应用密码学（第四讲） — 密码数学基础补充

林东岱

信息安全国家重点实验室

2022年9月

本节概要

数论基础

定义 1 (整除、因子)

设$a, b(b \neq 0)$是两个整数，如果存在另一整数c，使得$a = b \cdot c$, 则称b整除a，或称a被b整除，记作$b|a$, 并称b是a的因子。

一个大于1的正整数，如果只有因子1和它本身，则称该整数为素数。

定理 1

对任意正整数$a > 1$,一定存在互不相同的素数$p_1, p_2, \cdots, p_t$和正整数$a_1, a_2, \cdots, a_t$, 使得

$$a = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$$

且如果不考虑素数的次序，上述分解是唯一的。

定理 2

素数的个数是无穷的。

定义 2

对于正整数a, b, 如果正整数d满足$d|a$且$d|b$, 则称d是a和b的公因子。a和b的所有公因子中最大者称为a和b的最大公因子, 记为$\gcd(a, b)$，或简单记作(a, b). 特别，若a, b的最大公因子为1，则称a和b两数是互素的。

对于正整数a, b, 如果正整数m满足$a|m$且$b|m$, 则称m是a和b的公倍数。a和b的所有公倍数中最小者称为a和b的最小公倍数, 记为lcm(a, b)，或简记为$[a, b]$.

显然有：

- $\gcd(a, b) = \gcd(b, a) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b) = \gcd(a, a - b)$
- $\gcd(0, a) = a$.
- 设$a = \prod_p p^{a_p}, b = \prod_p p^{b_p}$是$a$和$b$的素数分解。令$d_p = \min(a_p, b_p)$, $m_p = \max(a_p, b_p)$, 则

$$(a, b) = \prod_p p^{d_p}, \quad [a, b] = \prod_p p^{m_p}$$

欧几里德算法

更相减损术:

“子之数，以少减多，更相减损，求其等也”

— 《九章算术》

算法 1 (辗转相除法, 欧几里德算法)

Euclid(a,b):

1. $X \leftarrow a$; $Y \leftarrow b$;
2. If $Y = 0$ then return X;
3. $R = X \bmod Y$;
4. $X = Y$;
5. $Y = R$;
6. Goto 2;

Example 1

求gcd(68, 28)

$$68 = 2 \times 28 + 12, \quad \gcd(28, 12)$$
$$28 = 2 \times 12 + 4, \quad \gcd(12, 4)$$
$$12 = 3 \times 4 + 0, \quad \gcd(4, 0)$$

所以$\gcd(68, 28) = 4$.

定理 3

任给正整数$a, b \in \mathbb{Z}^+$，令$d = \gcd(a, b)$，则一定存在$\alpha, \beta \in \mathbb{Z}$，使得

$$d = \alpha \cdot a + \beta \cdot b$$

证明：
令$S = \{ax + by | x, y \in \mathbb{Z}\}$，则$S$中一定存在非负整数，令$d$是$S$中最小的非负整数，则$d = \gcd(a, b)$.

推论 1

任给正整数$a, b \in \mathbb{Z}^+$, a和b互素当且仅当存在$\alpha, \beta \in \mathbb{Z}$, 使得

$$1 = \alpha \cdot a + \beta \cdot b$$

推论 2

任给正整数$a, b \in \mathbb{Z}^+$, 则:

1) 对a, b的任一个公因数c, 一定有$c|(a, b)$;
2) 对a, b的任一个公倍数m, 一定有$[a, b]|m$.

Example 2

求α, β, 满足$\gcd(68, 28) = 68\alpha + 28\beta$. 重新观察例1中的计算，我们有

$12 = 68 - 2 \times 28$

$4 = 28 - 2 \times 12 = 28 - 2 \times (68 - 2 \times 28) = (-2) \times 68 + 5 \times 28$

模运算 I

设n是一正整数，$a \in \mathbb{Z}^+$. 如果用n去除a, 则我们可得下列等式

$$a = qn + r, 0 \le r < n$$

其中$a = \lfloor a/n \rfloor$为小于或等于a/n的最大整数。用$a \bmod n$表示余数r. 如果$(a \bmod n) = (b \bmod n)$, 则称$a$和$b$模$n$同余，记为$a \equiv b \bmod n$或$a \equiv_n b$. 称与$a$模$n$同余的数的全体为$a$的同余类，记作$[a]$, 称$a$为这个同余类的代表元。

定理 4

- $a \equiv b \bmod n \Leftrightarrow n|(a-b)$;
- $a \equiv a \bmod n$;
- 若$a \equiv b \bmod n$, 则$b \equiv a \bmod n$;
- 若$a \equiv b \bmod n$, $b \equiv c \bmod n$, 则$a \equiv c \bmod n$.

模运算 II

定义 3 (乘法逆)

对于给定的$a \in \mathbb{Z}$，若存b使得$ab \equiv 1 \bmod n$，则称b是a模n的乘法逆。

定理 5

1. 一个整数存在模n的乘法逆的充要条件是该整数与n互素。求一个整数的乘法逆可用扩展的欧几理德算法。
2. 如果$ab \equiv ac \bmod n$且$(a, n) = 1$，那么$b \equiv c \bmod n$.

定义 4 (Euler函数)

设n是一正整数，小于n且与互素的正整数的个数称为n的欧拉*(Euler)*函数，记为$\phi(n)$.

例：$\phi(7) = 6, \phi(8) = 4$，$\phi(10) = 4$. 若p是素数，则显然有$\phi(p) = p - 1$.

