2,15)=1$，且$1=2\times(-7)+15\times 1$，所以$w_0=-7\times 8=-56, z_0=1\times 8=8$，则$w=-56+15s, z=8-2s$，其中$s$为任意常数。

- 因此该方程的解为$x=2(-56+15s)+5t=-112+30s+5t, y=-(-56+15s)-3t=56-15s-3t, z=8-2s$

3. 解一次同余方程：

(a) $24x\equiv 42(mod\,30)$

(b) $90x\equiv 21(mod\,429)$

解：

(a) 因为$(24,30)=6$，且$6|42$，所以方程有解
又$6=24\times(-1)+30\times 1$，所以$x_0\equiv(-1)\times 7\equiv -7\equiv 23(mod\,30)$，因此，方程的解为$x\equiv 23+\frac{30}{6}t\equiv 23+5t(mod\,30)$，其中$t=0,1,\cdots,5$

(b) 因为$(90,429)=3$，且$3|21$，所以方程有解
又$3=90\times 62+429\times(-13)$，所以$x_0\equiv 62\times 7\equiv 5(mod\,429)$，因此，方程的解为$x\equiv 5+\frac{429}{3}t\equiv 5+143t(mod\,429)$，其中$t=0,1,2$

4. 计算下列整数的阶$ord_m(a)$：

(a) $m=123,\ a=13$

(b) $m=2^7\times 3^4\times 7^2,\ a=13$

(c) $m=2^5\times 7^4,\ a=3^4$

解：

(a) $m=3\times 41$
又$13\equiv 1(mod\,3)$，则$ord_3(13)=1$
又$13^{40}\equiv 1(mod\,41)$，则则$ord_{41}(13)=40$

因此，$ord_{123}(13)=[1,40]=40$

(b) • 因为$13=2^2\cdot 3+1$，因此$ord_{2^7}(13)=2^{7-2}=2^5$

• 因为$13\not\equiv 1(mod\ 3^2), 13^2\not\equiv 1(mod\ 3^2), 13^3\equiv 1(mod\ 3^2)$，因此$ord_{3^2}(13)=3$。又$13^3-1=2196=2^2\times 3^2\times 61$，设$i=2, p=3$，满足$3^2|13^3-1$但$3^3\nmid 13^3-1$，所以$ord_{3^4}(13)=3^{4-2}\times 3=27$

• 又$ord_{7^2}(13)=14$，因此$ord_m(a)=[2^5,27,14]=6048$

(c) • 设$b=3^2=9=2^3+1$，所以$ord_{2^5}(b)=2^{5-3}=4$

• 又$ord_{7^4}(13)=1029$，所以$ord_m(b)=[4,1029]=4116$

• 因此$ord_m(a)=\frac{4116}{(2,4116)}=2058$

5. 计算下列素数的一个原根： 41， 61， 97 解：

• 对$p=41$，有$41-1=40=2^3\times 5$，取整数$a=7$，有$(7,41)=1$，且$7^{20}\not\equiv 1(mod\ 41), 7^8\not\equiv 1(mod\ 41)$，则$a=7$是41的一个原根。

• 对$p=61$，有$61-1=60=2^2\times 3\times 5$，取整数$a=2$，有$(2,61)=1$，且$2^{30}\not\equiv 1(mod\ 61), 2^{20}\not\equiv 1(mod\ 61), 2^{12}\not\equiv 1(mod\ 61)$，则$a=2$是61的一个原根。

• 对$p=97$，有$97-1=96=2^5\times 3$，取整数$a=5$，有$(5,97)=1$，且$7^{48}\not\equiv 1(mod\ 97), 7^{32}\not\equiv 1(mod\ 97)$，则$a=7$是97的一个原根。

6. 判断下列整数是否为素数：

(a) 67

(b) $73=2^3\times 3^2+1$

(c) $2543=62\times 41+1$

解：

• 由$\sqrt{p}=\sqrt{67}<\sqrt{81}=9$及小于9的素数$2,3,5,7$都不能整除67，由整数判别法得$p=67$是一个素数。

• $p-1=2^3\times 3^2$

取$p_1=2, a_1=3$，有$a_1^{73-1}\equiv 1(mod\ 73), a_1^{\frac{73-1}{2}}\not\equiv 1(mod\ 73)$
取$p_2=3, a_2=2$，有$a_2^{73-1}\equiv 1(mod\ 73), a_2^{\frac{73-1}{3}}\not\equiv 1(mod\ 73)$
根据莱梅判别法得$p=73$是一个素数。

