国家自然科学基金资助

编码理论及其应用

朱士信　编著

高等教育出版社

资助

编码理论及其应用

朱士信　编著

高等教育出版社·北京

内容提要

本书对有限环上编码理论的基本理论、方法和应用作了比较系统的介绍。全书共分六章。第一章是全书的基础知识，从有限域和有限环的基本概念引出本书中所需要的基础知识。第二章介绍有限环上线性码各种不同的重量分布。第三章介绍有限链环上常循环码的结构及其相关问题。第四、五章分别介绍有限环上线性码和迹码关于各种不同重量的 N-重量码及其 Gray 像。第六章介绍利用有限域上常循环码构造量子 MDS 和符号对 MDS 码。

本书可作为数学专业、信息专业以及计算机科学专业研究生和本科高年级学生的教材，也可供相关专业的教师和科研工作者参考。

图书在版编目(CIP)数据

编码理论及其应用／朱士信编著.--北京：高等教育出版社，2018.9

ISBN 978-7-04-050239-8

Ⅰ.①编… Ⅱ.①朱… Ⅲ.①编码理论-高等学校-教材 Ⅳ.①O157.4

中国版本图书馆 CIP 数据核字(2018)第 169716 号

策划编辑 李晓鹏　责任编辑 李晓鹏　特约编辑 董达英　封面设计 李小璐
版式设计 马　云　责任校对 高　歌　责任印制 耿　轩

出版发行 高等教育出版社
社　　址 北京市西城区德外大街 4 号
邮政编码 100120
印　　刷 北京市鑫霸印务有限公司
开　　本 787mm×960mm　1/16
印　　张 14.75
字　　数 260 千字
购书热线 010-58581118
咨询电话 400-810-0598

网　　址 http://www.hep.edu.cn
http://www.hep.com.cn
网上订购 http://www.hepmall.com.cn
http://www.hepmall.com
http://www.hepmall.cn

版　　次 2018 年 9 月第 1 版
印　　次 2018 年 9 月第 1 次印刷
定　　价 30.60 元

物 料 号 50239-00

前言

随着网络技术和数字通信的飞速发展，信息传输的可靠性和有效性成为一个非常重要的问题。1948 年，Shannon 在其开创性论文 *A Mathematical Theory of Communications* 中指出，在信息传输速率低于信道容量时，采用适当的编码技术可以将有扰信道产生的差错减少到任意低的限度，从而实现可靠通信，这奠定了通信的数学基础，纠错码理论也由此产生。纠错码从理论上保证了数字通信的可靠性，在移动通信、雷达、遥控遥测、航天等领域已有广泛的应用。许多纠错码，尤其是循环码，如 HAMMING 码、BCH 码、RS 码等在实践中得到广泛的应用，并且渗透到生活生产的各个领域。在信息技术飞速发展的今天，无论是国家的军事、政治、外交、航天等领域还是人们的日常生活、生产等领域都对信息传输的可靠性提出了更高的要求。而纠错码能降低数字信息传输的误码率，进而提高通信系统的可靠性。因此，纠错码理论就成了一门重要的学科。经过 60 多年的发展，有限域上的纠错码在各类通信中被广泛使用，对信息技术的发展起了极大的推动作用。

随着有限域上纠错码理论的深入发展，有限环上的纠错码也引起学者的兴趣，特别是 20 世纪 90 年代初，Nechev、Hammons 等人发现了二元 Kerdock 码和其他的一些高效的二元非线性码，如 Preparata、Delsarte-Goethols 和 Goethols 码等可被看作是整数模 4 的剩余类环上循环码在 Gray 映射下的二元像，由此解决了 Preparata 码与 Kerdock 码关于距离计数器具有形式对偶性这一困扰编码界 20 多年的疑惑，有限环上的编码理论获得重要突破，这推动有限环上纠错码理论研究获得了极大的发展。1997 年，万哲先院士编写了有限环上纠错码专著 *Quaternary Codes*，有限环上的纠错码理论进入了全面发展时期。一方面，人们利用有限环上的线性码构造了许多参数更好的线性或非线性码，另一方面利用有限环上的线性码构造各种序列，例如 CDMA 序列、调频序列和低相关性序列。同时，有限环上的纠错码还被用在无线通信系统的纠错编码方案中。我们相信，随着信息与网络技术的深入发展，有限环上的纠错码势必会在生活与生产的各个领域得到广泛的应用。