定理 6 (Euler定理)

对于正整数$a,n\in\mathbb{Z}^+$，若$(a,n)=1$，则

$$a^{\phi(n)}\equiv 1 \bmod n$$

证明：设$\mathbb{Z}_n^*:=\{x_1,x_2,\cdots,x_{\phi(n)}\}$是由所有小于$n$且与$n$互素的正整数的全体组成的集合。 定义$S:=\{ax_1(\bmod n),ax_2(\bmod n),\cdots,ax_{\phi(n)}(\bmod n)\}$，则容易证明$S=\mathbb{Z}_n^*$. 所以

$$\prod_{i=1}^{\phi(n)} ax_i\equiv\prod_{i=1}^{\phi(n)} x_i \bmod n\Rightarrow a^{\phi(n)}\equiv 1\bmod n.$$

□

推论 3 (Fermat定理)

设p是一素数，对任一$a\in\mathbb{Z}^+$，如果$(a,p)=1$，则一定有$a^p\equiv a\bmod p$.

定理 7

若$(m,n)=1$, 则必有
$$\mathbb{Z}_{mn}=\{my+nx|x\in\mathbb{Z}_m, y\in\mathbb{Z}_n\}.$$

证明：我们只需证明mn个数$\{my+nx|x\in\mathbb{Z}_m, y\in\mathbb{Z}_n\}$中没有两者相同即可。假设
$$my+nx\equiv my'+nx' \pmod{mn}$$
则
$$my\equiv my' \pmod{n}$$
$$nx\equiv nx' \pmod{m}$$
由于$(m,n)=1$, 所以有
$$y\equiv y' \pmod{n}, x\equiv x' \pmod{m}$$
从而定理得证。□

定理 8

若$(m,n)=1$, 则$\phi(mn)=\phi(m)\phi(n)$.

证明：设$\mathbb{Z}_m^*=\{x_1,x_2,\cdots,x_{\phi(m)}\}$, $\mathbb{Z}_n^*=\{y_1,y_2,\cdots,y_{\phi(n)}\}$. 下面我们证明$\mathbb{Z}_{mn}^*=\{my+nx|x\in\mathbb{Z}_m^*,y\in\mathbb{Z}_n^*\}$.
首先，$(my+nx,mn)=1$. 否则，必有一素数p, 使得

$$p|(mn,my+nx).$$

假定$p|m$, 则$p|nx$. 因$(m,n)=1$, 所以$(p,n)=1$, 从而$p|x$, 即$p|(m,x)$, 但根据x的选取，这是不可能的。
其次凡与mn互素之数a，必与形如

$$my+nx,\qquad (x,m)=(y,n)=1$$

之数$\pmod{mn}$同余.

由定理7知，必有整数x, y使

$$a \equiv my + nx \pmod{mn}.$$

今证$(x, m) = (y, n) = 1$. 若$(x, m) = d \neq 1$, 则

$$(a, m) = (my + nx, m) = (nx, m) = (x, m) = d \neq 1.$$

此与假设矛盾。同法可证$(n, y) = 1$. □

定理 9

设

$$n = \prod_{i=1}^{k} p_i^{e_i}$$

其中p_i是互不相同的素数，则

$$\phi(n) = \prod_{i=1}^{k} (p_i^{e_i} - p_i^{e_i - 1}) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i})$$

同余方程

今往讨论同余方程

$$ax + b \equiv 0 \pmod m \tag{1}$$

在何时有解，有几个解。
若$(a, m) = 1$, 则存在α, β, 使

$$a\alpha + m\beta = 1.$$

故$x = -b\alpha$即为方程(1)的一个解。下证唯一性。若

$$ax' + b \equiv 0 \pmod m, ax + b \equiv 0 \pmod m$$

则

$$a(x - x') \equiv 0 \pmod m$$

由于$(a, m) = 1$, 所以

$$x \equiv x' \pmod m.$$

若$(a,m)=d>1$, 则d必须整除b, 不然无解。如些得

$$\frac{a}{d}x+\frac{b}{d}\equiv 0(\bmod \frac{m}{d}),(\frac{a}{d},\frac{m}{d})=1. \tag{2}$$

根据上面的讨论，(2)式有唯一解x_1满足$0\leq x_1<\frac{m}{d}$. 而

$$x=x_1+\frac{m}{d}t$$

皆为(2)式之解。故对模m,

$$x_1,x_1+\frac{m}{d},x_1+2\frac{m}{d},\cdots,x_1+(d-1)\frac{m}{d}$$

皆不同余，且均适合方程(1)。

定理 10

若$(a,m)|b$, 则方程*(1)*有(a,m)个模m互不同余的解。不然，则无解。

中国剩余定理

“物不知其数”问题: 今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？（《孙子算经》）

求解口诀：

三人同行七十稀，五树梅花廿一枝，
七子团圆正半月，除百零五便得知。

即用70乘以用3除所得余数，加上21乘以用5除所得余数，加上15乘以用7除所得余数，其总各用105的倍数减之。

$$2 \times 70 + 3 \times 21 + 2 \times 15 = 233 \equiv 23 \pmod{105}$$

“物不知其数”问题用现在的数学语言来描述，就是求正整数x,使下列同余方程成立：

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

定理 11 (中国剩余定理)

设$m_1, m_2, \cdots, m_k$是k个两两互素的正整数，$M = m_1 m_2 \cdots m_k$. 则一次同余方程

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \qquad \vdots \\ x \equiv a_k \bmod m_k \end{cases} \tag{3}$$

则存在唯一小于M的解

$$x = \frac{M}{m_1} \cdot e_1 a_1 + \frac{M}{m_2} \cdot e_2 a_2 + \cdots + \frac{M}{m_k} \cdot e_k a_k \bmod M$$

其中$\frac{M}{m_i} \cdot e_i \equiv 1 \bmod m_i, 1 \leq i \leq k$.

证明：设
$$M_i = \frac{M}{m_i} = \prod_{l=1, l\neq i}^{k} m_l, i = 1, 2, \cdots, k$$
由M_i的定义可知$(M_i, m_i) = 1$, 所以M_i在模m_i下，有唯一的乘法逆元e_i, 即:
$$\frac{M}{m_i} \cdot e_i \equiv 1 \bmod m_i$$
由于对任何$i \neq j$, $m_i | M_j$, 所以容易看出：
$$x \equiv a_i (\bmod m_i), i = 1, 2, \cdots, k$$
因此只需证在模M的意义下，解是唯一的即可。假设有另外一解y, 即
$$y \equiv a_i (\bmod m_i), i = 1, 2, \cdots, k$$
所以
$$x - y \equiv 0 (\bmod m_i), \quad m_i | x - y, i = 1, 2, \cdots, k.$$
鉴于m_i两两互素，所以有$M | x - y$, 从而$x \equiv y (\bmod M)$.

