第十一章 多项式环
2015年11月09日

信息安全数学基础

陈恭亮 教授 博士生导师

上海交通大学信息安全工程学院

chengl@sjtu.edu.cn

11.1.1 基本定义

11.1 多项式整环

本节考虑多项式环. 因为多项式理论和方法在信息安全和密码学中有重要的应用,特别是有限域的构造, 所以我们关注更多的多项式性质.

设R 是整环, x 为变量. 则R 上形为

$$a_nx^n + \cdots + a_1x + a_0, \quad a_i \in R$$

的元素称为R 上的多项式.

设$f(x) = a_nx^n + \cdots + a_1x + a_0,\ a_n \neq 0$ 是整环R 上的多项式, 则称多项式$f(x)$ 的**次数**为n, 记为$\deg\ f = n$.

例11.1.1 $\mathbf{Z}[X]$ 中的$2x+3$ 的次数为1, x^2+2x+3 的次数为2, x^4+1 的次数为4, $x^8+x^4+x^3+x+1$ 的次数为8.

设整环R 上的全体多项式组成的集合为

$$R[X] = \{f(x) = a_n x^n + \cdots + a_1 x + a_0 \mid a_i \in R,\ 0 \le i \le n,\ \ n \in \mathbf{N}\}. \tag{1}$$

首先, 定义$R[X]$ 上的加法. 设

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \quad g(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0,$$

定义$f(x)$ 和$g(x)$ 的加法为

$$(f+g)(x) = (a_n+b_n)x^n + (a_{n-1}+b_{n-1})x^{n-1} + \cdots + (a_1+b_1)x + (a_0+b_0) \tag{2}$$

则$R[X]$ 中的零元为0, $f(x)$ 的负元为$(-f)(x) = (-a_n)x^n + \cdots + (-a_1)x + (-a_0)$.

其次, 定义$R[X]$ 上的乘法. 设

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,\ a_n \neq 0, \quad g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0,$$

定义$f(x)$ 和$g(x)$ 的乘法为

$$(f \cdot g)(x) = c_{n+m} x^{n+m} + c_{n+m-1} x^{n+m-1} + \cdots + c_1 x + c_0, \qquad (3)$$

其中

$$c_k = \sum_{i+j=k,\ 0\le i\le n,\ 0\le j\le m} a_i b_j = a_k b_0 + a_{k-1} b_1 + \cdots + a_1 b_{k-1} + a_0 b_k,\ 0 \le k \le n+m, \qquad (4)$$

即

$$c_{n+m} = a_n b_m,\ c_{n+m-1} = a_n b_{m-1} + a_{n-1} b_m,\ \ldots,\ c_k = \sum_{i+j=k} a_i b_j,\ \ldots,\ c_0 = a_0 b_0,$$

则$R[X]$ 中的单位元为1.

定理11.1.1 设$R[x]$ 是整环R 上的多项式环(1). 则对于多项式的加法(2) 以及多项式的乘法(3), $R[x]$ 是一个整环.

证 易知, $R[X]$ 对于多项式的加法(2) 是一个交换加群. 具有结合律, 零多项式是零元0, 多项式f 的负元是$(-f)$, 也有交换律.

$R[X]$ 对于多项式的加法(3) , 具有结合律, 1_R 是单位元$1_{R[x]}$, 也有交换律. 此外, $R[x]$ 无零因子. 事实上, 设

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,\ \ a_n \neq 0, \quad g(x) = b_m x^m + \cdots + b_1 x + b_0,\ \ b_m \neq 0,$$

使得

$$(f \cdot g)(x) = c_{n+m} x^{n+m} + c_{n+m-1} x^{n+m-1} + \cdots + c_1 x + c_0 = 0,$$

其中$c_k = \sum\limits_{i+j=k} a_i b_j,\ \ 0 \leq k \leq n+m$, 即

$$c_{n+m} = a_n b_m,\ c_{n+m-1} = a_n b_{m-1} + a_{n-1} b_m, \ldots,\ c_0 = a_0 b_0.$$

则$c_{n+m} = a_n b_m = 0$. 因为R 是整环, 所以有$a_n = 0$ 或$b_m = 0$, 矛盾. 故$R[x]$ 是一个整环. 证毕