本书主要介绍有限环上几类重要的纠错码，包括阿贝尔码，N-重量码和常循环码等基本理论，通过它们阐述有限环上纠错码的主要研究方法和最新的研究进展。另外，本书也介绍常循环码在量子纠错码与符号对码的构造方面的应用。

全书共分六章，第一章由李平、孙中华编写，第二章由唐永生编写，第三章由开晓山、李平编写，第四、五章由施敏加编写，第六章由开晓山编写。全书由朱士信统稿。

由于编者水平有限，书中定有不完备的叙述与欠缺，欢迎大家批评指正！作者的研究工作得到国家自然科学基金（编号：61370089）的资助。

编　者

2017.8

目录

第一章　基本理论

§1.1　环和有限域

许多代数结构，譬如，整数集 $\mathbb{Z}$，有理数集 $\mathbb{Q}$，复数集 $\mathbb{C}$，都有两个二元运算，加法和乘法.更确切地说，在加法下，构成一个阿贝尔群.乘法是一个二元运算，且存在单位元 1.同时，两个运算间存在分配律，进而形成一个新的代数结构——环.首先，给出环的定义.

定义 1.1　设集合 R 上存在加法+和乘法 · 两种运算，则 R 称为含幺环，如果下列条件成立：

(1) R 关于加法为阿贝尔群，记它的单位元为 0；

(2) R 关于乘法满足结合律且有单位元 1；

(3) 加法和乘法运算满足分配律，即对任意 $a,b,c\in R$，

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

如果乘法满足交换律，则称 R 为交换环.

注 1.1　(1) 定义 1.1 给出的是含幺环，更一般地，条件(2)中，对于乘法不一定存在单位元，但是，任意一个环都可以嵌入到一个含幺环中.

(2) 在环 R 中，我们称加法的单位元为环 R 的零元.乘法单位元称为环 R 的单位元.

例 1.1　设 $\mathbb{Z}$ 表示整数集，m 是一个固定的正整数，模 m 的剩余类集合 $\mathbb{Z}_m$，关于模 m 类加法和乘法：$\bar{a}+\bar{b}=\overline{a+b}$，$\bar{a}\,\bar{b}=\overline{ab}$，构成一个交换环.

由环的定义我们可以得到下面的基本性质.

定理 1.1　设 R 为环，则

(1) 对任意 $a\in R$，$0\cdot a=a\cdot 0=0$；

(2) 对任意正整数 n，$a\in R$，记 na 为 n 个 a 之和，记 $-na$ 为 na 的加法逆元，则对 $n\in\mathbb{Z}$，$a,b\in R$，我们有 $(na)b=a(nb)=nab$；

(3) 对任意 $a_i,b_j\in R$，$\sum\limits_i a_i\cdot\sum\limits_j b_j=\sum\limits_i\sum\limits_j a_ib_j$.

考虑环的加法群，对任意的 $a\in R$，阶 $\mathrm{ord}(a)$ 定义为最小的正整数 n，使得

$na=0$. 如果不存在这样的整数 n, 则 $\mathrm{ord}(a)=\infty$.

定义 1.2 若环 R 的元素(对加法)有最大阶 n, 则称 n 为环 R 的特征, 记作 $\mathrm{char}(R)=n$. 若环 R 的元素(对加法)有无穷最大阶, 则称环 R 的特征为无限, 记作 $\mathrm{char}(R)=\infty$.

记 $|R|$ 表示环 R 所含元素的个数, 如果 $|R|>1$, 则 $1\neq 0$.

定义 1.3 环 R 中非零元 a 叫作环 R 的左零因子(left zero divisor), 是指存在非零元素 $b\in R$, 使得 $ab=0$. 类似地, 若 $ba=0$, 则 a 叫作环 R 的右零因子(right zero divisor). 如果 a 同时是左零因子和右零因子, 则称 a 为环 R 的零因子(zero divisor).

若环 R 是交换环, 则左零因子、右零因子、零因子是一回事.

定义 1.4 如果 R 为环, a 称为左可逆的(left invertible), 如果存在元素 $b\in R$, 使得 $ba=1$. 类似地, 若 $ab=1$, 则 a 叫作右可逆的(right invertible). 如果 a 既是左可逆的又是右可逆的, 称 a 为可逆(invertible)的, 也称作环 R 的单位(unit).

注 1.2 含幺环 R 中单位集合构成一个群, 称作环 R 的单位群, 记作 R^*. 若环 R 是交换环, 则左可逆的、右可逆的、可逆的是一个概念.

定义 1.5 设 R 是一个交换环. 如果 R 没有零因子, 则环 R 为整环(integral domain).

