[苏]M．Б斯维尔德利克 著

最佳离散信号

Zuijia lisan xinhao

郭桂蓉 译
陆仲良 校

電子工業出版社

内 容 简 介

本书系统地论述了在现代雷达和通信等系统中广泛采用的二元最佳离散编码信号的综合方法。书中所涉及的信号有：单值周期自相关函数码、双值周期自相关函数码、“重合不多于一”非规则脉冲序列、具有“重合不多于一”特性和最小非周期性的最佳码等四大类，计12种。后两类信号对于在干扰环境下多目标无模糊测距和测速有重要意义。书中还研究了由最佳周期信号演生最佳脉冲式信号的算法化方法，提供了大量的计算机计算结果。该书内容既有理论高度又结合工程运用，并附有大量例题和习题。

本书可供从事信号理论和无线电系统设计的科技人员和大专院校有关专业师生阅读。

Оптимальные Дискретные Сигналы

М. Б. Свердлик

Москва《Советское Радио》1975

最佳离散信号

〔苏〕М. Б. 斯维尔德利克 著

郭桂蓉 译 陆仲良 校

责任编辑：张殿阁

*

电子工业出版社出版

山东电子工业印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

*

1984年2月第1版 开本：850×1168 1/32

1984年2月第1次印刷 印张：6.5

印数：1-5,000 册 字数：174,720

统一书号：15290·52

定价：0.85元

译 者 的 话

在现代的雷达、通信、制导、空间测控以及电子对抗等无线电系统的优化设计中，信号的优化设计已日益显示出它的重要性。探索具有更好性能且便于实现的信号型式，拟定综合它们的正规方法并将其完全算法化，已成为亟待解决的问题。

本书是针对离散编码信号并根据极小极大最佳准则来解决这个问题的。该书可贵之处在于：对各式各样信号的综合，均立足于一种利用伽罗瓦域论的统一方法进行，并把最佳信号的寻找完全算法化。书中既系统地介绍了最佳周期信号的综合问题，也介绍了如何利用差集的倍乘变换由最佳周期信号演生最佳脉冲式信号的问题。特别是本书最后两章中所介绍的最佳“重合不多于一”码及最佳最小非周期性码，对于在干扰环境中解决多目标无模糊测距和测速问题，更有着重要的现实意义。

在翻译过程中，对所发现的原书中一些排印错误，均作了更正，但未一一注明，仅在几处比较重要的地方加有译者注。原书中一些符号系用俄文字母作下标，为便于阅读，在译文中均改为相应词意的英文字母。有些常用数学符号如矩阵等也改成了国内读者所习惯的形式。

周祖同教授审阅了译稿，并提出了许多宝贵的意见。庄钊文、张永军、戴长华、申强同志在核对原书例题及表格的数值计算结果方面，协助作了不少工作。此外，在翻译过程中还得到过陈荣锦、刘彬等同志的帮助，特在此一并致谢。

由于我们的水平所限，译文中定有不少缺点甚至错误，请读者批评指正。

译　者

目　　录

前　言

对于现代的通信和雷达来说，其时宽频宽积远大于一的复杂信号有着重要意义。因此研究综合复杂信号的有效方法，使信号具有良好的相关特性，便成为一个亟待解决的问题。这时，对信号提出的基本要求是：在给定的压缩系数条件下，其自相关函数的旁瓣应最小，或者，更一般地说，其模糊函数在(τ,ν)平面上某一区域内的旁瓣应最小。

本书是针对单一频率的离散编码信号和极小极大最佳准则来解决这个问题的。

所谓离散编码信号，在本书中系指这样的复杂信号，即其相干连续载波的调幅和调相是在离散时刻进行的，而且这些时刻是离散化间隔τ_0的整数倍。书中论及的离散编码信号可以分成两组。

单一频率的二元相位键控信号为一组，脉冲序列为另一组。本书如此取材，一则因为上述两组信号在通信和雷达中用途最广泛，再就是由于允许采用统一的方法，即立足于利用伽罗瓦域的性质对它们进行综合。自然，还可用这两组信号来构成更为复杂的单频离散信号，以便最大限度地全面满足各种具体情况下提出的要求。

