有限域讲义

张世武　编著

解放军外国语学院军事情报系

二〇〇五十一月

目　　录

有限域因为具有有限个元素，使得它有许多奇妙的性质，人们利用有限域的优美特性构作出具有各种对称性质的组合结构。这些组合结构有效地应用于密码学、计算机科学和数字通信领域。近年来俄美等国的数学家们把有限域理论用于编码通信领域，构作出性能优于前人的纠错码，提出了保密通信的新体制。

我们在介绍有限域的理论前，先复习初等数论及近世代数的有关知识。

§1. 整数 mod n 的剩余类环和剩余类域

任意取定一个正整数 n，令 Z_n 为由 n 个同余类

$$\bar{0}, \bar{1}, \cdots, \overline{n-1}$$

作成的集合，其中 $\bar{i}=\bar{j} \Leftrightarrow n \mid i-j$。下面规定同余类的加法与乘法，使 Z_n 作成一个环。

任取 $\bar{i}, \bar{j} \in Z_n$，规定

$$\bar{i}+\bar{j}=\overline{i+j}, \qquad \bar{i}\,\bar{j}=\overline{ij}$$

下面证明这是 Z_n 的两个代数运算。

设 $\bar{i}=\bar{s}$, $\bar{j}=\bar{t}$，则 $n \mid i-s$，$n \mid j-t$。从而 $n \mid (i+j)-(s+t)$，即有 $\overline{i+j}=\overline{s+t}$。这就是说，同余类的加法与每类中代表元素的选择无关，故加法是 Z_n 的一个代数运算。

此加法显然满足结合律与交换律；又 $\bar{0}$ 是零元，$\overline{-i}$ 是 $\bar{i}$ 的负元。因此，Z_n 对加法作成一个加群。

同法可证，同余类乘法 $\bar{i}\,\bar{j}=\overline{ij}$ 也是 Z_n 的一个代数运算。

又易知乘法满足结合律和交换律，且乘法对加法满足分配律，故 Z_n 作

成一个环，且是一个 n 阶有单位元的交换环。我们称其为以 n **为模的剩余类环，或简称模** n **剩余类环。**

下面进一步讨论这种环的一些性质。

首先，对任意整数 i，由于 $(i,n)=(i+nq,n)$，故类 $\bar{i}$ 中若有一个整数同 n 互素，则这个类中的所有整数都同 i 互素。因此，我们就说类 $\bar{i}$ 与 n 互素。

这样，在类 $\bar{0}$，$\bar{2}$，$\cdots$，$\overline{n-1}$ 中，有且只有 $\varphi(n)$ 个类同 n 互素。

定理 1.1 Z_n 中非零元 $\bar{m}$ 若与 n 互素，则为可逆元；若不与 n 互素，则为零因子。

证明：设 $\bar{m}\neq\bar{0}$，且 $(m,n)=1$，则存在整数 s,t 使 $ms+nt=1$，于是，$\bar{m}\,\bar{s}=\overline{ms+nt}=\bar{1}$，即 $\bar{s}$ 是 $\bar{m}$ 的逆元。

又当 $(m,n)=d>1$ 时，令

$$m=dm_1,\ n=dn_1,\ 1\le n_1<n,$$

则 $\overline{n_1}\neq\bar{0}$ 且 $\overline{mn_1}=\overline{mn_1}=\overline{nm_1}=\bar{0}$，即此时 $\bar{m}$ 是 Z_n 的一个零因子。#

此定理表明，模 n 剩余类环 Z_n 的全体与 n 互素的类 Z_n^* 关于同余类的乘法作成一个 $\varphi(n)$ 阶的交换群。

定理 1.2 若 p 是素数，则环 Z_p 是一个域；若 n 是合数，则环 Z_n 有零因子，从而不是域。

证明：因为 Z_p 的所有非零元素都同 p 互素，于是由定理 1.1 知，每个非零元素都有逆元，故 Z_p 是一个域。

当 n 是合数时，设 $n=n_1n_2,1<n_1,n_2<n$，则 $\overline{n_1}\neq\bar{0},\overline{n_2}\neq\bar{0}$，且 $\overline{n_1}\cdot\overline{n_2}=\bar{n}=\bar{0}$，故 Z_n 有零因子，从而不是域。 #