例11.1.2 设$f(x)=x^6+x^4+x^2+x+1,\ g(x)=x^7+x+1\in\mathbf{F}_2[x]$, 则

$$f(x)+g(x)=x^7+x^6+x^4+x^2,$$

$$f(x)g(x)=x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1.$$

事实上,

$$\begin{aligned}
&(x^6+x^4+x^2+x+1)\cdot(x^7+x+1)\\
=\ &x^{13}+x^{11}+x^9+x^8+x^7\\
&+x^7+x^5+x^3+x^2+x\\
&+x^6+x^4+x^2+x+1\\
=\ &x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1
\end{aligned}$$

11.2.2 多项式整除与不可约多项式

本节考虑多项式的整除性.

定义11.2.1 设$f(x)$, $g(x)$ 是整环R 上的任意两个多项式, 其中$g(x)\neq 0$. 如果存在一个多项式$q(x)$ 使得等式

$$f(x)=q(x)\cdot g(x) \tag{5}$$

成立, 就称$g(x)$ **整除** $f(x)$ 或者$f(x)$ 被$g(x)$ 整除, 记作$g(x)\mid f(x)$. 这时, 把$g(x)$叫做$f(x)$ 的**因式**, 把$f(x)$ 叫做$g(x)$ 的**倍式**. 否则, 就称$g(x)$ 不能整除$f(x)$ 或者$f(x)$ 不能被$g(x)$ 整除,记作$g(x)\nmid f(x)$.

例11.2.1 **Z**$[X]$ 中的$2x+3\mid 2x^2+3x$, $x^2+1\mid x^4-1$.

多项式整除具有传递性, 即

定理11.2.1 设$f(x),\ g(x),\ h(x)$ 是整环R 上的多项式, 其中$g(x)\neq 0,\ h(x)\neq 0$. 若 $g(x)\mid f(x),\ \ h(x)\mid g(x)$, 则$h(x)\mid f(x)$.

证 设 $g(x)\mid f(x),\ \ h(x)\mid g(x)$, 根据整除的定义, 分别存在多项式$q_1(x),\ q_2(x)$ 使得

$$f(x)=q_1(x)\cdot g(x),\quad g(x)=q_2(x)\cdot h(x).$$

因此, 我们有

$$f(x)=q_1(x)\cdot g(x)=q_1(x)\cdot(q_2(x)\cdot g(x))=q(x)\cdot h(x).$$

因为$q(x)=q_1(x)\cdot q_2(x)$ 是多项式, 所以根据整除的定义, 有$h(x)\mid f(x)$. 证毕

在多项式$f(x)$, $g(x)$ 的线性组合中, 整除的性质是保持的.

定 理11.2.2 设$f(x)$, $g(x)$, $h(x) \neq 0$ 是整环R 上的多项式. 若$h(x) \mid f(x)$, $h(x) \mid g(x)$, 则对任意多项式$s(x)$, $t(x)$, 有

$$h(x) \mid s(x) \cdot f(x) + t(x) \cdot g(x).$$

证 设$h(x) \mid f(x)$, $h(x) \mid g(x)$, 那么存在两个多项式$q_1(x)$, $q_2(x)$ 分别使得

$$f(x) = q_1(x) \cdot h(x), \quad g(x) = q_2(x) \cdot h(x).$$

因此,

$$\begin{aligned} s(x) \cdot f(x) + t(x) \cdot g(x) &= s(x)(q_1(x) \cdot h(x)) + t(x)(q_2(x) \cdot h(x)) \\ &= (s(x) \cdot q_1(x) + t(x) \cdot q_2(x)) \cdot h(x). \end{aligned}$$

因为$s(x) \cdot q_1(x) + t(x) \cdot q_2(x)$ 是多项式, 所以$s(x) \cdot f(x) + t(x) \cdot g(x)$ 被$h(x)$ 整除. 证毕

前面我们考虑了多项式整除和因式, 现在考虑对于乘法的次数最小的多项式, 也就是不能继续分解的多项式, 即下面的不可约多项式:

定义11.2.2 设$f(x)$ 是整环R 上的非常数多项式. 如果除了显然因式1 和$f(x)$ 外, $f(x)$ 没有其它非常数因式, 那么, $f(x)$ 叫做**不可约多项式**, 否则, $f(x)$ 叫做**合式**.