定义 1.6 设 R 是一个环. 如果 R 的非零元组成的集合关于乘法形成一个群, 则称环 R 为除环(division ring)或体.

定义 1.7 交换的除环称作域. 如果域 $\mathbb{F}$ 只有有限个元素, 则称其为有限域.

由于代数编码中主要应用的是交换环, 下面的定义均是针对交换含幺环.

定义 1.8 设 R 是一个交换环. R 的任意非空子集 I 称作环 R 的理想(ideal), 如果 $a,b\in I$ 且 $r\in R$, 有 $a\pm b\in I$ 且 $ra\in I$.

由于 I 非空, 设 $x\in I$, 则 $x-x=0\in I$. 显然 $\{0\}$ 与 R 均是环 R 的理想, 称为 R 的平凡理想(trivial ideal). 如果 $I\neq R$, 称 I 为 R 的真理想(proper ideal).

定义 1.9 设 R 是一个交换环和 $a\in R$. 理想 $Ra=\{ra\mid r\in R\}$ 称为环 R 的主理想, 记作 $\langle a\rangle$, 称为由 a 生成的理想.

例如, $R=\langle 1\rangle$, $\{0\}=\langle 0\rangle$.

例 1.2 整数 $\mathbb{Z}$ 关于通常的加法和乘法形成一个环, 且 $\mathbb{Z}$ 的每个理想均是主理想. 即设 I 是 $\mathbb{Z}$ 的理想, 则存在 $m\in\mathbb{Z}$ 使得 $I=\langle m\rangle=m\mathbb{Z}$.

例 1.3 设 $\mathbb{F}$ 表示一个域, $\mathbb{F}[x]$ 表示系数属于域 $\mathbb{F}$ 未定元为 x 的多项式环. 则 $\mathbb{F}[x]$ 的每个理想均为主理想. 即设 I 是 $\mathbb{F}[x]$ 的理想, 则存在 $f(x)\in\mathbb{F}[x]$, 使得

$$I=\langle f(x)\rangle=f(x)\,\mathbb{F}[x].$$

定义 1.10 设 R 是一个交换环.如果环 R 的每个理想均是主理想,则称 R 为主理想环.

设 I 是环 R 的理想.对任意的 $a,b\in R$,定义

$$a\equiv b(\mathrm{mod}\ I)\text{当且仅当}\ a-b\in I. \tag{1.1}$$

读作 a 与 b 模 I 同余.这是对整数集 $\mathbb{Z}$ 上模 m 运算的推广.可以验证关系 $a\equiv b(\mathrm{mod}\ I)$ 是环 R 的一个等价关系.关于该等价关系的每个等价类称作模 I 的剩余类,记作 $\bar{a}$.显然,

$$\bar{a}=a+I=\{a+x\mid x\in I\}$$

且 $\bar{a}\cap\bar{b}=\varnothing$ 当且仅当 $a\not\equiv b(\mathrm{mod}\ I)$.因此,模 I 的不同剩余类给出环 R 的一个划分.将模 I 的不同剩余类构成一个集合,记作 R/I.例如,$\mathbb{Z}_m=\mathbb{Z}/\langle m\rangle$.对任意的 $\bar{a},\bar{b}\in R/I$,定义加法和乘法:

$$\bar{a}+\bar{b}=\overline{a+b}, \tag{1.2}$$

$$\bar{a}\cdot\bar{b}=\overline{ab}. \tag{1.3}$$

可以验证(1.2)和(1.3)的合理性,我们有如下结论.

定理 1.2 设 R 是环,I 是环 R 的理想,则 R/I 关于(1.2)和(1.3)形成一个环.

设 R 是环,I 是环 R 的理想.环 R/I 称为 R 关于 I 的商环.

定义 1.11 设 R 和 R' 是环.映射 $\phi:R\to R'$ 称为环同态(homomorphism of rings),如果下列两个条件成立:

(1) $\phi(a+b)=\phi(a)+\phi(b)$;

(2) $\phi(ab)=\phi(a)\phi(b)$,

对任意的 $a,b\in R$.

设 $\phi:R\to R'$ 是环同态,显然,$\phi(0)=0'$ 是环 R' 的零元且 $\phi(-a)=-\phi(a)$,对任意的 $a\in R$.此外,如果 ϕ 是一个满射,$\phi(1)=1'$ 是环 R' 的单位元.