Z_p 正好有 p 个元素，因此它是个有限域。因为素数的个数是无限的，并且对任一素数，我们都如上定义了一个 p 元有限域，所以我们得到了无限多个有限域。今后 Z_n 记成 $\{0,1,\cdots,n-1\}$。我们还可以证明：

定理 1.3 Z_p^* 关于剩余类的乘法作成一个循环群。

证明：记 $p-1=h=\prod_{i=1}^{m} p_i^{r_i}$ 是其素因数的标准分解式。我们约定，群 G 中元素 a 的阶用 $\circ(a)$ 表示。并且有如下事实：设 a,b 是群 G 的元素，若 $ab=ba$ 且 $(\circ(a),\circ(b))=1$，则 $\circ(ab)=\circ(a)\circ(b)$。所以，假如在 Z_p^* 中我们能够找到阶数是 $p_i^{r_i}$ 的元 a_i，由上面的事实，$a=\prod_{i=1}^{m} a_i$ 就是 Z_p^* 中阶数是 h 的元，因此 $Z_p^*=\langle a\rangle$，于是 Z_p^* 就是循环群。 #

在近世代数中我们知道：在一个域中，n 次多项式在域中的零点不能多于 n 个，因此多项式 $x^{\frac{h}{p_i}}-1$ 在 Z_p^* 中最多只有 $\frac{h}{p_i}$ 个零点，于是 Z_p^* 中最少有一个使 $b_i^{\frac{h}{p_i}}\neq 1$ 的 b_i，我们记 $a_i=b_i^{h/p_i^{r_i}}$。因为 $a_i^{p_i^{r_i}}=b_i^h=1$，得 a_i 的阶数是 $p_i^{r_i}$ 的因数，但 $a_i^{p_i^{r_i-1}}=b_i^{\frac{h}{p_i}}\neq 1$。因此 $a_i^{p_i^{s_i}}\neq 1, s_i<r_i$。于是 a_i 的阶数是 $p_i^{r_i}$，定理得证。

利用 *Lagrange* 定理，我们可以给出数论中费马小定理 (*Fermat' little Theorem*) 的一个简短的证明。

定理 1.4（费马小定理）如果 p 是素数，并且 a 不是 p 的倍数，则

$$a^{p-1}\equiv 1 \bmod p$$

证明：由于 a 不是 p 的倍数，因此 $\bar{a}\in Z_p^*$，由于 $|Z_p^*|=p-1$，由

Lagrange 定理得 $(\tilde{a})^{p-1}=\tilde{1}$，即 $\overline{a^{p-1}}=\tilde{1}$。从而 $a^{p-1}\equiv 1 \bmod p$。 #

习题 1

1、求 Z_{18} 的所有子环。

2、求出 Z_{18} 的所有可逆元和零因子。

3、求出 Z_{18} 的所有幂零元。

4、找出 Z_{15} 到 Z_3 的所有同态。

5、证明：剩余类环 $(Z_n,+,\cdot)$ 是整环的充分必要条件是，n 为素数。

6、证明：剩余类环 Z_n 有非零幂零元的充分必要条件是，n 有素数平方因子。试决定 Z_{180} 的所有幂零元。

§2. 域的特征和素域

我们注意到，Q, R 和 C 这一类域与 Z_p 有一点很不一样。就是说：对于前者来说，任意有限个 1 的和都不等于 0；而对于后者来说，p 个 1 的和等于 0。为了区别这两类域，考察元素的序列

$$e, 2e, 3e, \cdots \qquad (2.1)$$

是有益处的，其中 e 是域的单位元素。首先，我们给出下面的定义。

定义 2.1 设 F 是一个域，e 是它的单位元素。如果对于任意正整数 m，都有 $me \neq 0$，我们说 F 的特征是 0，或 F 是特征 0 (*characteristic* 0) 的域。如果存在正整数 m，使得 $me = 0$，那么适合条件 $pe = 0$ 的最小正整数 p 就叫做 F 的特征，或者说 F 是特征 p 的 (*characteristic* p) 域。