多项式是否可约与所在的环或域相关.

例11.2.2 多项式x^2+1 在$\mathbf{Z}[x]$ 中是不可约的, 但在$\mathbf{F}_2[x]$ 中是可约的.

例11.2.3 在$\mathbf{F}_2[x]$ 中的4 次以下的不可约多项式和可约多项式.

次数	不可约多项式	可约多项式
1	$x, x+1$	
2	x^2+x+1	$x^2,\ x^2+1=(x+1)^2,\ x^2+x$
3	$x^3+x+1,\ x^3+x^2+1$	$x^3,\ x^3+1=(x+1)(x^2+x+1),\ x^3+x$ $x^3+x^2+x,\ x^3+x^2+x+1=(x+1)(x^2+1)$
4	$x^4+x+1,\ x^4+x^3+1$ $x^4+x^3+x^2+x+1$	$x^4,\ x^4+1,\ x^4+x,\ x^4+x^2,\ x^4+x^3,\ x^4+x^2+1$ $x^4+x^2+x,\ x^4+x^3+x,\ x^4+x^3+x^2,\ x^4+x^2+x+1$ $x^4+x^3+x+1,\ x^4+x^3+x^2+1, x^4+x^3+x^2+x$

下面我们要证明域K 上的每个可约多项式必有不可约因式.

定理11.2.3 设$f(x)$ 是域K 上的n 次可约多项式, $p(x)$ 是$f(x)$ 的次数最小的非常数因式. 则$p(x)$ 一定是不可约多项式, 且$\deg\ p \leq \frac{1}{2}\deg\ f$.

证 反证法. 如果$p(x)$ 是可约多项式, 则存在多项式$q(x)$, $1 \leq \deg\ q(x) < n$, 使得$q(x) \mid p(x)$. 但$p(x) \mid f(x)$, 根据多项式整除的传递性(定理11.2.1), 我们有$q(x) \mid f(x)$. 这与$p(x)$ 是$f(x)$ 的次数最小的非常数因式矛盾. 所以, $p(x)$ 是不可约多项式.

因为$f(x)$ 是可约多项式, 所以存在多项式$f_1(x)$ 使得

$$f(x) = f_1(x) \cdot p(x), \quad 1 \leq \deg\ p \leq \deg\ f_1 < n.$$

因此, $\deg\ p \leq n/2$. 证毕

注 定理11.2.3 告知我们, 不可约多项式为乘法的最小单元.

根据定理11.2.3, 可约多项式$f(x)$ 的次数最小的非常数因式为不可约多项式, 且$\deg\ p \leq (\deg\ f)/2$. 由此, 我们立即得到一个判断多项式是否为不可约多项式的法则.

定理11.2.4 设$f(x)$ 是域K 上的多项式. 如果对所有的不可约多项式$p(x)$, $\deg\ p \leq \frac{1}{2}\deg\ f$, 都有$p(x) \nmid f(x)$, 则$f(x)$ 一定是不可约多项式.

11.3 多项式欧几里得除法

本节考虑多项式欧几里得除法.

定理11.3.1 设$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$, $g(x)=x^m+\cdots+b_1x+b_0$ 是整环R 上的两个多项式, 则一定存在多项式$q(x)$ 和$r(x)$ 使得

$$f(x)=q(x)\cdot g(x)+r(x),\quad \deg\ r<\deg\ g. \tag{6}$$

证 我们对$f(x)$ 的次数$\deg f=n$ 作数学归纳法.

(i) 如果$\deg f<\deg g$, 则取$q(x)=0,\ r(x)=f(x)$. 结论成立.

(ii) 设$\deg f\geq\deg g$. 假设结论对$\deg f<n$ 的多项式成立.