定义 1.12 设 $\phi:R\to R'$ 是环同态.定义

$$\mathrm{Im}\ \phi=\{\phi(a)\mid a\in R\},$$

$$\mathrm{Ker}\ \phi=\{a\in R\mid\phi(a)=0'\}.$$

$\mathrm{Im}\ \phi$ 称为 ϕ 的像(image),$\mathrm{Ker}\ \phi$ 称为 ϕ 的核(kernel).

如果环同态 ϕ 是一个双射,则称 ϕ 为同构映射.如果环 R 和环 R' 之间存在同构映射,则称 R 与 R' 是同构的,记作 $R\cong R'$.

定理 1.3 (1) 设 R 是环,I 是环 R 的一个理想.则

$$\phi:R\to R/I,$$

$$a\mapsto\bar{a}=a+I$$

是一个环同态(自然同态映射,natural homomorphism),$\mathrm{Ker}\ \phi=I$ 且 $\mathrm{Im}\ \phi=R/I$.

(2) 设 $\phi: R \to R'$ 是环同态且 $\phi(1)=1'$ 是 R' 的单位元. 则 $\mathrm{Im}\,\phi$ 是环 R' 的子环, $\mathrm{Ker}\,\phi$ 是环 R 的理想. 此外,

$$\bar{\phi}: R/\mathrm{Ker}\,\phi \to R/I,$$
$$\bar{a}=a+\mathrm{Ker}\,\phi \mapsto \phi(a)$$

是一个环同构.

由定理 1.3, 我们可以得到如下同态基本定理.

定理 1.4 设 $\phi: R \to R'$ 是环同态且 ϕ 是一个满射, 则

(1) 如果 I 是 R 的理想, 则 $\phi(I)$ 是 R' 的理想.

(2) 如果 I' 是 R' 的理想, 则 $\phi^{-1}(I')$ 是环 R 的理想, $\mathrm{Ker}\,\phi \subseteq \phi^{-1}(I')$ 且 $\phi^{-1}(I')/\mathrm{Ker}\,\phi \cong I'$.

(3) 如果 I 是 R 的理想且 $\phi(I)=I'$, 则

$$R/I \to R'/I',$$
$$a+I \mapsto \phi(a)+I'$$

是环同态. 如果 $I \supseteq \mathrm{Ker}\phi$, 则 $\phi^{-1}(\phi(I))=I$ 且上面的映射为环同构.

下面我们介绍极大理想, 素理想的概念.

定义 1.13 设 R 是一个环.

(1) 环 R 的真理想 M 称为极大理想, 如果 R 中没有包含 M 的其他真理想.

(2) 环 R 的理想 P 称为素理想, 如果 $P \neq R$, 且由 $ab \in P$ 可以推出 $a \in P$ 或 $b \in P$.

我们有如下判定定理.

定理 1.5 设 R 是一个环, I 是环 R 的理想.

(1) I 是极大理想当且仅当 R/I 是域.

(2) I 是素理想当且仅当 R/I 是整环.

下面, 我们介绍环的直和.

定义 1.14 设 R 是一个环, $R_1, R_2, \cdots, R_r$ 是环 R 的子环. 称 R 可表示为 $R_1, R_2, \cdots, R_r$ 的直和, 如果下列条件成立:

(1) 每个 R_i 都是 R 的理想, $i=1,2,\cdots,r$;

(2) $R=R_1+R_2+\cdots+R_r$, 其中 $R_1+R_2+\cdots+R_r=\{a_1+a_2+\cdots+a_r \mid a_i \in R_i, i=1,\cdots,r\}$;

(3) $R_i \cap (R_1+\cdots+R_{i-1}+R_{i+1}+\cdots+R_r)=\{0\}$, $i=1,2,\cdots,r$.

由此, 我们可得如下重要的定理——中国剩余定理.

定理 1.6 设 $m_1, m_2, \cdots, m_r$ 是 r 个大于 1 的整数且两两互素. 令 $m=m_1m_2\cdots m_r$ 且 $\hat{m}_i=\dfrac{m}{m_i}$. 则存在 $c_1, c_2, \cdots, c_r$ 使得 $c_1\hat{m}_1+c_2\hat{m}_2+\cdots+c_r\hat{m}_r=1$. 对每个 $i=1,2,\cdots,r$, 映射

$$\phi_i: \mathbb{Z}/\langle m_i\rangle \to \mathbb{Z}/\langle m\rangle,$$

$$a+\langle m_i\rangle \mapsto ac_i\hat{m}_i+\langle m\rangle$$

是一个 $\mathbb{Z}/\langle m_i\rangle$ 到 $\mathbb{Z}/\langle m\rangle$ 的一个嵌入同构映射.此外,

$$\mathbb{Z}/\langle m\rangle=\phi_1(\mathbb{Z}/\langle m_1\rangle)+\phi_2(\mathbb{Z}/\langle m_2\rangle)+\cdots+\phi_r(\mathbb{Z}/\langle m_r\rangle).$$

下面,我们讨论有限域的基本性质.