用 *char* F 表示域 F 的特征。

下面我们证明

定理 2.1 设 F 是任意一域。那么 F 的特征是 0，或者是一个素数 p。

证明：设 *char* $F = p$，而 $p \neq 0$。我们用反证法来证明 p 必为素数。如果 p 不是素数，那么 p 有因数分解 $p = p_1 p_2$，这里 $1 < p_1, p_2 < p$。因此 $pe = (p_1 p_2)e = 0$。因为 $e^2 = e$，且域无零因子，所以有

$$(p_1 e)(p_2 e) = (p_1 e)(p_2 e) = 0$$

推出

$$p_1 e = 0 \text{ 或 } p_2 e = 0$$

但 $1 < p_1, p_2 < p$，这与 p 的最小性相矛盾，因此 p 必为素数。

注意，Q, R 和 C 都是特征 0 的域，而 Z_p 是特征 p 的域。

进一步，我们有

定理 2.2　设 F 是任意一域。如果 *char* $F = 0$，那么对于 F 中任意

一个非零元素 a 和任意正整数 m，都有 $ma \neq 0$，而且下列元素

$$0, \pm a, \pm 2a, \pm 3a, \cdots \tag{2.2}$$

两两不同；如果 F 是特征 p 的域，那么对于 F 中任意一个非零元素 a，都有 $pa = 0$，p 是适合条件 $pa = 0$ 的最小正整数，而且下列 p 个元素

$$0, a, 2a, 3a, \cdots, (p-1)a \tag{2.3}$$

两两不同；进一步，设 m 是一个整数，那么 $ma = 0$ 当且仅当 $p \mid m$。

证明：先设 F 是特征 0 的域。如果对于 F 中的某个非零元素 a，存在正整数 m，使得 $ma = 0$，那么

$$a(me) = m(ae) = ma = 0$$

但是 $a \neq 0$，因此一定有 $me = 0$，这与 F 的特征是 0 相矛盾。所以对于 F 中任意一个非零元素 a 和任意正整数 m，一定有 $ma \neq 0$。其次，如果（2.2）中有两个元素相等，譬如 $ka = la$，并且 $k < l$，那么

$$(l-k)a = la - ka = 0$$

但是 $l - k > 0$，所以这是不可能的。

再设 F 的特征是 p，那么 $pe = 0$。设 a 是 F 中任意一个非零元素，那么

$$pa = p(ea) = (pe)a = 0a = 0$$

又若 m 是一个使得 $ma = 0$ 的正整数，那么

$$(me)a = m(ea) = ma = 0$$

因为 $a \neq 0$，所以 $me = 0$。根据域的特征的定义，p 是适合条件 $pe = 0$ 的

最小正整数，所以，$p \le m$。因此 p 是适合条件 $pa=0$ 的最小正整数。

其次，如果(2.3)中有两个元素相等，譬如 $ka=la$，并且 $0 \le k < l < p$，那么

$$(l-k)a = la - ka = 0$$

但 $0 < l-k < p$，这与 p 是适合条件 $pa=0$ 的最小正整数着这一事实相矛盾。

最后我们证明，如果 F 是一个特征为 p 的域，a 是 F 中任意一个非零元素，m 是一个整数，那么 $ma=0$ 当且仅当 $p \mid m$。首先，如果 $p \mid m$，即 $m=pq$，这里 q 是一个整数，那么

$$ma = (pq)a = q(pa) = q0 = 0$$

反过来，设 $ma=0$，如果 p 不整除 m，那么 $(p,m)=1$。于是有整数 c 和 d，使得

$$1 = cp + dm$$

因此

$$\begin{aligned} a = 1a &= (cp+dm)a = (cp)a + (dm)a \\ &= c(pa) + d(ma) = c0 + d0 = 0 \end{aligned}$$