对于$\deg f=n\geq\deg g$, 我们有

$$\begin{aligned}&f(x)-a_nx^{n-m}\cdot g(x)\\ =\ &(a_{n-1}-a_nb_{m-1})x^{n-1}+\cdots+(a_{n-m}-a_nb_0)x^{n-m}+a_{n-m-1}x^{n-m-1}+\cdots+a_0.\end{aligned}$$

这说明$f(x)-a_nx^{n-m}\cdot g(x)$ 是次数$\leq n-1$ 的多项式. 对其运用归纳假设或情形(I), 存在整系数多项式$q_1(x)$ 和$r_1(x)$ 使得

$$f(x)-a_nx^{n-m}\cdot g(x)=q_1(x)\cdot g(x)+r_1(x),\quad \deg\ r_1(x)<\deg\ g(x).$$

因此, $q(x)=a_nx^{n-m}+g_1(x),\ r(x)=r_1(x)$ 为所求.

根据数学归纳法原理, 结论是成立的. 证毕

定义11.3.1 (6) 式中的$q(x)$ 叫做$f(x)$ 被$g(x)$ 除所得的**不完全商**, $r(x)$ 叫做$f(x)$ 被$g(x)$ 除所得的**余式**.

定理11.3.1 叫做**多项式欧几里得除法**.

推论1 设$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是整环R 上的多项式, $a\in R$, 则一定存在多项式$q(x)$ 和常数$c=f(a)$ 使得

$$f(x)=q(x)\cdot(x-a)+f(a).$$

证 根据定理11.3.1, 对于$f(x), g(x)=x-a\in R[x]$, 存在多项式$q(x), r(x)$ 使得

$$f(x)=q(x)\cdot g(x)+r(x),\quad \deg\ r<\deg\ g.$$

因为$\deg\ g=1,\ \deg\ r<\deg\ g$, 所以$\deg\ r=0,\ r(x)=c\in R$. 即有

$$f(x)=q(x)\cdot(x-a)+c.$$

特别, 取$x=a$, 有$c=f(a)$. 证毕

推论2 设$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是整环R 上的多项式, $a\in R$, 则$x-a\mid f(x)$的充要条件是$f(a)=0$.

证 根据推论1, 存在$q(x)\in R[x]$, 使得

$$f(x)=q(x)\cdot(x-a)+f(a).$$

因此, $x-a\mid f(x)$的充要条件是$f(a)=0$. 证毕

定理11.3.1 所论述的是整环上的多项式除法, 因此须对除式$g(x)$ 的作首项系数为1 的要求. 对于域上的多项式, 就不需要作要求. 为便于应用, 我们给出如下表述.

定理11.3.2 设

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,\ g(x) = b_m x^m + \cdots + b_1 x + b_0,\ b_m \neq 0$$

是域**K** 上的两个多项式, 则一定存在多项式$q(x),\ r(x) \in \mathbf{K}[x]$ 使得

$$f(x) = q(x) \cdot g(x) + r(x), \quad \deg\ r < \deg\ g. \tag{7}$$

证 我们对$f(x)$ 的次数$\deg f = n$ 作数学归纳法.

(i) 如果$\deg f < \deg g$, 则取$q(x) = 0,\ r(x) = f(x)$. 结论成立.

(ii) 设$\deg f \geq \deg g$. 假设结论对$\deg f < n$ 的多项式成立.
对于$\deg f = n \geq \deg g$, 我们有

$$
\begin{aligned}
& f(x) - (a_n \cdot b_m^{-1}) x^{n-m} \cdot g(x) \\
= \; & (a_{n-1} - a_n \cdot b_m^{-1} b_{m-1}) x^{n-1} + \cdots + (a_{n-m} - a_n \cdot b_m^{-1} b_0) x^{n-m} \\
& + a_{n-m-1} x^{n-m-1} + \cdots + a_0.
\end{aligned}
$$

这说明$f(x) - (a_n \cdot b_m^{-1}) x^{n-m} \cdot g(x)$ 是次数$\leq n-1$ 的多项式. 对其运用归纳假设或情形(I), 存在多项式$q_1(x),\ r_1(x) \in \mathbf{K}[x]$ 使得

$$
f(x) - (a_n \cdot b_m^{-1}) x^{n-m} \cdot g(x) = q_1(x) \cdot g(x) + r_1(x), \quad \deg\ r_1(x) < \deg\ g(x).
$$