专论二元相位键控信号和脉冲序列综合问题的文献很多。在俄文版的专著中，值得在此提出的有：阿米安托夫（Амиантов И.Н.）、瓦克曼(Вакман Д. Е.)和谢德列茨基(Седлецкий Р. М.)、瓦拉金（Варакин Л.Е.）、戈洛蒙勃（Голомб С.）、库克(Кук Ч.)和别伦费利德(Бернфельд М.)、吉洪诺夫(Тихонов В.И.)等的著作[1—6]。

本书把已问世的材料系统化，并为二元相位键控信号和“重合不多于一”脉冲序列的综合拟定新的有效方法。但是作为本书的主要目的，还是在于：发展一种立足于利用伽罗瓦域论的统一方法，来对各类单频离散信号进行综合，并对位数在一千以内的“最佳”码给出便于实际应用的计算和表示方法。

本书着眼于无线电工程师、雷达和通信系统专业的大学生和研究生，以及从事编码问题的科学工作者的需要。设想的主要一类读者，通常不大熟悉伽罗瓦域论和其它有关数学工具，而这些内容却是本书所论综合方法的理论基础，因此在第一章中，我们作了按工程水准阐述伽罗瓦域论基本问题的尝试。在阐述这些材料的同时辅以大量的实例；有的读者可能在上述数学分支方面还说不上是非常富有经验，我们的这一作法想必也会得到他们的赞同。无疑，通晓大学课程范围内伽罗瓦域论的读者，则只需熟悉一下第一章所用的符号，便可立即从第二章开始阅读本书。

第二、三、四章介绍二元相位键控信号，第五、六章介绍具有“重合不多于一”性质的非规则脉冲序列，在一定准则的意义下，它们是最佳的。

如果读者主要对属于非规则脉冲序列方面的问题感兴趣，那末，本书在结构上为他们提供了方便，读者在读完第一章后，可以直接去阅读第五章。

（以下从略）

第一章 伽罗瓦域

本章按其性质来说，是全书的数学导论，旨在介绍给读者一些本书中用到的有限域论和乘群的基本知识。这里仅提供最核心的材料，缺少它们将难以领会后续章节中所论述的综合方法。

本书的读者应具有高等技术院校课程大纲范围内的数学修养，上面提出的数学问题将以他们所能接受的方式进行阐述，基于这种意图，我们不得不略去一些证明。由于这个缘故，对本章的材料作了大量举例说明，照我们的看法，这些举例将有助于理解有限域论的许多抽象概念。为了较好地消化材料，读者自己做一做例题后边的练习会是十分有益处的。

读者要是对有限域论感兴趣，希望详尽了解这一对编码理论有根本意义的数学领域，可以参阅，例如，契鲍塔列夫（Н. Г. Чеботарев）所著“伽罗瓦理论基础”[1]和范德瓦尔登（Ван-дер-Варден）所著“近世代数”①[8]。

§1.1 基本定义

代数所研究的是一些任意元素的集合，这些元素类似于数，可加或乘，或者是同时经历这两种基本运算。

所谓集合上的运算，是指一种对应关系，在此关系下，集合的每对元素应有该集合中唯一确定的元素与之对应。集合的元素常用字母 $a, b, c, d, \cdots\cdots$ 来表示，集合用 $M=\{a, b, c, d, \cdots\cdots\}$ 表示，而运算则以符号记为 $c=a*b$。加法运算写作 $c=a+b$，而乘法运算则写作 $c=a\ b$。一般不把减法和除法作为基本运算看