这是不可能的。因此一定有 $p \mid m$。

现在我们来考察特征 p 的域。设 F 是特征 p 的任意域，e 是它的单位元素。令

$$F_p = \{0, e, 2e, \cdots, (p-1)e\}$$

因为 $pe=0$，所以对任意整数 k，$(kp)e = k(pe) = k0 = 0$。因此 F_p 中任意两个元素 ke 和 le 的和与积可以按照下面的公式进行计算：

$$(ke+le)=(k+l)_p e$$
$$(ke)(le)=(kl)_p e$$

其中$(k+l)_p,(kl)_p$表示$k+l$及kl模p的余数。则F_p对于F中的加法运算和乘法运算来说是封闭的，并且F的零元素0和单位元素e都在F_p中。显然F_p中的任意元素ke的负元素$(p-k)e$也在F_p中。进一步，仿照Z_p中任一非零元素都有逆元素存在的证明，可以证明F_p中任一非零元素的逆元素一定属于F_p。这就证明了F_p是F的子域。

更进一步，因为F的任一子域都含有F的单位元素e，因而也含有$2e,3e,\cdots,(p-1)e$，所以一定包含F_p。这就是说，F_p是F的最小子域。我们把F_p叫做F的素域(*prime field*)。

与Z_p比较，可以发现从F_p到Z_p的映射

$$ke\to k\quad(0\le k<p)$$

是一个双射，而且这个映射保持运算。所以，F_p和Z_p是同构的。

我们再来考察特征0的域。设F是特征0的任意域，e是它的单位元素。由定理2.2，下列元素

$$\cdots -2e,-e,e,2e,\cdots \qquad (2.4)$$

两两不同。当$n\neq 0$时，将ne的逆元素记作$(ne)^{-1}$。令

$$\Delta=\{(me)(ne)^{-1}\mid m,n\in Z,n\neq 0\}$$

显然，$(0e)(ne)^{-1}=0,(ne)(ne)^{-1}=e$。因此$F$的零元素和单位元素都属于$\Delta$。进而有

$$(me)(ne)^{-1}=(m'e)(n'e)^{-1}$$

当且仅当

$$mn' = nm'$$

不难验证

$$(me)(ne)^{-1} + (m'e)(n'e)^{-1} = [(mn' + nm')e][(nn')e]^{-1}$$
$$((me)(ne)^{-1})((m'e)(n'e)^{-1}) = [(mm')e][(nn')e]^{-1}$$

因此Δ对于 F 中的加法运算和乘法运算是封闭的。

设 $(me)(ne)^{-1}$ 是Δ中任意一元素，那么 $(-me)(ne)^{-1}$ 也属于Δ，并且

$$(me)(ne)^{-1} + (-me)(ne)^{-1} = 0$$

当 $m \neq 0$, 即当 $(me)(ne)^{-1} \neq 0$ 时，$(ne)(me)^{-1}$ 也属于Δ，并且

$$((me)(ne)^{-1})\ ((ne)(me)^{-1}) = e$$

这就证明了Δ是 F 的子域。

进一步，因为 F 的任一子域都含有 F 的单位元素 e，因而也含有(2.4)中的每一个元素，所以也含有每一个形如

$$(me)(ne)^{-1}, (m, n \in Z, n \neq 0)$$

的元素。这就是说，Δ是 F 的最小的子域。我们把Δ叫做 F 的素域(*prime field*)。

与有理数域 Q 相比较：我们知道，每个有理数都可以表示成形状

$$\frac{m}{n},\ (m, n \in Z, n \neq 0)$$

即

$$Q = \{\frac{m}{n} \mid m, n \in Z, n \neq 0\}$$

并且 $\frac{m}{n} = \frac{m'}{n'}$ 当且仅当 $mn' = nm'$。可见从Δ到 Q 的映射

$$(me)(ne)^{-1} \to \frac{m}{n}$$

是一个双射，并且它将 Δ 中任意两个元素 $((me)(ne))^{-1}$ 与 $(m'e)(n'e)^{-1}$ 的和 $[(mn'+nm')e][(nn')e]^{-1}$ 映到 $(me)(ne)^{-1}$ 的像 $\frac{m}{n}$ 与 $(m'e)(n'e)^{-1}$ 的像 $\frac{m'}{n'}$ 的和 $\frac{mn'+nm'}{nn'}$，并把 $(me)(ne)^{-1}$ 与 $(m'e)(n'e)^{-1}$ 的积 $[(mm')e][(nn')e]^{-1}$ 映到 $\frac{m}{n}$ 与 $\frac{m'}{n'}$ 的积 $\frac{mm'}{nn'}$。因此，Δ 与 Q 同构。