因此, $q(x) = a_n \cdot b_m^{-1} x^{n-m} + g_1(x),\ r(x) = r_1(x)$ 为所求.
根据数学归纳法原理, 结论是成立的. 证毕

例11.3.1 设$\mathbf{F}_2[x]$ 上多项式

$f(x) = x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1$, $g(x) = x^8+x^4+x^3+x+1$,

求$q(x)$ 和$r(x)$ 使得

$$f(x) = q_1(x) \cdot g(x) + r(x), \quad \deg\ r < \deg\ g.$$

解 逐次消除最高次项,

$$\begin{aligned} r_0(x) = f(x) - x^5 \cdot g(x) &= x^{11} + x^4 + x^3 + 1, \\ r_1(x) = r_0(x) - x^3 \cdot g(x) &= x^7 + x^6 + 1. \end{aligned}$$

因此, $q(x) = x^5 + x^3$, $r(x) = x^7 + x^6 + 1$.

根据多项式整除的定义和定理11.3.2, 我们有

定理11.3.3 设$f(x)$, $g(x)$ 是域**K** 上的多项式. 则$f(x)$ 被$g(x)$ 整除的充要条件是$f(x)$ 被$g(x)$ 除所得余式为0.

根据定理11.3.3 和定理11.2.4, 我们可以有效地判断一个多项式是否为不可约多项式.

例11.3.2 设$\mathbf{F}_2[x]$ 上多项式$f(x)=x^8+x^4+x^3+x+1$. 证明$f(x)$ 是不可约多项式.

解 只需对次数≤ 4 的不可约多项式$p(x)$: $x,\ x+1,\ x^2+x+1,\ x^3+x+1, x^3+x^2+1, x^4+x+1,\ x^4+x^3+1,\ x^4+x^3+x^2+x+1$, 作整除$p(x)\mid f(x)$ 是否成立的判断:

$$
\begin{array}{rcrcr}
f(x) & = & (x^7+x^3+x^2+1)\cdot x & + & 1\\
f(x) & = & (x^7+x^6+x^5+x^4+x^2+x)\cdot(x+1) & + & 1\\
f(x) & = & (x^6+x^5+x^3)\cdot(x^2+x+1) & + & x+1\\
f(x) & = & (x^5+x^3+x^2+1)\cdot(x^3+x+1) & + & x^2\\
f(x) & = & (x^5+x^4+x^3)\cdot(x^3+x^2+1) & + & x+1\\
f(x) & = & (x^4+x)\cdot(x^4+x+1) & + & x^3+x^2+1\\
f(x) & = & (x^4+x^3+x^2+x+1)\cdot(x^4+x^3+1) & + & x^3+x^2\\
f(x) & = & (x^4+x^3+1)\cdot(x^4+x^3+x^2+x+1) & + & x^3+x^2
\end{array}
$$

故$f(x)$ 是不可约多项式. 证毕

类似于整数中的最大公因数和最小公倍数, 可以给出多项式环$R[x]$ 中的最大公因式和最小公倍式.

设$f(x),\ g(x) \in R[x]$. $d(x) \in R[x]$ 叫做$f(x),\ g(x)$ 的**最大公因式**, 如果

(1) $d(x) \mid f(x),\ d(x) \mid g(x)$.

(2) 若$h(x) \mid f(x),\ h(x) \mid g(x)$, 则$h(x) \mid d(x)$.

$f(x),\ g(x)$ 的最大公因式记作$(f(x), g(x))$.

当考虑域K 上的最大公因式时, 约定其最高次项系数为1, 则最大公因式是惟一的.

$f(x)$ 与$g(x)$ 叫做**互素**(或**互质**)的, 如果它们的最大公因式$(f(x), g(x)) = 1$.

设$f(x),\ g(x)\in R[x]$. $D(x)\in R[x]$ 叫做$f(x),\ g(x)$ 的**最小公倍式**, 如果

(1) $f(x)\mid D(x),\ g(x)\mid D(x)$.

(2) 若$f(x)\mid h(x),\ g(x)\mid D(x)$, 则$D(x)\mid h(x)$.

$f(x),\ g(x)$ 的最小公倍式记作$[f(x), g(x)]$.