中国剩余定理

例： 求下列同余方程的解

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 2 \bmod 7 \end{cases} \tag{4}$$

解：$M = 3 \cdot 5 \cdot 7 = 105$, $M_1 = 35, M_2 = 21, M_3 = 15$. 易知

$$e_1 = M_1^{-1} \equiv 2 \bmod 3$$

$$e_2 = M_2^{-1} \equiv 1 \bmod 5$$

$$e_3 = M_3^{-1} \equiv 1 \bmod 7$$

所以

$$x \equiv 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 \pmod{105} = 23$$

课程练习

1. 试编写一段程序实现求解定理3中α，β和gcd(a,b)的扩展欧几里德算法。
2. 试证同余方程
$$a_1x_1+\cdots+a_nx_n\equiv b(\operatorname{mod} m)$$
有解$(x_1,\cdots,x_n)$之充分必要条件为
$$(a_1,\cdots,a_n,m)|b.$$
若此条件适合，则其解的个数（对模m不同余者）为
$$m^{n-1}(a_1,\cdots,a_n,m).$$
3. 二数余一，五数余二，七数余三，九数余四，问本数。

本节概要

群的基本概念

设S是一非空集合，我们把$S \times S \to S$的一个映射$\circ$称为S上的(二元)运算,而把$a, b \in S$的像$\circ(a, b)$记做$a \circ b$，或省略$\circ$，只简单地写作ab.

定义 5

我们说一个非空集合G对于G上的一个二元运算$\circ$来说作成一个群，如果：

1) $\circ$是结合的，即对任何$a, b, c \in G, a \circ (b \circ c) = (a \circ b) \circ c$
2) G中存在一个元素e满足：$\forall a \in G, a \circ e = e \circ a = a$。这个元素称为$G$中的单位元
3) 对$\forall a \in G$,存在一个元素$a^{-1} \in G$满足$a \circ a^{-1} = a^{-1} \circ a = e$, 称为$a$的逆元

如果G中的元素还满足:

4) 对$\forall a, b \in G$, $a \circ b = b \circ a$, 则G称为交换群或Abel群。（这时也把$\circ$表示成+），因此也称为加法群。

容易证明在一个群中，单位元和元素的逆元是唯一的，而且对$\forall a, b \in G, (a \circ b)^{-1} = b^{-1} \circ a^{-1}$. 我们约定：

$a^0 = e$

$a^n = \underbrace{a \circ a \circ \ldots \circ a}_{\text{（n个）}}$ 或$na = \underbrace{a + a + \ldots + a}_{\text{（n个）}}$

$a^{-n} = (a^{-1})^n$

显然有:

$a^n a^m = a^{m+n}, (a^n)^m = a^{mn}$

Example 3

所有整数的集合在加法运算下构成一个交换群。

Example 4

只含有一个元素e的集合在运算$e * e = e$下构成一个群。

定义 6 (有限群、子群、循环群)

1) 一个群G称作有限群（无限群）如果G中含有有限多个元素（无限多个元素）。 有限群中元素的个数称为G的阶，用$|G|$表示。
2) 群G的一个子集H，如果在G的运算下，仍构成一个群, 则称H为G一个子群。
3) 一个群G称为循环群，如果存在一个元素$a \in G$使得$\forall b \in G$, 存在整数t满足$b = a^t$。这样的元素a称为G的生成元。记作$G = \langle a \rangle$.

定义 7 (元素的阶)

$\forall a \in G$,定义$\langle a \rangle = \{a^i | i \in \mathbf{Z}\}$. 则$\langle a \rangle$为子群。如果$\langle a \rangle$是有限群则$\langle a \rangle$的阶也称为$a$的阶，否则称$a$为无限阶的。

显然一个元素a的阶k是满足$a^k = e$的最小的正整数。

定义 8 (等价关系)

$R \subset S \times S$称为等价关系，如果：
a) $(s, s) \in R$ （自反性）；
b) $(s, t) \in R \Rightarrow (t, s) \in R$ （对称性）；
c) $(s, t), (t, u) \in R \Rightarrow (s, u) \in R$ （传递性）；

显然模整数n的同余关系是一个等价关系。将$\mathbf{Z}$分成n个等价类$[0], [1], [2], ..., [n-1]$.

Example 5

$\{[0], [1], [2], ..., [n-1]\}$在运算$[a]+[b]=[a+b]$下构成一个加法群，称为模$n$的整数群。记作$\mathbf{Z}_n$.

显然，$\mathbf{Z}_n$是一个循环群。$\mathbf{Z}_n = \langle [1] \rangle$，而且任何一个与n互素的整数t，$[t]$都是$\mathbf{Z}_n$的生成元。

定理 12 (lagrange定理)

对于一个有限群G, 其任何一个子群H的阶整除群G的阶，任一元素的阶也整除G的阶。

定理 13

1) 任意循环群的子群仍是循环群。
2) 在一个阶为m的有限阶循环群$\langle a\rangle$中，a^k生成一个阶为$\frac{m}{gcd(k,m)}$的子群。
3) 设f是有限循环群$\langle a\rangle$的阶的正因子，则$\langle a\rangle$中有$\phi(f)$个阶为f的元素。$\phi(f)$是Euler函数即 与f互素的整数的个数。
4) 阶为m的有限循环群$\langle a\rangle$正好有$\phi(m)$个生成元，即a^r满足$\langle a^r\rangle = \langle a\rangle$.这些生成元形为$a^r$, 其中$(r, m) = 1$.