定义 1.15 设 F 是域 E 的非空子集,如果 F 在 E 的加法和乘法下构成域,则称 F 是域 E 的子域,或 E 称为 F 的扩域,记作 $F\subseteq E$.

为有效地讨论具有包含关系的域的结构,我们引入下面的概念.

定义 1.16 设 V 是一个阿贝尔群,$\mathbb{F}$ 是一个域,映射 $\phi:\mathbb{F}\times V\to V$,我们以 $rx(r\in\mathbb{F},x\in V)$ 表示 $\phi(r,x)$,满足下列条件:

(1) $r(x+y)=rx+ry$;

(2) $(r+s)x=rx+sx$;

(3) $(rs)x=r(sx)$;

(4) $1x=x$,

其中 $r,s,1\in\mathbb{F},x,y\in V$,则称 V 为域 $\mathbb{F}$ 上的向量空间.

由定义 1.16,如果 F,E 为域且 $F\subseteq E$,则 E 可以视为域 F 上的向量空间.

定义 1.17 设 F,E 为域且 $F\subseteq E$,用 $[E:F]$ 表示将 E 视为域 F 上的向量空间的维数,并称为 E 对 F 的扩张次数.如果 $[E:F]<\infty$,则称 E 对 F 的扩张为有限扩张,否则称作无限扩张.

设 p 是任意一个素数,$\mathbb{Z}_p$ 表示整数模 p 的剩余类环.关于加法和乘法:

$$\bar{a}+\bar{b}=\overline{a+b},\bar{a}\cdot\bar{b}=\overline{ab}$$

形成一个域,$|\mathbb{Z}_p|=p$.故域 $\mathbb{Z}_p$ 是一个有限域(finite field).

设 $\mathbb{F}$ 是一个有限域且 1 是域 $\mathbb{F}$ 的单位元.对任意整数 n,定义

$$n\cdot 1=\underbrace{1+1+\cdots+1}_{n},$$

且 $0\cdot a=0$.

定义 1.18 设 $\mathbb{F}$ 是一个域且 1 是域 $\mathbb{F}$ 的单位元.如果对任意正整数 $m,m\cdot 1\neq 0$,则称 $\mathbb{F}$ 是特征(characteristic)为 0 的域.如果存在正整数 m 使得 $m\cdot 1=0$,则称满足这种条件的最小正整数 m 为域的特征,此时 $\mathbb{F}$ 称为特征为 m 的域.

例如,域 $\mathbb{Z}_p$ 的特征为 p.更一般地,如果 $\mathbb{F}$ 是一个有限域,则 $\mathbb{F}$ 的特征为一个素数.

定理 1.7 设 $\mathbb{F}$ 是一个有限域,则域 $\mathbb{F}$ 的特征是一个素数.

设 p 是一个素数,域 $\mathbb{F}$ 是一个特征为 p 的有限域.因 $p\cdot 1=0$,故对任意 $a\in\mathbb{F}$,

$$p\cdot a=p\cdot(1a)=(p\cdot 1)a=0\cdot a=0.$$

反之,如果 $m\cdot 1=0$,可推出 $p\mid m$.设 $\Delta=\{1,2\cdot 1,\cdots,(p-1)\cdot 1\}$,可验证 Δ 是域 $\mathbb{F}$的子域.映射

$$\Delta\to\mathbb{Z}_p,$$

$$k\cdot 1\mapsto\bar{k},\quad 0\leqslant k\leqslant p-1$$

是一个同构映射.因此,在同构意义下,我们认为域 Δ 与域 $\mathbb{Z}_p$是一样的.

定理 1.8 设域 $\mathbb{F}$是一个特征为 p 的有限域,则 $|\mathbb{F}|=p^m$,其中 $m=[\mathbb{F}:\mathbb{Z}_p]$.

注 1.3 通常,我们将特征为 p 且含有 p^m 个元素的有限域,记作 $\mathbb{F}_{p^m}$.