当考虑域**K** 上的最小公倍式时, 约定其最高次项系数为1, 则最小公倍式是惟一的.

定理11.3.4 设$f(x)$, $g(x)$, $h(x)$ 是域K 上的三个非零多项式. 如果

$$f(x) = q(x) \cdot g(x) + h(x),$$

其中$q(x)$ 是域K 上的多项式, 则$(f(x), g(x)) = (g(x), h(x))$.

证 设$d(x) = (f(x), g(x))$, $d'(x) = (g(x), h(x))$, 则$d(x) \mid f(x)$, $d(x) \mid g(x)$. 进而

$$d(x) \mid f(x) + (-q(x)) \cdot g(x) = h(x),$$

因此, $d(x)$ 是$g(x)$, $h(x)$ 的公因式, $d(x) \mid d'(x)$.
同理, $d'(x)$ 是$f(x)$, $g(x)$ 的公因式, $d'(x) \mid d(x)$.
因此, $d(x) = d'(x)$. 定理成立. 证毕

多项式广义欧几里得除法

设$f(x)$, $g(x)$ 是域K 上多项式, $\deg g \geq 1$. 记$r_{-2}(x) = f(x)$, $r_{-1}(x) = g(x)$.
反复运用多项式欧几里得除法(定理11.3.2), 我们有

$$
\begin{array}{rcrcll}
r_{-2}(x) & = & q_0(x)\cdot r_{-1}(x) & + & r_0(x), & 0 \leq \deg\ r_0 < \deg\ r_{-1}, \\
r_{-1}(x) & = & q_1(x)\cdot r_0(x) & + & r_1(x), & 0 \leq \deg\ r_1 < \deg\ r_0, \\
r_0(x) & = & q_2(x)\cdot r_1(x) & + & r_2(x), & 0 \leq \deg\ r_2 < \deg\ r_1, \\
r_1(x) & = & q_2(x)\cdot r_2(x) & + & r_3(x), & 0 \leq \deg\ r_3 < \deg\ r_2, \\
 & & \cdots\cdots & & & \\
r_{k-3}(x) & = & q_{k-1}(x)\cdot r_{k-2}(x) & + & r_{k-1}(x), & 0 \leq \deg\ r_{k-1} < \deg\ r_{k-2}, \\
r_{k-2}(x) & = & q_k(x)\cdot r_{k-1}(x) & + & r_k(x), & 0 \leq \deg\ r_k < \deg\ r_{k-1}, \\
r_{k-1}(x) & = & q_{k+1}(x)\cdot r_k(x) & + & r_{k+1}(x), & \deg\ r_{k+1} = 0.
\end{array}
\tag{8}
$$

经过有限步骤, 必然存在$k+1$ 使得$r_{k+1}(x) = 0$, 这是因为

$$0 = \deg\ r_{k+1} < \deg\ r_k < \deg\ r_{k-1} < \ldots < \deg\ r_1 < \deg\ r_0 < \deg\ r_{-1} = \deg\ g,$$

且$\deg\ g$是有限正整数.

定理11.3.5 设$f(x)$, $g(x)$ 是域K 上多项式, $\deg\ g \geq 1$, 则

$$(f(x), g(x)) = r_k(x),$$

其中$r_k(x)$ 是多项式广义欧几里得除法中最后一个非零余式.

证 应用定理11.3.4, 有

$$\begin{aligned}
(f(x), g(x)) &= (r_{-2}(x), r_{-1}(x)) \\
&= (r_{-1}(x), r_0(x)) \\
&= (r_0(x), r_1(x)) \\
&= \ \ \ldots \\
&= (r_{k-2}(x), r_{k-1}(x)) \\
&= (r_{k-1}(x), r_k(x)) \\
&= (r_k(x), 0). \\
&= r_k(x).
\end{aligned}$$