• $p-1=62\times 41$，$q=41$是一个奇素数，且$2q+1=2\times 41+1=83>\sqrt{2543}$，又有$a=2$满足$a^{2543-1}\equiv 1(mod\ 2543)$，$a^{62}\not\equiv 1(mod\ 2543)$
根据普罗兹判别法得$p=2543$是一个素数。

3.8 逻辑学

1. 将下列命题符号化：

(a) 小王是游泳冠军或百米赛跑冠军。

(b) 如果我上街，我就去花店看看，除非我很累。

解：

(a) 用p表示“小王是游泳冠军”，q表示“小王是百米赛跑冠军”，则命题符号化为：$p \vee q$

(b) 用p表示“我上街”，q表示“我去花店”，r表示“我很累”，则命题符号化为：$p \to (q \wedge \neg r)$

2. 验证下列等值式：

(a) $((p \to q) \to r) \Leftrightarrow ((\neg q \wedge p) \vee r)$

(b) $((p \vee q) \to r) \Leftrightarrow ((p \to r) \wedge (q \to r))$

解：

(a)

$((p \to q) \to r)$ //前提式

$\Leftrightarrow ((\neg(p \to q)) \vee r)$ //E-PL12

$\Leftrightarrow ((\neg((\neg p) \vee q)) \vee r)$ //E-PL12

$\Leftrightarrow ((p \wedge (\neg q)) \vee r)$ //E-PL6

$\Leftrightarrow ((\neg q \wedge p) \vee r)$

(b)

$((p \vee q) \to r)$ //前提式

$\Leftrightarrow ((\neg(p \vee q)) \vee r)$ //E-PL12

$\Leftrightarrow (((\neg p) \wedge (\neg q)) \vee r)$ //E-PL6

$\Leftrightarrow (((\neg p) \vee r) \wedge ((\neg q) \vee r))$ //E-PL5

$\Leftrightarrow ((p \to r) \wedge (q \to r))$ //E-PL12

3. 将下列命题符号化：

(a) 每一个有理数都是实数。

(b) 没有不犯错误的人。

(c) 任何金属均可溶解于某种液体中。

解：

(a) 令谓词$Q(x)$表示“x是有理数”，$F(x)$表示“x是实数”，则命题表示

为：$(\forall x)(Q(x) \rightarrow F(x))$

(b) 令谓词$Q(x)$表示"人x犯错误"，则命题表示为：$\neg((\exists x)Q(x))$

(c) 令谓词$Q(x,y)$表示"金属x可溶解于液体y"，则命题表示为：$(\forall x)((\exists y)Q(x,y))$

4. 将下列公式翻译成自然语言，并确定其真值，这里假定个体域是正整数：

(a) $(\forall x)(\exists y)G(x,y)$，其中$G(x,y)$表示$x \times y = y$。

(b) $(\forall x)(\exists y)F(x,y)$，其中$M(x,y)$表示$x \times y = 1$。

解：

(a) "任意x，存在y，使得$x \times y = y$"，真值为0。

(b) "任意x，存在y，使得$x \times y = 1$"，真值为1。

5. 将下列命题符号化，并研究其推理是否正确：

每一个大学生不是文科生就是理科生；有的大学生是优等生；小张不是文科生但他是优等生。因此，如果小张是大学生，它就是理科生。

解：引入谓词：

$P(x)$表示"x是大学生"，$Q(x)$表示"x是文科生"，$R(x)$表示"x是理科生"，$S(x)$表示"x是优等生"。

前提可以符号化为：$\forall x(P(x \rightarrow (Q(x) \vee R(x))))$、$\exists x S(x)$、$(\neg Q(a) \wedge S(a))$，结论符号化为：$P(a) \rightarrow R(a)$，验证该结论的公式序列为：

(a) $\forall x(P(x) \rightarrow (Q(x) \vee R(x)))$ //前提

(b) $P(c) \rightarrow (Q(c) \vee R(c)$ //R-UI

(c) $(\neg P(c)) \vee (Q(c) \vee R(c))$ //E-PL12

(d) $(\neg Q(a) \wedge S(a))$ //前提

(e) $\neg Q(a)$ //T-FL2

(f) $(\neg P(a)) \vee R(a))$ //(c)、(e)

(g) $P(a) \rightarrow R(a)$ //E-PL12

因此，上述推理正确。