定义 9

设$f: G \to H$是群G到群H的一个映射。如果$\forall a, b \in G, f(a \cdot b) = f(a) \cdot f(b)$则称$f$为$G$到$H$的同态。进一步如果$f(G) = H$,则称$f$为满同态(或称$f$为$G$到$H$上的同态), 这时$H$称为$G$的同态像；如果$f$是单射，则称$f$为单同态映射；如果$f$是一一对应， 则称$f$为同构映射，这时称$G$和$H$是同构的， 记做$G \cong H$。$G$到$G$自身的同构映射称为自同构。

同态映射总是把单位元映到单位元，把逆元素映射成像的逆元素。

例 1 (内自同构)

设G是群。$\forall a \in G$，定义f_a: $f_a(b) = aba^{-1}, b \in G$. 则$f_a$称为群$G$的由$a$定义的内自同构，而把一个元素在内自同构下的像称为该元素的 共轭元。显然群中元素的共轭关系是一个等价关系。

本节概要

定义 10

一个集合R称为一个环，如果R有两个运算$+$和$\cdot$满足：
1. $(R,+)$是一个交换群。
2. $\cdot$是结合的，即$(a\cdot b)\cdot c=a\cdot(b\cdot c)$.
3. 满足分配率：即对任何$a,b,c\in R, a(b+c)=ab+ac,(b+c)a=ba+ca$.

定义 11

1. 一个环称为有单位元的，如果它有乘法单位元。
2. 一个环称为交换环，如果其中的乘法运算是交换的。
3. 一个环称为整环，如果它是一个交换的有单位元的环且$e\neq 0$,对于任意的$a\neq 0, b\neq 0, \Rightarrow ab\neq 0$.
4. 一个环称为除环，如果所有非零元在乘法运算$\cdot$下构成一个群。
5. 一个交换的除环称为域。

定义 12

环R的一个子集S称为R的一个子环，如果S关于$+$和$\cdot$是封闭的并且在这两种运算下形成一个环。

定义 13

环R的一个子集J称为一个理想，如果J是R的一个子环并且对所有$a \in J$，$r \in R$,有$ar \in J$和$ra \in J$.

Example 6

1) 设R为有理数域，则整数集**Z**是R的子环，但不是理想。 因为$1 \in \mathbf{Z}$, $\frac{1}{2} \in Q$,但是$\frac{1}{2} \cdot 1 = \frac{1}{2} \notin \mathbf{Z}$.
2) 设R为交换环，$a \in R$, 则包含a的最小理想$(a) = \{ra + na : r \in R, n \in \mathbf{Z}\}$.如果R包含一个单位元，则$(a) = \{ra : r \in R, \}$

定义 14

R是一个交换环，R的一个理想J称为主理想，如果存在$a \in R$使得$J = (a)$.这时，J也称为由a生成的主理想。

定义 15

设R是一整环。如果R中的每一个理想都是主理想，则称R是主理想整环。

定义 16

设$P \neq R$是R的一个理想，如果$ab \in P \Rightarrow a \in P$或$b \in P$, 则称$P$为素理想。

$M \neq R$是R的一个理想。如果J是R的理想且$M \subset J \Rightarrow J = R$或$J = M$, 则称$M$是极大理想。

Example 7

1) R为任意运算为+的Abel群，对$a, b \in R$, 定义$ab = 0$.则R为环。
2) 所有的整数在通常数的加法和乘法运算下形成一个整环，称为整数环。整数环是一主理想整环。
3) 所有偶数在通常数的加法和乘法运算下形成一个没有单位元的交换环。
4) 所有从实数到实数的映射按照运算 $(f+g)(x) = f(x)+g(x)$, $(fg)(x) = f(x)g(x)$, $\forall x \in R$. 形成一个有单位元的交换环。
5) $\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\}$, $a, b, c, d \in R$按照矩阵的加法和乘法构成有单位元的环。
6) 所有的有理数在通常数的加法和乘法运算下构成一域，称为有理数域。
7) 模n的剩余类环$\mathbf{Z}_n = \mathbf{Z}/(n)$.

商环

设J是环R的一个理想，则我们可以定义环R中元素的等价关系$\sim$:

$$a \sim b \Longleftrightarrow a - b \in J.$$

该等价关系将环R分成了一些互不相交的等价类的并，每个等价类叫作模J的剩余类。 剩余类中的元素记为$[a] = a + J$(因为里面的元素都是具有形式$a + c, c \in J$).

可以直接验证，环R模J的剩余类按运算

$(a + J) + (b + J) = (a + b) + J$

$(a + J)(b + J) = ab + J$

可以形成一个环。

定义 17 (商环)

按上述运算所作成的剩余类环称为R模J的剩余类环(或商环)，记作R/J.

定义 18 (同态、同构)

设R,S为环，$a,b \in R$. 一个映射$\varphi : R \to S$称为环同态, 如果：

1) $\varphi(a+b) = \varphi(a) + \varphi(b)$
2) $\varphi(ab) = \varphi(a)\varphi(b)$

而集合$ker\varphi = \{a \in R : \varphi(a) = 0 \in S\}$称为同态映射$\varphi$的核. 一个同态映射，如果既是单的又是满的，则称为同构映射。如果两个环之间存在同构映射，我们则说这 两个环是同构的，用$\cong$表示。

定理 14 (同态基本定理)

设R和S是环。如果$\varphi : R \to S$是满同态，则$ker\varphi$为R的理想，且$S \cong R/ker\varphi$. 反过来，如果J为R的理想，定义映射$\varphi(a) = a + J, a \in R$. 则映射$\varphi : R \to R/J$是满同态且$ker\varphi = J$.