① 中译本名为“代数学”——译者注。

待，因为它们分别是加法和乘法的逆运算。

域的定义。元素的这样一个集合称作域，如果对它给定一加法运算和一乘法运算，而这两种运算适合下列定律[7,8]：

定　　律	运　　算	
	加　　法	乘　　法
自闭律：对于每对元素 $a, b \in M$，存在唯一的元素 $c \in M$，使得 $c = a * b$	$A1.$ $a+b=c$	$M1.$ $ab=c$
结合律：$(a*b)*c=a*(b*c)$	$A2.$ $(a+b)+c=a+(b+c)$	$M2.$ $(ab)c=a(bc)$
交换律：$a*b=b*a$	$A3.$ $a+b=b+a$	$M3.$ $ab=ba$
存在单位元：存在一元素，$e \in M$，使得，$a*e=e*a=a$，其中 $a \in M$	$A4.$ $a+e=e+a=a$ $(e=0)$	$M4.$ $ae=ea=a$ $(e=1)$
存在逆元：对于任一元素，$a \in M$，存在一元素 $\bar{a} \in M$，使得 $a*\bar{a}=\bar{a}*a=e$	$A5.$ $a+\bar{a}=\bar{a}+a=0$ $(\bar{a}=-a)$	$M5.$ $a\bar{a}=\bar{a}a=1$ $(\bar{a}=a^{-1}, a\neq 0)$
分配律：	$D1.a(b+c)=ab+ac$ $D2.(b+c)a=ba+ca$	

于是，域遵守通常意义下的自闭律、结合律、交换律和分配律。一个域恒有一单位元 e。对于加法运算，单位元称作零（0）；对于乘法运算，称作幺（1）。域的任一元素 a 与 0 之和及其与 1 之积，均等于 a（$A4$, $M4$）。任一元素 a，均存有加性逆元 $\bar{a}=-a$，它是唯一满足方程 $a+(-a)=0$ 的域元素（$A5$）。继之，任一非零元素 a，均存有积性逆元 $\bar{a}=a^{-1}$，它是唯一满足方程 $a\,a^{-1}=1$ 的域元素（$M5$）。

含有有限（q）个元素的域，叫做有限域，并用 $GF(q)$ 来表示（GF——伽罗瓦域）。域的元素数称为有限域的阶。

群的定义。一个这样的集合称作交换加群，如果对它仅给定一加法基本运算，而此运算适合定律 $A1$—$A5$；一个这样的集合称作交换乘群，如果对它仅给定一乘法基本运算，而此运算适合定律 M1—M5。常用“阿贝耳群”一词作为“交换群“的代称。因本书只讨论交换群，故今后简记为群。

含有有限个元素的群叫做有限群，并用 $G=\{a, b, c, \cdots\}$ 来表示。群的元素数称为有限群的阶。

任一有限域的全体元素必构成加群，因此域的加群的阶与域的阶相同。域的乘群包括除零元素以外的全体域元素，故 q 阶域的乘群的阶为 $q-1$。

在着手研究有限域的基本性质之前，有必要先来介绍几个有限域的例子。

素域。素域乃是有限域的基本示例，该域的元素是以素数 p 为模的整数。

由定义知，整数 x 与 y 关于模 m 同余[9]

$$x\equiv y \pmod{m} \tag{1.1}$$

应与等式

$$x-y=km \tag{1.2}$$

等价，其中 k 为某一整数。

对于一规定的 r，适合同余式 $x\equiv r(\mathrm{mod}\ m)$ 的全体整数 x，也就是说，除以 m 得余数 r 的全体整数，必组成一模 m 的整数类，常用 $\{r\}$ 或 $r(\mathrm{mod}\ m)$ 表示。可见，同一个余数对应于同一类的全体整数，且同一类的全体整数可通过在表达式 $mk+r$ 中令 k 遍历全体整数而得出。有 m 个互异的 r 值，相应地就有 m 个模 m 的整数类。类的任一整数称作是对于该类全体整数模 m 的剩余。

由同余的性质知[9]，若 $x\equiv a(\mathrm{mod}\ m)$ 和 $y\equiv b(\mathrm{mod}\ m)$，则 $x+y\equiv a+b \pmod{m}$ 和 $xy\equiv ab \pmod{m}$。因此模 m 的剩余类