综合上面的讨论，我们有

定理 2.3 设 F 是任意域。用 Δ 表示 F 的素域。那么，当 F 的特征是一个素数 p 时，Δ 与 Z_p 同构；当 F 的特征是 0 时，Δ 与 Q 同构。

因为 p(素数)元有限域与 Z_p 同构，今后我们记 p 元有限域 $F_p = Z_p$。

由定理 2.3 我们得到如下推论

推论 2.1　如果 F 是一个有限域，那么 F 的特征一定不是 0。

推论 2.2　设 F 和 F' 是两个同构的域。那么 F 和 F' 的特征一定相等。

从推论 2.2 可以看到，域的特征的确是域的一个特征性质。

习题 2

1、证明：一个域的任一自同构都将其素域的每个元素映到自身，然后推断出恒等自同构是有理数域Q和域F_p（p是任一素数）仅有的自同构。

2、证明：实数域R只有一个自同构。

3、试求$Z[i]/(1+i)$的特征数。这里$Z[i]$是高斯整数环。

4、假定K是除环，p是素数，$|K|\geq p$，如果对于K中任意元素a,b总有$(a+b)^p=a^p+b^p$,那么p是K的特征数。

5、证明：域F的任一非零元a与F的单位元e在加法群的阶相同。

§3. F_p 上一元多项式环 $F_p[x]$

设 p 是一个素数，F_p 是 p 元有限域，令

$$F_p[x]=\{\ \sum_{i=0}^{n}a_ix^{n-i}\mid a_i\in F_p,0\le i\le n,n=0,1,2,\cdots\ \}$$

我们现在定义 $F_p[x]$ 的加法和乘法，$\forall\ f(x),g(x)\in F_p[x]$，令

$$f(x)=\sum_{i=0}^{n}a_ix^{n-i},g(x)=\sum_{i=0}^{n}b_ix^{n-i},a_i,b_i\in F_p$$

则

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

其中，a_i+b_i 按 F_p 内的加法相加。$\forall\ a\in F_p,af(x)=\sum_{i=0}^{n}aa_ix^{n-i},aa_i$ 按 F_p 中的乘法相乘。$f(x)g(x)$ 按普通多项式的乘法，计算系数时，按 F_p 内的加法与乘法进行运算。

我们可以验证，$F_p[x]$ 关于上面定义的加法和乘法作成一个交换环。它和数域 F 上的一元多项式环 $F[x]$ 在性质上有类似的地方，也有差异的地方。例如：因式、倍式、最大公因式与最小公倍式、互素、不可约多项式以及因式分解唯一性定理等，都是类似的。下面我们用一个例子来说明辗转相除法。

例 3.1 设 $f(x)=x^5+x^4+x^3+x^2+x+1$，$g(x)=x^4+x^2+x+1\in F_2[x]$，求 $F_2[x]$ 中多项式 $u(x)$ 和 $v(x)$ 使

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

解：我们可以采用下面的竖式来进行辗转相除法：

x^2+x	x^4+x^2+x+1 x^4+x^3	$x^5+x^4+x^3+x^2+x+1$ $x^5+x^3+x^2+x$	$x+1$
	x^3+x^2+x+1 x^3+x^2	x^4+1 x^4+x^2+x+1	
	$x+1$	x^2+x x^2+x 0	x

因此

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

上面的竖式也可以用下面的简式来代替：

1 1 0	1 0 1 1 1 1 1	1 1 1 1 1 1 1 0 1 1 1	1 1
	1 1 1 1 1 1 1 1	1 0 0 0 1 1 0 1 1 1 1 1 1 1 0	1 0