定理 15

设*R*是一个有单位元的交换环，则：
1) 理想*M*是极大理想$\Leftrightarrow R/M$是域。
2) 理想*P*是素理想$\Leftrightarrow R/P$是整环。
3) 每个极大理想都是素理想。
4) 如果*R*是主理想整环，则$R/(c)$是域$\Leftrightarrow c$是*R*中的素元。

证明：
1) $\Rightarrow$，如果M是极大理想。$\forall a \notin M$，则$J = \{ar+m|r \in R, m \in M\}$是一个理想且$J \supsetneq M$，从而$J = R$. 所以$\exists r \in R, m \in M$使得$ar+m=1$，因此$\overline{a} \cdot \overline{r} = \overline{1}$. 所以$R/M$是域。
$\Leftarrow$，假设R/M是域， 假设$J \supseteq M$，$J \neq M$，则存在$a \in J$，$a \notin M$，所以$\overline{a} \neq 0$. 设$\overline{a}$的逆元$\overline{r}$，即$(a+M)(r+M) = 1+M$. 所以$ar+m=1$对某些$m \in M$. 又因为$m \in M \subseteq J, a \in J$,所以 $ar+m \in J$，所以$1 \in J$，从而$J = R$.

2) $\Rightarrow$，假设P是素理想，则R/P是一个交换环。单位元为$\bar{1}=1+P\neq 0+P$. 假设$(a+P)(b+P)=0+P\Rightarrow ab+P=0+p$, 所以$ab\in P$, 从而$a\in P$或$b\in P$ 即$\bar{a}=0$或$\bar{b}=0$. 所以 R/P没有零因子。
$\Leftarrow$, 设$ab\in P$, 所以$\bar{a}\bar{b}=0$. 所以$\bar{a}=0$或$\bar{b}=0$, 即 $a\in P$或$b\in P$。
3) 由1)和2)即得。
4) $\Rightarrow$，如果$R/(c)$是域，则c不是单位（否则，$R/(c)=0$, 不是域）。假设c不是素元， 则c有一因子a既不是单位也不是c的 相伴元素。($a\neq 0$, 否则$c=0$, 从而a和c相伴). 记$c=a\cdot b$, $b\in R$. 我们有$a\notin(c)$, 否则$a=c\cdot d=abd$. 所以$a(1-bd)=0$, 由于R是整环。所以$(1-bd)=0$，即b和d 为单位，所以a和c相伴，矛盾。从而$(a)\supset(c)$, 这与由1)得出的(c)是极大理想矛盾。
$\Leftarrow$, 假设c是素的，则$(c)\neq R$。假设$J\supset(c)$是R的一个理想，由于R是主理想整环，所以$\exists a\in R, J=(a)$. 所以a或者是单位或者与c相伴。所以$J=R$或$J=(c)$，所以(c)是极大的。从而$R/(c)$是域。

推论 4

$\mathbf{Z}_p=\mathbf{Z}/(p)$是域$\Leftrightarrow$ p是素数。$\mathbf{Z}_p$也称为阶为p的*Galois*域

定义 19 (环的特征)

设R是任一环，如果存在正整数n使得对任何$r \in R$,$n \cdot r = 0$. 且对任何小于n的正整数n', $n' \cdot r \neq 0$, 则称n为环R的特征， 否则则称R的特征为0。

定理 16

域的特征或者是0, 或者是一素数。特别，有限域的特征一定是一素数。

定义 20 (子域、扩域)

设F是域，K是F的子集。如果K在F的运算下也构成一个域则称K为F的子域，而F则称为K的扩域。 如果$K \neq F$则称K为F的真子域。

一个域如果不包含任何子域，则称为素域。如果一个域F的子域作为域是素域，则称该子域为F的素子域。

多项式环 I

定义 21

由系数在R中的多项式组成的环称为R上的多项式环，记为$R[x]$.

定理 17

假设R是一个环，则：

1) $R[x]$是交换的$\Leftrightarrow R$是交换的。
2) $R[x]$有单位元$\Leftrightarrow R$有单位元。
3) $R[x]$是一个整环$\Leftrightarrow R$是整环。

特别当R是一个域F时，$F[x]$是一个整环。

定理 18 (除法)

$g \neq 0,\ g \in F[x]$, 则对任何$f \in F[x]$, $\exists q, r \in F[x]$, 满足$f = g \cdot q + r, \deg(r) < \deg(g)$.

多项式环 II

Example 8

$f(x)=2x^5+x^4+4x+3\in F_5[x]$, $g(x)=3x^2+1\in F_5[x]$.

答案：$q(x)=4x^3+2x^2+2x+1, r(x)=2x+2$.

定理 19

$F[x]$是主理想整环。事实上对任何$J\neq(0)\subset F[x]$, 存在唯一的首一多项式$g\in F[x]$使得$J=(g)$.

定理 20

假设$f_1, f_2, ..., f_n$是$F[x]$中不全为零的一组多项式，则存在唯一的首一多项式*d*满足：

1) *d*整除每一个f_i.

2) 整除每个f_i的*c*一定整除*d*. 更进一步，$\exists b_i\in F[x]$使得$d=\sum b_i f_i$.

多项式环 III

证明：$J=\{\sum c_i f_i | c_i \in F[x]\}$, 则J是$F[x]$中的理想，则$f_i \in J$. 由于$F[x]$是主理想整环，所以$\exists d \in F[x]$, 使$J=(d)$(d是某一首一多项式)。所以$d/f_i$且$d=\sum c_i f_i$(因为$d \in J$). 所以2)成立。
假设有另一个d_1满足1)和2), 则d_1和d是相伴的, 因此$d_1=d$.
上述定理中的首一多项式d称为$f_1,\cdots,f_n$的最大公因子，表示为$d=\gcd(f_1,\cdots,f_n)$. 如果$d=1$，则称 $f_1,\cdots,f_n$是互素的。

定义 22 (不可约多项式)

一个多项式$p \in F[x]$称为不可约的或素的，如果p是$F[x]$中的素元，即p的次数不为零且p不能分成两个正次数 多项式的乘积。

定理 21 (唯一分解)

$deg(f) \geq 1, f \in F[x]$可以唯一写成$f=ap_1^{e_1}...p_k^{e_k}$. 其中$a \in F$, p_i是不同的不可约多项式，$e_i \geq 1$而且在 不计次序的情况下，这种分解是唯一的。

多项式环 IV

定理 22

$f \in F[x]$，则$F[x]/(f)$是域$\Leftrightarrow$ f是不可约多项式。

证明：作为练习。

推论 5

如果$F[x]$中的不可约多项式p整除$f_1, f_2, ..., f_m$则p整除至少其中的一个因子。

证明：考虑$F[x]/(p)$，由题设知$\overline{f_1 f_2}...\overline{f_m} = 0$. 由于$p$是不可约多项式，所以$F[x]/(p)$是域。所以 至少有一个$\overline{f_j} = 0$，即$f_j \in (p)$. 所以$p \mid f_j$.