加法和乘法定义为：

$$\{a\}+\{b\}=\{a+b\}, \tag{1.3}$$

$$\{a\}\cdot\{b\}=\{ab\}。 \tag{1.4}$$

容易验证，对于任意 m，此剩余类加法和乘法适合域的全部定律，但 $M5$ 除外。而 $M5$ 则仅当 $m=p$ 且 p 为素数时才能满足。

从每一类当中各取一剩余，便得到一完全剩余系。常用最小非负剩余 0，1，2，……，$p-1$ 作为完全剩余系。素模 p 的完全剩余系适合域的全部定律。

因此，素模 p 的完全剩余系组成一 p 阶有限域，并以 $GF(p)$ 来表示，称作伽罗瓦素域。

域的元素加法和乘法，应在相应整数上作模 p 的算术运算来完成。

例1.1 整数 0，1，2，3，4 是域 $GF(5)$ 的元素。域 $GF(5)$ 的加群由整数 0，1，2，3，4 组成，而乘群则由整数 1，2，3，4 组成。域 $GF(5)$ 的元素加法规则和乘法规则分别确定如下：

表1.1 域 $GF(5)$ 中加法

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

表1.2 域 $GF(5)$ 中乘法

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

习题1 请验证域 $GF(5)$ 遵守定律 $A1$—$A5$，$M1$—$M5$，$D1$，$D2$；该域的加群遵守定律 $A1$—$A5$，其乘群遵守定律 $M1$—$M5$。

习题2 请构制域 $GF(5)$ 的元素加法表和乘法表。

扩域 $GF(p^n)$。仿照整数关于模m同余，也可以定义域$GF(p)$上多项式的同余。

一个多项式 $A(x)=\sum_{i=0}^{n} a_i x^i$，如果式中的系数 a_i 属于域 $GF(p)$，便称它为域 $GF(p)$ 上多项式。使得 $a_n \not\equiv 0 \pmod p$ 的最大整数 n 叫做多项式 $A(x)$ 的次数。

多项式 $A(x)$ 和 $B(x)$ 关于多项式模 $F(x)$ 同余[7,8]

$$A(x)\equiv B(x) \quad [\bmod F(x)], \tag{1.5}$$

根据定义应与等式

$$A(x)-B(x)=K(x)\ F(x) \tag{1.6}$$

等价，其中 $K(x)$ 为某一多项式。

在同余式(1.5)中，全部运算均应以 p 为模来完成，为此常用

$$A(x)\equiv B(x) \quad [\text{modd } F(x), p] \tag{1.7}$$

来表示，并读作：多项式 $A(x)$ 与 $B(x)$ 关于重模 $(F(x), p)$ 同余[10]。

对于一规定的 $R(x)$，适合同余式 $A(x)\equiv B(x)$ [modd $F(x), p$] 的全体域 $GF(p)$ 上多项式 $A(x)$，也就是说，除以 $F(x)$ 得剩余 $R(x)$ 的全体多项式，必组成一重模 $(F(x), p)$ 的多项式类，常用 $\{R(x)\}$ 或 $R(x)$ [modd $F(x), p$] 表示它。

可见，同一个剩余 $R(x)$ 对应于同一类的全体多项式，且同一类的全体多项式可通过在表达式 $F(x)K(x)+R(x)$ 中令 $K(x)$ 遍历系数取自域 $GF(p)$ 的全体多项式而得出。

倘若 $F(x)$ 是一域 $GF(p)$ 上 n 次多项式，那末所有可能的剩余 $R(x)$ 当是次数不高于 $n-1$ 的多项式：

$$R(x)=a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots\cdots+a_1x+a_0, \tag{1.8}$$