定理 1.9 在有限域 $\mathbb{F}_{p^m}$中,对任意的 $a,b\in\mathbb{F}_{p^m}$有

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

下面,我们给出多项式环的概念,并给出 Galois 环和有限域的结构.

§1.2 多 项 式

设 R 是一个含幺环,x 是环 R 上的未定元.假设 i 是一个非负整数,表达式 a_ix^i 称为次数为 i 的单项式(monomials),$a_i\in R$.环 R 上的多项式定义为

$$f(x)=a_0x^0+a_1x^1+\cdots+a_nx^n,$$

其中 $a_0,a_1,\cdots,a_n\in R$,n 是一个非负整数.在 $f(x)$ 中,a_ix^i 称为第 i-次项(i-th degree term),a_i 称为项的系数(coefficient).当 $a_i=1$,写 $a_ix^i=x^i$.当 $a_i=0$,则在 $f(x)$ 中省去 a_ix^i 项.特别地,$x^0=1$,$x^1=x$ 且 a_0x^0 写成 a_0.即 $f(x)=a_0+a_1x+\cdots+a_nx^n$ 且 $a_n\neq 0$.我们称 $f(x)$ 的次数为 n,记作 $\deg(f(x))$,称 a_n 为 $f(x)$ 的首项系数(leading coefficient).当 $f(x)$ 的所有系数都是 0,$f(x)$ 称为零多项式,记为 0,规定 $\deg(0)=-\infty$.在不引起混淆的情况下,可将 $f(x)$ 和 $\deg(f(x))$ 分别简记为 f 和 $\deg(f)$.如果 $a_n=1$,则 $f(x)$ 称为首一多项式.

设 $f(x)$ 和 $g(x)$ 是环 R 上的多项式.如果两者的每一项系数都对应相等,则 $f(x)$ 和 $g(x)$ 是两个相同的多项式,写作 $f(x)=g(x)$.通常,我们使用符号 $\sum$ 简记

$$f(x)=a_0+a_1x+\cdots+a_nx^n$$

为 $f(x)=\sum_{i=0}^{n}a_ix^i$.

记 $R[x]$ 表示环 R 上关于未定元 x 的多项式构成的集合.设 $f(x),g(x)\in R[x]$ 且

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

记 $M=\max\{n,m\}$，如果 $n\neq m$，譬如，$m<n$，则令 $b_{m+1}=b_{m+2}=\cdots=b_n=0$. 因此，我们写

$$f(x)=\sum_{i=0}^{M} a_i x^i, \quad g(x)=\sum_{i=0}^{M} b_i x^i.$$

定义 $f(x)$ 和 $g(x)$ 的和，记作 $f(x)+g(x)$，

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

显然，$f(x)+g(x)\in R[x]$，因此 $R[x]$ 关于上面定义的加法是封闭的.

如果 $m\geqslant 1$，令 $a_{n+1}=a_{n+2}=\cdots=a_{n+m}=0$；如果 $n\geqslant 1$，令 $b_{m+1}=b_{m+2}=\cdots=b_{m+n}=0$. 则

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

定义 $f(x)$ 和 $g(x)$ 的乘积，记作 $f(x)g(x)$，

$$f(x)g(x)=\sum_{i=0}^{n+m} \Big(\sum_{j=0}^{i} a_j b_{i-j} \Big) x^i.$$

显然，$f(x)g(x)\in R[x]$，因此 $R[x]$ 关于上面定义的乘法是封闭的. 进一步可检验 $R[x]$ 关于上面定义的加法和乘法形成一个环，称为环 R 上关于未定元 x 的多项式环.

定理 1.10 设 $f(x),g(x)\in R[x]$. 则

(1) $\deg(f+g)\leqslant\max\{\deg(f),\deg(g)\}$.

(2) $\deg(fg)\leqslant\deg(f)+\deg(g)$，且如果 $f(x)$ 或 $g(x)$ 的首项系数不是零因子，则等号成立. 特别地，若 R 为整环，则等号恒成立.

如果 $\mathbb{F}$ 为有限域，则对于多项式 $f(x),g(x)\in\mathbb{F}[x]$ 且 $g(x)\neq 0$，由带余除法，存在唯一的多项式 $q(x),r(x)\in\mathbb{F}[x]$，使得 $\deg r<\deg g$，且

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

对于环上的多项式，我们有如下定理.

定理 1.11 如果 $f(x),g(x)\in R[x]$ 且 $g(x)$ 的首项系数是环 R 的单位，则存在唯一的多项式 $q(x),r(x)$ 使得 $f(x)=q(x)g(x)+r(x)$，$\deg r<\deg g$.