本节概要

有限域的特征性质 I

定理 23

假设*F*是一个有限域，*K*为其子域。如果K有*q*个元素，则*F*有q^m个元素，其中$m = [F : K]$。

证明：F可以看作K上的向量空间。如果$m = [F : K]$，则F有由m个元素组成的基底$b_1, b_2, ..., b_m$，且每一个元素唯一的表示成$\sum a_i b_i$的形式, 其中$a_i \in K$，所以 F有q^m个元素。

定理 24

假设*F*是一个有限域，则*F*有p^n个元素。其中*p*是*F*的特征，*n*是*F*关于其素域的扩张次数。

证明：由于F的特征为p，则F的素子域同构于F_p。因此含有p个元素。由定理23知F有p^n个元素。

有限域的特征性质 II

定理 25

假设F是有q个元素的有限域，则$\forall a \in F, a^q = a$。

证明：首先$a^q = a$对$a = 0$成立。F中所有非零元素组成一个$q-1$阶有限群，所以$a^{q-1} = 1$对所有$a \neq 0$成立。所以$a^q = a$。

定理 26

如果F是有q个元素的有限域。K为一子域，则$K[x]$中的多项式$x^q - x$在$F[x]$中可分解为：$x^q - x = \prod_{a\in F}(x-a)$且$F$是$K$上多项式$x^q - x$的分裂域。

证明：我们知道$x^q - x$在F中至多含有q个根，而根据定理25，F中的q元素都是这个多项式的根。所以$x^q - x$在F中是分裂的，而且不能在任何更小的域中分裂。

有限域的特征性质 III

定理 27 (存在，唯一性定理)

对任何素数p和正整数n，存在一个有限域含有p^n个元素。且任何具有$q = p^n$个元素的有限域同构于$x^q - x$在F_p上的分裂域。

证明：（存在性）对$q = p^n$，考虑F_p上的多项式$x^q - x$，假设F是F_p上$x^q - x$的分裂域。我们知道$x^q - x$有q个不同的根，令S是F中多项式$x^q - x$的所有根组成的集合。则：

1) $0, 1 \in S$.

2) $a, b \in S \Rightarrow a - b \in S$, 因为$(a-b)^q = a^q - b^q = a - b$.

3) $a, b \in S \Rightarrow (ab^{-1}) \in S$, 因为$(ab^{-1})^q = a^q \cdot b^{-q} = ab^{-1}$. 所以S为$F$的一子域。另一方面$x^q - x$在S中分裂，所以$S = F$，所以F具有q个元素。

（唯一性）假设F是具有$q = p^n$个元素的有限域。则F的特征为p且以F_p为其子域。所以F是F_p上多项式$x^q - x$的分裂域。由于多项式 的分裂域是唯一的（在同构意义下）。所以具有q个元素的有限域唯一，且同构于$x^q - x$在F_p上的分裂域。

有限域的特征性质 IV

定理 28 (子域准则)

假设F_q是一个具有$q=p^n$个元素的有限域，则F_q的每一个有限域含有p^m个元素，则$m \mid n$。反之，对n的任一正因子m，存在 唯一F_q的子域含有p^m个元素。

证明：假设K是F_q的子域。显然有$|K|=p^m$。对某一$m \in N^+$。由定理23，知q是$|K|$的某一幂次。 所以$(p^m)^r=p^n$。所以$m \mid n$. 反之，假设$m \mid n$，则$p^m-1|p^n-1$。所以$x^{p^m-1}-1 \mid x^{p^n-1}-1$。因此$x^{p^m}-x \mid x^{p^n}-x$。从而 $x^{p^m}-x$的分裂域为F_q的子域且此子域含有p^m个元素。 假设F_q有两个不同的含有p^m个元素的子域则这两个子域中元素都是$x^{p^m}-x$的根。从而这两个子域相等。

定理 29

对每一个有限域F_q，其乘法群F_q^*是$q-1$阶的循环群。

有限域的特征性质 V

证明：假设$q \geq 3$且$h = q-1 = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$下面构造阶为$p_i^{r_i}$的元素$b_i$如下： 对每一个$i$, 多项式$x^{h/p_i}-1$最多只有$h/p_i$个根在$F_q$中， 所以$F_q$中至少有一个$a_i$不是$x^{h/p_i}-1$的根，即$a_i^{h/p_i} \neq 1$

令$b_i = a_i^{h/p_i^{r_i}}$则$b_i^{p_i^{r_i}} = a_i^h = 1$. 所以$b_i$的阶整除$p_i^{r_i}$, 但$b_i^{p_i^{r_i-1}} = a_i^{h/p_i} \neq 1$。所以$b_i$的阶为$p_i^{r_i}$。 下面证明： $b = b_1 b_2 ... b_m$的阶为h. 否则则b的阶至少为某一h/p_i的因子。假设为h/p_1， 则得

到$1 = b^{h/p_1} = b_1^{h/p_1} ... b_m^{h/p_1} = b_1^{h/p_1}$。 所以$p^r \mid h/p_1$,矛盾。所以$b$的阶为$h$。

定义 23

F_q^*中的生成元称为F_q的本原元。

显然F_q中有$\phi(q-1)$个本原元,其中ϕ是欧拉函数。

有限域的特征性质 VI

定理 30

设F_q是一个有限域，F_r是一个有限扩域，则F_r为F_q的一个单扩张，且任一F_r的本原元都是F_r在F_q上的定义元。

证明：假设ξ为F_r的本原元。显然$F_q(\xi) \subset F_r$。同时有$F_r \subset F_q(\xi)$。所以$F_r = F_q(\xi)$

定理 31

对任意的有限域F_q和正整数*n*，存在*n*次不可约多项式$\in F_q[x]$。

证明：根据定理27, 存在有限域F_{q^n}. 显然F_{q^n}是F_q的n次扩张，即$[F_{q^n} : F_q] = n$。 则由定理30，$F_{q^n} = F_q(\xi)$对某个$\xi \in F_{q^n}$从而知ξ的极小多项式的次数n.