为了把 $x+1$ 表示为 $x^5+x^4+x^3+x^2+x+1$ 和 x^4+x^2+x+1 的线性组合，需把上面辗转相除的竖式改写为

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

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

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

那么

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

$(x+1)(x^4+x^2+x+1)]$

$=(x^2+x)[(x^5+x^4+x^3+x^2+x+1)+(x^3+x+1)(x^4+x^2+x+1)]$

因此，$u(x)=x^2+x, v(x)=x^3+x+1$，而有

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

$F_p[x]$ 与 $F[x]$ 不同的地方，标志 $F_p[x]$ 的特点的性质有下面五条：

（1）对任意 $f(x)\in F_p[x]$，有 $p\cdot f(x)=0$；

（2）设 $f_1(x), f_2(x)\in F_p[x]$，则

$$(f_1(x)\pm f_2(x))^{p^n}=f_1(x)^{p^n}\pm f_2(x)^{p^n}$$

这可推广到多个多项式的情形。

特别地，当 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n\in F_p[x]$ 时，则

$$f^p(x)=a_0x^{np}+a_1x^{(n-1)p}+\cdots+a_n=f(x^p)$$

(3) 设 $f(x)\in F_p[x], \deg f\geq 1$，则下面命题是等价的：

(i)　$f(x)=g^p(x), g(x)$ 是 $F_p[x]$ 中的多项式；

(ii)　$f(x)=g(x^p)$；

(iii)　$f(x)$ 的微商 $f'(x)=0$。

我们证明 $(iii)\Rightarrow(i)$，其余留给读者。

设 $f(x)=a_0+a_1x+\cdots+a_nx^n$，　$a_i\in F_p, i=0,1,\cdots,n.$

则

$$f'(x)=a_1+2a_2x+\cdots+na_nx^{n-1}=0$$

$\Rightarrow f'(x)$ 的各项系数均为零，即 $ka_k=0$，$k=1,2,\cdots n$．当 k 不是 p 的倍数时，必须 $a_k=0$。因此 $f(x)$ 的表达式中，凡脚标不是 p 的倍数的系数全是零，剩下的各项，它的脚标都是 p 的倍数。因而 $f(x)$ 可写成：

$$\begin{aligned} f(x) &= a_{pi_1}x^{pi_1}+a_{pi_2}x^{pi_2}+\cdots+a_{pi_k}x^{pi_k} \\ &= (a_{pi_1}x^{i_1}+a_{pi_2}x^{i_2}+\cdots+a_{pi_k}x^{i_k})^p \\ &= g^p(x) \end{aligned}$$

其中，$g(x)=a_{pi_1}x^{i_1}+a_{pi_2}x^{i_2}+\cdots+a_{pi_k}x^{i_k}$。因而，（$i$）成立。

(4) 设 $f(x)\in F_p[x],\deg f\geq 1$，而且 $f'(x)\neq 0$。又设一个不可约多项式 $p(x)$ 是 $f(x)$ 的 k 重因式，则 $p\nmid k$ 时，$p(x)$ 是 $f'(x)$ 的 $k-1$ 重因式，而当 $p\mid k$ 时，$p(x)$ 至少是 $f'(x)$ 的 k 重因式。

(5) $F_p[x]$ 内次数小于 n 的多项式（包括 0 在内）共有 p^n 个，而次数 $=n$ 的多项式共有 $(p-1)p^n$ 个。

以上性质很容易证明，下面为了说明性质 4，我们举两个例子。

例 3.2 设 $f(x)=(x+1)^3(x^3+x^2+1)\in F_2[x]$，求 $x+1$ 在 $f'(x)$ 中的重数。

解：这里 $p=2$，$p(x)=x+1$ 是 $f(x)$ 的 3 重因式，而 $k=3,p\nmid k$

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

所以，$p(x)=x+1$ 为 $f'(x)$ 的 2 重因式。

例 3.3 设 $f(x)=(x+1)^2(x^3+x+1)\in F_2[x]$，求 $x+1$ 在 $f'(x)$ 中的重数。