下面，进一步讨论多项式环 $\mathbb{F}[x]$. 关于域 $\mathbb{F}$ 上多项式的整除、因式、最大公因式、不可约多项式、互素、因式分解及其零点等概念和相应定理，对于一般域上的多项式都成立.

定义 1.19 多项式 $f\in\mathbb{F}[x]$ 称作不可约的(irreducible)，如果 $f=bc$，则 b 或 c 为常数多项式(constant polynomial).

定理 1.12(唯一分解定理) 设 $f(x)\in\mathbb{F}[x]$,则 $f(x)$ 可唯一分解为不可约因式的乘积

$$f(x)=ap_1(x)^{e_1}\cdots p_k(x)^{e_k},$$

其中,$a\in\mathbb{F}$,$p_1(x),\cdots,p_k(x)$ 是不同的不可约多项式,$e_1,\cdots,e_k$ 为正整数.若不计因式的次序,则上面的分解是唯一的.

定义 1.20 设 b 是域$\mathbb{F}$的某一扩域中的元素,称 b 是多项式 $f(x)\in\mathbb{F}[x]$ 的一个根(root)或零点(zero),如果 $f(b)=0$.

注 1.4 b 是多项式 $f(x)\in\mathbb{F}[x]$ 的根当且仅当 $x-b\mid f(x)$.

定义 1.21 设 b 是域$\mathbb{F}$的某一扩域中的元素,且 b 是多项式 $f(x)\in\mathbb{F}[x]$ 的一个根.如果 k 是一个正整数使得 $(x-b)^k\mid f(x)$ 但 $(x-b)^{k+1}\nmid f(x)$,则 k 称为元素 b 的重数.如果 $k=1$,则称 b 为 $f(x)$ 的单根,当 $k\geqslant 2$,则称 b 为重根.

定义 1.22 域$\mathbb{F}$的一个扩域$\mathbb{K}$叫作$\mathbb{F}[x]$中的 n 次多项式 $f(x)$ 在$\mathbb{F}$上的一个分裂域(splitting field),如果 $f(x)$ 在$\mathbb{K}$上可以分解成一次因式的乘积,而在任何一个$\mathbb{K}$的真子域 E 上,$f(x)$ 都不能分解成一次因式的乘积.

下面定理说明分裂域是唯一的.

定理 1.13(existence and uniqueness of splitting fields) 设$\mathbb{F}$是域,$f(x)\in\mathbb{F}[x]$是次数$\geqslant 1$ 的多项式,则 $f(x)$ 的分裂域存在,且 $f(x)$ 的任意两个分裂域是同构的.

下面,我们回到有限域 $\mathbb{F}_{p^m}$.

引理 1.1 设 $\mathbb{F}_q$ 是一个含有 q 个元素的有限域,则 $a^q=a$,对任意 $a\in\mathbb{F}_q$.

引理 1.2 设 $\mathbb{F}_q$ 是一个含有 q 个元素的有限域,$\mathbb{K}$ 是 $\mathbb{F}_q$ 的一个子域,则多项式 $x^q-x\in\mathbb{K}[x]$ 在 $\mathbb{F}_q$ 上分裂,

$$x^q-x=\prod_{a\in\mathbb{F}_q}(x-a)$$

且 $\mathbb{F}_q$ 是多项式 $x^q-x\in\mathbb{K}[x]$ 的分裂域.

定理 1.14(existence and uniqueness of finite fields) 对于任意素数 p 和正整数 m,存在一个有限域含有 p^m 个元素.任意具有 p^m 个元素的有限域同构于 $x^{p^m}-x$ 在 $\mathbb{F}_p$ 上的分裂域同构.

定理 1.14 说明域 $\mathbb{F}_q$ 存在且唯一,其中 $q=p^m$,p 为素数.特别地,记有限域 $\mathbb{F}_q$ 的乘法群为 $\mathbb{F}_q^*$.下面定理给出 $\mathbb{F}_q^*$ 的一个重要性质.

定理 1.15 设 $\mathbb{F}_q$ 为有限域,其乘法群 $\mathbb{F}_q^*$ 为 $q-1$ 阶循环群.

设 $\mathbb{F}_q$ 为有限域,$\xi\in\mathbb{F}_q^*$ 称作本原元(primitive element),如果 ξ 是 $\mathbb{F}_q^*$ 的生成元.