式中每个系数 $(a_{n-1}, a_{n-2}, \cdots, a_1, a_0)$ 可以是域 $GF(p)$ 的 p 个元素当中任意一个。

由此可见，恰好存在着 p^n 个互异的多项式$R(x)$，相应地便有 p^n 个重模 [$F(x), p$] 的多项式类。类的任一多项式称作是对于

该类全体多项式重模〔$F(x)$，p〕的剩余。

由同余的性质知[7,8]，若

$$A(x)\equiv R(x) \quad 〔\text{modd } F(x),\ p〕$$

和

$$B(x)\equiv P(x) \quad 〔\text{modd } F(x),\ p〕,$$

则 $$A(x)+B(x)\equiv R(x)+P(x) \quad 〔\text{modd } F(x),\ p〕$$

和 $$A(x)B(x)\equiv R(x)P(x) \quad 〔\text{modd } F(x),\ p〕。$$

因此重模〔$F(x)$，p〕的剩余类加法和乘法定义为：

$$\{R(x)\}+\{P(x)\}=\{R(x)+P(x)\}$$

和

$$\{R(x)\}\cdot\{P(x)\}=\{R(x)P(x)\}。 \tag{1.9}$$

不难验证，对于任意的域 $GF(p)$ 上多项式 $F(x)$，此剩余类加法和乘法适合域的全部定律，但 $M5$ 除外。而且同整数同余一样，只有当 $F(x)=f(x)$ 且 $f(x)$ 为域 $GF(p)$ 上不可约多项式时，$M5$ 才能满足。

一个系数取自域 $GF(p)$ 的 $n\geqslant 1$ 次多项式 $f(x)$，如果不能将它表示成：$f(x)=A(x)\ B(x)$，式中 $A(x)$ 和 $B(x)$ 为域 $GF(p)$ 上多项式，它便是域 $GF(p)$ 上不可约的[7]。

从每一类当中各取一剩余，便得到一完全剩余系。常用次数不高于 $n-1$ 的多项式，也就是形如 (1.8) 式的多项式作为完全剩余系。

重模〔$f(x)$，p〕的完全剩余系适合域的全部定律，这里 $f(x)$ 系域 $GF(p)$ 上不可约多项式，p 为素数。

因此，重模〔$f(x)$，p〕的完全剩余系组成一含 p^n 个元素的有限域，并以 $GF(p^n)$ 来表示，称作扩域或素域 $GF(p)$ 的 n 次扩张。

必须着重指出，扩域 $GF(p^n)$ 的元素与素域的不同，它们已不再是整数，而是系数取自域 $GF(p)$、次数不高于 $n-1$ 的多项式。

例1.2 求扩域$GF(3^2)$的元素。在(1.8)式中，令 $n=2$，并独立地赋予系数 a_i 以域 $GF(3)$ 的元素值(域 $GF(3)$ 的元素为 0，1，2)，求得

$$GF(3^2)=\{0,\ 1,\ 2,\ x,\ 2x,\ x+1,\ 2x+1,\ x+2,\ 2x+2\}。$$

不难看出，域 $GF(3^2)$ 的元素正是系数取自域 $GF(3)$ 次数不高于 $n-1=2-1=1$ 的全体多项式。以 $p=3$ 为模作域 $GF(3^2)$ 的元素加法，得到表1.3。

表1.3 域 $GF(3^2)$ 中 加 法

+	1	2	x	$2x$	$x+1$	$2x+1$	$x+2$	$2x+2$
1	2	0	$x+1$	$2x+1$	$x+2$	$2x+2$	x	$2x$
2	0	1	$x+2$	$2x+2$	x	$2x$	$x+1$	$2x+1$
x	$x+1$	$x+2$	$2x$	0	$2x+1$	1	$2x+2$	2
$2x$	$2x+1$	$2x+2$	0	x	1	$x+1$	2	$x+2$
$x+1$	$x+2$	x	$2x+1$	1	$2x+2$	2	$2x$	0
$2x+1$	$2x+2$	$2x$	1	$x+1$	2	$x+2$	0	x
$x+2$	x	$x+1$	$2x+2$	2	$2x$	0	$2x+1$	1
$2x+2$	$2x$	$2x+1$	2	$x+2$	0	x	1	$x+1$