不可约多项式的根 I

定理 32

设$f(x) \in F_q[x]$，是一个不可约多项式。α是f在F_q的某一个扩域上的根，则$h \in F_q[x], h(\alpha) = 0 \Leftrightarrow f \mid h$。

证明：假设a是f的首项次数。定义$g(x) = a^{-1}f(x)$。显然g是一个首一的不可约多项式且$g(\alpha) = 0$。所以是α在F_q上的极小多项式。 所以$h(\alpha) = 0 \Leftrightarrow g(x) \mid h \Leftrightarrow f \mid h$。

定理 33

设$f \in F_q[x]$是m次不可约多项式。则$f(x) \mid x^{q^n} - x \Leftrightarrow m \mid n$。

证明：假设$f(x) \mid x^{q^n} - x$。α是f在某一个分裂域中的根，则$\alpha^{q^n} = \alpha$。所以$\alpha \in F_{q^n}$。这说明 $F_q(\alpha) \subset F_{q^n}$但$[F_q(\alpha) : F_q] = m$, $[F_{q^n} : F_q] = n$。所以$m \mid n$。 反之，如果$m \mid n$。则F_{q^m}可以看作F_{q^n}的子域。如果α是f在

不可约多项式的根 II

某一个分裂域中的一个根，则$[F_q(\alpha):F_q]=m$，所以 $F_q(\alpha)=F_{q^m}$。因此$\alpha\in F_{q^n}$。所以$\alpha^{q^n}=\alpha$。即α是$x^{q^n}-x$的根。所以$f(x)\mid x^{q^n}-x$。

定理 34

设f是$F_q[x]$中次数为m的不可约多项式。则f有根α在F_{q^m}中。进一步，f的所有根正好为F_{q^m}中如下m个元素：$\alpha,\alpha^q,\alpha^{q^2},...,\alpha^{q^{m-1}}$。

证明：假设α是f在某一分裂域中的根则$[F_q(\alpha):F_q]=m$。所以$F_q(\alpha)=F_{q^m}$。所以$\alpha\in F_{q^m}$。因为如果$\beta\in F_{q^m}$是f的一个根，则β^q也是f的根，所以$\alpha,\alpha^q,...,\alpha^{q^{m-1}}$都是$f$的根。下面证明 这些元素互不相同。假设$\alpha^{q^j}=\alpha^{q^k},0\le j<k\le m-1$，$(\alpha^{q^j})^{q^{m-k}}=(\alpha^{q^k})^{q^{m-k}}$。所以$\alpha^{q^{m-k+j}}=\alpha^{q^m}=\alpha$。从而$f(x)\mid x^{q^{m-k+j}}-x$。由定理33，得$m\mid m-k+j$与$k>j$矛盾。

不可约多项式的根 III

推论 6

设f是F_q上的m次不可约多项式，则：f在F_q上的分裂域为F_{q^m}。

证明：首先，定理34说明f在F_{q^m}中是分裂的。另一方面$F_q(\alpha, \alpha^q, ..., \alpha^{q^{m-1}}) = F_q(\alpha) = F_{q^m}$。

推论 7

$F_q[x]$中同次不可约多项式有同构的分裂域。

定义 24

假设F_{q^m}是F_q的扩域，$\alpha \in F_{q^m}$，则$\alpha, \alpha^q, ..., \alpha^{q^{m-1}}$称为$\alpha$相对于$F_q$的共轭元。

不可约多项式的根 IV

定理 35

$\alpha \in F_q^*$相对于任意子域的共轭在F_q^*中有相同的阶。

证明：因为$\circ(\alpha) \mid q-1$。但特征的任一次幂都与$q-1$互素。所以α^{q^i}的阶都为$\circ(\alpha)$。

推论 8

如果α是F_q的本原元，则α相对于任一子域的共轭元也是本原元。

Example 9

$f(x) = x^4 + x + 1 \in F_2[x]$，$\alpha \in F_{16}$，则共轭元为$\alpha, \alpha^2, \alpha^4 = \alpha + 1, \alpha^8 = \alpha^2 + 1$。但相对于$F_4$ 的共轭元的$\alpha, \alpha^4 = \alpha + 1$。

元素的迹 I

定义 25 (迹的定义)

设$\alpha \in F = F_{q^m}, K = F_q$，元素$\alpha$的迹定义为$\alpha$所有共轭元素之和，即：$Tr_{F/K}(\alpha) = \alpha + \alpha^q +, ..., +\alpha^{q^{m-1}}$. 若$K$是$F$的素子域，则称为绝对迹。

定理 36

设$K = F_q, F = F_{q^m}$，则迹函数$Tr_{F/K}$满足：

1) $\forall \alpha \in F$，$Tr_{F/K}(\alpha) \in K$.
2) $Tr_{F/K}(\alpha + \beta) = Tr_{F/K}(\alpha) + Tr_{F/K}(\beta)$.
3) $Tr_{F/K}(c\alpha) = cTr_{F/K}(\alpha), c \in K, \alpha \in F$.
4) $Tr_{F/K}$是F到K上的（作为K上向量之间的）线形变换。
5) $Tr_{F/K}(a) = ma, a \in K$.
6) $Tr_{F/K}(\alpha^q) = Tr_{F/K}(\alpha), \forall a \in F$