设$\mathbb{K}$是 $\mathbb{F}_q$ 的子域,则 $\mathbb{Z}_p\subseteq\mathbb{K}\subseteq\mathbb{F}_q$.由此,

$$m=[\mathbb{F}_q:\mathbb{Z}_p]=[\mathbb{K}:\mathbb{Z}_p][\mathbb{F}_q:\mathbb{K}].$$

由定理 1.14，$\mathbb{K}\cong\mathbb{F}_{p^n}$，其中 $n\mid m$.

对于任意的 $\theta\in\mathbb{F}_q^*$，存在多项式 $f(x)\in\mathbb{K}[x]$ 使得 $f(\theta)=0$. 那么 $\mathbb{K}[x]$ 中满足 $f(\theta)=0$ 的次数最小的首一多项式叫作 θ 在 $\mathbb{K}$ 上的极小多项式. 特别地，极小多项式为域 $\mathbb{K}$ 上的不可约多项式. 多项式 $f(x)\in\mathbb{F}_q[x]$ 称作 m 次本原多项式(primitive polynomial)，如果 $f(x)$ 为 $\mathbb{F}_{q^m}$ 的一个本原元的极小多项式. 关于有限域上的不可约多项式有如下性质.

定理 1.16 设 $f(x)\in\mathbb{F}_q[x]$ 是次数为 m 的不可约多项式，则 $f(x)$ 在 $\mathbb{F}_{q^m}$ 上有根 α. 此外，$f(x)$ 的 m 个不同的根为

$$\alpha,\alpha^q,\cdots,\alpha^{q^{m-1}}\in\mathbb{F}_{q^m},$$

即有限域 $\mathbb{F}_q$ 上的 m 次不可约多项式的分裂域为 $\mathbb{F}_{q^m}$.

设 $\mathbb{F}_q$ 是含有 q 个元素的有限域，$q=p^m$. 下面，我们研究多项式 $x^n-1\in\mathbb{F}_q[x]$ 在有限域 $\mathbb{F}_q$ 上的分解. 记 $n=n'p^e$，其中 $\gcd(n',p)=1$，$e\geqslant 0$ 为整数. 则在 $\mathbb{F}_q$ 中，

$$x^n-1=x^{n'p^e}-1=(x^{n'}-1)^{p^e}.$$

因此，我们假设 $\gcd(n,p)=1$，并且 $\mathbb{F}_Q$ 是多项式 $x^n-1\in\mathbb{F}_q[x]$ 在 $\mathbb{F}_q$ 上的分裂域，x^n-1 在域 $\mathbb{F}_Q$ 上的根称为 $\mathbb{F}_q$ 上的 n 次单位根(n-th root of unity)，n 次单位根构成集合 $E^{(n)}$，则 $E^{(n)}$ 关于 $\mathbb{F}_Q$ 中的乘法运算是一个阶为 n 的循环群，称 $E^{(n)}$ 的生成元为域 $\mathbb{F}_q$ 上的一个 n 次本原单位根(primitive n-th root of unity).

定义 1.23 设 $\mathbb{F}_q$ 是一个含有 $q=p^m$ 个元素的有限域，n 是一个与 p 互素的正整数，ξ 为域 $\mathbb{F}_q$ 上的 n 次本原单位根，则

$$Q_n(x)=\prod_{\substack{s=1\\ \gcd(s,n)=1}}^{n}(x-\xi^s)$$

称作域 $\mathbb{F}_q$ 上的 n 次割圆多项式(n-th cyclotomic polynomial).

定理 1.17 设 $\mathbb{F}_q$ 是一个含有 $q=p^m$ 个元素的有限域，n 是一个与 p 互素的正整数，则

(1) $x^n-1=\prod\limits_{d\mid n}Q_d(x)$；

(2) $Q_n(x)$ 的系数属于 $\mathbb{F}_p$，即，$Q_n(x)\in\mathbb{F}_p[x]$；

(3) $Q_n(x)$ 在 $\mathbb{F}_q[x]$ 可以分解为 $\phi(n)/d$ 个不同的 d 次首一不可约多项式的乘积，其中，$d=[\mathbb{F}_Q:\mathbb{F}_q]$，$d$ 是最小的满足 $q^d\equiv 1(\bmod n)$ 的正整数.

对于与 p 互素的正整数 n，记 $\mathbb{Z}_n$ 表示整数模 n 的剩余类环. 在 $\mathbb{Z}_n$ 中定义等价关系：

$$i\sim j\Leftrightarrow\exists\, s\in\mathbb{Z},\text{使得 } j\equiv iq^s(\bmod n).$$