构制域 $GF(p^n)$ 的元素乘法表时，需把不可约多项式 $f(x)$ 具体化，这是因为元素的乘法应以 $(f(x),\ p)$ 为重模来完成。

今选用域 $GF(3)$ 上二次不可约多项式$f(x)=x^2-2$[12]①。

作为举例，我们来求元素 $2x$ 和 $2x+1$ 的乘积。完成乘法运算，得到

$$2x(2x+1)=4x^2+2x\equiv x^2+2x\ (\mathrm{mod}\ 3)。$$

将多项式 x^2+2x 除以多项式 x^2-2 后，再注意到作加法运算时以 3 为模，得

① 验证域 $GF(3)$ 上多项式 $f(x)=x^2-2$ 不能被系数取自域$GF(3)$的$n-1=1$次多项式 x，$x-1$ 和 $x-2$ 整除后，不难证明，$f(x)=x^2-2$ 是域 $GF(3)$ 上不可约的。

$$
\begin{array}{r|l}
x^2+2x & x^2-2 \\
+\quad 2x^2-4 & 2 \\
\hline
2x-4 &
\end{array}
$$

故　　$2x(2x+1)\equiv 2x-1\ (\mathrm{modd}\ x^2-2,\ 3)$。

类似地可求得域 $GF(3^2)$ 所有元素对的乘积；计算结果列于表1.4中。

表1.4　域 $GF(3^2)$ 中 乘 法

·	1	2	x	$2x$	$x+1$	$2x+1$	$x+2$	$2x+2$
1	1	2	x	$2x$	$x+1$	$2x+1$	$x+2$	$2x+2$
2	2	1	$2x$	x	$2x+2$	$x+2$	$2x+1$	$x+1$
x	x	$2x$	2	1	$x+2$	$x+1$	$2x+2$	$2x+1$
$2x$	$2x$	x	1	2	$2x+1$	$2x+2$	$x+1$	$x+2$
$x+1$	$x+1$	$2x+2$	$x+2$	$2x+1$	$2x$	2	1	x
$2x+1$	$2x+1$	$x+2$	$x+1$	$2x+2$	2	x	$2x$	1
$x+2$	$x+2$	$2x+1$	$2x+2$	$x+1$	1	$2x$	x	2
$2x+2$	$2x+2$	$x+1$	$2x+1$	$x+2$	x	1	2	$2x$

习题1　请验证域 $GF(3^2)$ 遵守定律 $A1$—$A5$，$M1$—$M5$，$D1$，$D2$；该域的加群遵守定律$A1$—$A5$，其乘群遵守定律 $M1$—$M5$。

习题2　请求出扩域 $GF(2^2)$ 的元素，并构制元素加法表和乘法表。取多项式 $f(x)=x^2+x+1$ 作为域 $GF(2)$ 上 $n=2$ 次不可约多项式。

扩域 $GF[(p^n)^S]$。 p^{ns} 阶域不仅可由域 $GF(p)$ 的 ns 次扩张得到，而且也可由域 $GF(p^n)$ 的 s 次扩张得到[7,8]。

类似于对域 $GF(p^n)$ 那样进行推论，结果表明，三重模 $(f_s(x),\ f_n(x),\ p)$ 的完全剩余系适合域的全部定律，这里 $f_s(x)$ 系域 $GF(p^n)$ 上 s 次不可约多项式，$f_n(x)$ 系域 $GF(p)$ 上 n 次不