元素的迹 II

证明：
1) 不难验证$(Tr_{F/K}(\alpha))^q = Tr_{F/K}(\alpha)$，所以$Tr_{F/K}(\alpha)$是$x^q - x$的根。
2)和3)保证了$Tr_{F/K}$为一线形变换，因此只需要证$Tr_{F/K}$是满的，而这只要证明$\exists\alpha \in F, Tr_{F/K}(\alpha) \neq 0$即可。考虑到
$Tr_{F/K}(\alpha) = 0 \Leftrightarrow \alpha$是$x^{q^{m-1}} + ... + x^q + x$的根，而该多项式最多只有$q^{m-1}$个根而F中$q^m$个元素。因而命题得证。 □

定理 37 (迹的传递性)

假设K是一个有限域，F是K的有限扩张，E是F的有限扩张，
则$\forall\alpha \in E, Tr_{E/K}(\alpha) = Tr_{F/K}(Tr_{E/F}(\alpha))$。

证明：
设$K = F_q, [F:K] = m, [E:F] = n$，则$[E:K] = mn$。$\forall\alpha \in E$，我们有：

元素的迹 III

$Tr_{F/K}(Tr_{E/F}(\alpha)) = \sum_{i=0}^{m-1}(Tr_{E/F}(\alpha))^{q^i} = \sum_{i=0}^{m-1}(\sum_{j=0}^{n-1}\alpha^{q^{jm}})^{q^i} = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\alpha^{q^{jm+i}} = \sum_{k=0}^{mn-1}\alpha^{q^k} = Tr_{E/K}(\alpha)$ □

定理 38

设F是有限域K的有限扩张。把它们都看作K上的向量空间，则F到K的所有线形变换正好是如下形式的映射$L_\beta, \beta \in F$。其中$L_\beta(\alpha) = Tr_{F/K}(\beta\alpha)$。进一步，如果$\beta$和$\gamma$是不同的元素，则$L_\beta \neq L_\gamma$。

证明：根据定理36(3), L_β是线形变换是显然的。假设$\beta \neq \gamma$，由于$Tr_{F/K}$是F到K上的线形变换，所以$\exists\alpha \in F$使得$Tr_{F/K}((\beta-\gamma)\alpha) \neq 0$。因此$L_\beta(\alpha) - L_\gamma(\alpha) = Tr((\beta-\gamma)\alpha) \neq 0$。从而$L_\beta \neq L_\gamma$。这样$\{L_\beta : \beta \in F\}$共给出$q^m$个线形变换。但$F \to K$仅有$q^m$个不同的线形变换。所以$\{L_\beta : \beta \in F\}$就是线形变换的全体。 □

多项式的阶和本原多项式 I

引理 1

设$f \in F_q[x]$是一次数大于0的多项式，$f(0) \neq 0$，则存在正整数$e \leq q^m - 1$使得$f(x) \mid x^e - 1$

证明：剩余类环$F_q[x]/(f)$含有$q^m - 1$个非零元素。而q^m个剩余类$x^j + (f), j = 0, 1, 2, ..., q^m - 1$是$q^m$个非零元素。所以存在$0 \leq r < s \leq q^m - 1$， 使得$x^s \equiv x^r \ mod \ f(x)$，$x^{s-r} \equiv 1 \ mod \ f(x)$，即$f(x) \mid x^{s-r} - 1$, $0 < s - r \leq q^m - 1$。 □

定义 26 (多项式的阶（周期）)

设$f(x) \in F_q[x]$是一非零多项式。如果$f(x) \neq 0$，则$f(x)$的阶（*order*）定义为满足$f(x) \mid x^e - 1$的最小的正整数e。并记作 $ord(f)$。如果$f(0) = 0$，则$f(x) = x^h \cdot g(x)$。其中$g(0) \neq 0$。这时$f(x)$的阶定义为$g(x)$的阶。

多项式的阶和本原多项式 II

定理 39

设$f(x) \in F_q[x]$是一不可约多项式，阶数为m。$f(0) \neq 0$，则$ord(f)$等于$f(x)$任一根在乘法群$F_{q^m}^*$中的阶。

证明：我们知道F_{q^m}是$f(x)$的分裂域, 而且$f(x)$的所有根都有相同阶（因为所有的根都是共轭的）. 设$\alpha \in F_{q^m}^*$是$f(x)$的根，则根据定理32, $\alpha^e = 1 \Leftrightarrow f(x) \mid x^e - 1$， 所以$\alpha$的阶就是$f(x)$的阶。 □

推论 9

设$f(x) \in F_q[x]$是F_q上次数为m的不可约多项式，则$ord(f) \mid q^m - 1$。

证明：如果$f(x) = c \cdot x, c \in F_q^*$，则$ord(f) = 1$，所以定理成立。 不然我们有$ord(f)$等于$f(x)$的根在$F_{q^m}$中的阶，所以应整除$q^m - 1$。

参考书

1. 华罗庚：数论导引，科学出版社。
2. 万哲先：代数与编码，高等教育出版社。
3. 林东岱：代数学基础与有限域，高等教育出版社。

埃瓦里斯特.伽罗瓦(1811-1832)，法国数学家。现代数学分支群论的创立者。 用群论彻底解决了根式求解代数方程的问题，而且由此发展了一整套关于群和域的理论， 人们称之为伽罗瓦理论。在世时在数学上研究成果的重要意义没被人们所认识，曾呈送科学院3篇学术论文， 均被退回或遗失。21岁时死于一次决斗。在决斗的前夜，他预料到自己将会死去，通宵达旦奋笔疾书， 与时间赛跑，力图把他的所有数学成果纪录下来，时不时在一旁写下“我没有时间”、 “我没有时间”。 美国数学家贝尔说： “他在黎明前那些绝望的最后时刻写下的东西，将会使一代代数学家忙上几百年。 ”