表 1.5 域 $FG[(2^2)^2]$ 中加法

+	1	a	$1+a$	x	$x+1$	$x+a$
1	0	$1+a$	a	$x+1$	x	$x+a+1$
a	$a+1$	0	1	$x+a$	$x+a+1$	x
$a+1$	a	1	0	$x+a+1$	$x+a$	$x+1$
x	$x+1$	$x+a$	$x+a+1$	a	1	a
$x+1$	x	$x+a+1$	$x+a$	1	0	$a+1$
$x+a$	$x+a+1$	x	$x+1$	a	$a+1$	0
$x+a+1$	$x+a$	$x+1$	x	$a+1$	a	1
ax	$ax+1$	$ax+a$	$ax+a+1$	$(a+1)x$	$(a+1)x+1$	$(a+1)x+a$
$ax+1$	ax	$ax+a+1$	$ax+a$	$(a+1)x+1$	$(a+1)x$	$(a+1)x+a+1$
$ax+a$	$ax+a+1$	ax	$ax+1$	$(a+1)x+a$	$(a+1)x+a+1$	$(a+1)x$
$ax+a+1$	$ax+a$	$ax+1$	ax	$(a+1)x+a+1$	$(a+1)x+a$	$(a+1)x+1$
$(a+1)x$	$(a+1)x+1$	$(a+1)x+a$	$(a+1)x+a+1$	ax	$ax+1$	$ax+a$
$(a+1)x+1$	$(a+1)x$	$(a+1)x+a+1$	$(a+1)x+a$	$ax+1$	ax	$ax+a+1$
$(a+1)x+a$	$(a+1)x+1+a$	$(a+1)x$	$(a+1)x+1$	$ax+a$	$ax+a+1$	ax
$(a+1)x+a+1$	$(a+1)x+a$	$(a+1)x+1$	$(a+1)x$	$ax+a+1$	$ax+a$	$ax+1$

可约多项式。因此次数不高于 $s-1$ 的多项式

$$R(x)=a_{s-1}x^{s-1}+a_{s-2}x^{s-2}+\cdots+a_1x+a_0 \qquad (1.10)$$

必组成一有限域 $GF[(p^n)^s]$，式中每个系数（a_{s-1}，a_{s-2}，…，a_1，a_0）可以是域 $GF(p^n)$ 的 p^n 个元素当中任意一个。

由此可见，恰好存在着 p^{ns} 个互异的多项式 $R(x)$。故域 $GF[(p^n)^s]$ 含有 p^{ns} 个元素。并称该域为域 $GF(p^n)$ 的 s 次扩张。

必须强调指出，扩域 $GF[(p^n)^s]$ 与扩域 $GF(p^n)$ 不同，$GF(p^n)$ 的元素为系数取自域 $GF(p)$ 的多项式，而 $GF[(p^n)^s]$ 的元素则是系数取自域 $GF(p^n)$ 的多项式。

例 1.3 求扩域 $GF[(p^n)^s]$ 的元素，条件为：$p=2$，$n=2$ 和 $s=2$。

在 (1.10) 式中令 $s=2$，并独立地赋予系数 a_i 以域 $GF(2^2)$ 的元素值，我们来求域 $[GF(2^2)^2]$ 的元素。

域 $GF(2^2)$ 的元素为 0，1，a，$a+1$（请检查例1.2后边的习题答案）；故

$$GF[(2^2)]=\{0,\ 1,\ a,\ 1+a,\ x,\ x+1,\ x+a,\ x+a+1,$$
$$ax,\ ax+1,\ ax+a,\ ax+a+1,\ (1+a)x,$$
$$(1+a)x+1,\ (1+a)x+a,\ (1+a)x+a+1\}。$$

不难看出，域 $GF[(2^2)^2]$ 的元素正是系数取自域 $GF(2^2)$ 次数不高于 $s-1=2-1=1$ 的全体多项式。考虑到域 $GF[(2^2)^2]$ 的元素加法应以 $p=2$ 为模来完成，所以我们把该域中的加法运算表示成表1.5的形式。

构制域 $GF[(p^n)^s]$ 的元素乘法表时，首先，需要把域 $GF(p^n)$ 上 s 次不可约多项式具体化，其次，还需要有域 $GF(p^n)$ 的元素乘法表。域 $GF(2^2)$ 的元素乘法规则如表 1.6 所示（请检查例 1.2 后边的习题答案）。

表 1.6 域 $GF(2^2)$ 中乘法

·	0	1	a	$a+1$
0	0	0	0	0
1	0	1	a	$a+1$
a	0	a	$a+1$	1
$a+1$	0	$a+1$	1	a

例如，选用多项式 $f(x)=x^2+x+a$ 作为域 $GF(2^2)$ 上不可约多项式，其中 a 系域 $GF(2^2)$ 的元素，且 $a^2+a+1\equiv 0$。

作为举例，我们来求元素 $x+a$ 和 $ax+a+1$ 的乘积。完成乘法运算，求得