证毕

从多项式广义欧几里得除法中逐次消去

$$r_{k-1}(x),\ r_{k-2}(x),\ \ldots, r_1(x),\ r_0(x),$$

我们可找到多项式$s(x),\ t(x)$ 使得

$$s(x)\cdot f(x)+t(x)\cdot g(x)=(f(x),g(x)).$$

定理11.3.6 设$f(x),\ g(x)$ 是域K 上多项式, 则

$$s_k(x)\cdot f(x)+t_k(x)\cdot g(x)=(f(x),g(x)),$$

对于$j=0,\ 1,\ 2,\ \ldots,\ k$, 这里$s_j,\ t_j$ 归纳地定义为

$$\begin{cases} s_{-2}(x)=1,\ s_{-1}(x)=0,\ s_j(x)=(-q_j(x))\cdot s_{j-1}(x)+s_{j-2}(x), \\ t_{-2}(x)=0,\ t_{-1}(x)=1,\ t_j(x)=(-q_j(x))\cdot t_{j-1}(x)+t_{j-2}(x), \end{cases} \quad j=0,1,2,\ldots,k \tag{9}$$

其中$q_j(x)$ 是(8)式中的不完全商.

证 我们只需证明: 对于$j=-2,\ -1,\ 0,\ 1,\ \ldots,k$,

$$s_j(x)\cdot f(x)+t_j(x)\cdot g(x)=r_j(x), \tag{10}$$

其中$r_j(x)=(-q_j(x))\cdot r_{j-1}(x)+r_{j-2}(x)$ 是(8)式中的余式. 因为$(f(x),g(x))=r_k$, 所以

$$s_k\cdot f(x)+t_k\cdot g(x)=(f(x),g(x)).$$

对j 作数学归纳法来证明(10).

$j=-2$ 时, 我们有$s_{-2}(x)=1,\ t_{-2}(x)=0$, 以及

$$s_{-2}(x)\cdot f(x)+t_{-2}(x)\cdot g(x)=f(x)=r_{-2}(x).$$

结论对于$j=-2$ 成立.

$j=-1$ 时, 我们有$s_{-1}(x)=0,\ t_{-1}(x)=1$, 以及

$$s_{-1}(x)\cdot f(x)+t_{-1}(x)\cdot g(x)=g(x)=r_{-1}(x).$$

结论对于$j=-1$ 成立.

假设结论对于$-2 \le j \le k-1$ 成立. 即

$$s_j(x)\cdot f(x)+t_j(x)\cdot g(x)=r_j(x).$$

对于$j=k$, 我们有

$$r_k(x)=(-q_k(x))\cdot r_{k-1}(x)+r_{k-2}(x).$$

利用归纳假设, 我们得到

$$\begin{aligned}
r_k(x) &= (-q_k(x))(s_{k-1}(x)\cdot f(x)+t_{k-1}(x))\cdot g(x)\\
&\quad +(s_{k-2}(x)\cdot f(x)+t_{k-2}(x))\cdot g(x)\\
&= ((-q_k(x))\cdot s_{k-1}(x)+s_{k-2}(x))\cdot f(x)\\
&\quad +((-q_k(x))\cdot t_{k-1}(x)+t_{k-2}(x))\cdot g(x)\\
&= s_k(x)\cdot f(x)\ +\ t_k(x)\cdot g(x)
\end{aligned}$$

因此, 结论对于$j=k$ 成立. 根据数学归纳法原理, (9) 对所有的j 成立. 这就完成了证明. 证毕

例11.3.3 设$\mathbf{F}_2[x]$ 中有

$$f(x)=x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1,\ g(x)=x^8+x^4+x^3+x+1,$$

求多项式$s(x)$, $t(x)$ 使得 $\quad s(x)\cdot f(x)+t(x)\cdot g(x)=(f(x),g(x)).$

解 运用广义多项式欧几里得除法, 我们有

$$\begin{array}{lll}
f(x)=q_0(x)\cdot g(x)+r_0(x), & q_0(x)=x^5+x^3, & r_0(x)=x^7+x^6+1,\\
g(x)=q_1(x)\cdot r_0(x)+r_1(x), & q_1(x)=x+1, & r_1(x)=x^6+x^4+x^3,\\
r_0(x)=q_2(x)\cdot r_1(x)+r_2(x), & q_2(x)=x+1, & r_2(x)=x^5+x^3+1,\\
r_1(x)=q_3(x)\cdot r_2(x)+r_3(x), & q_3(x)=x, & r_3(x)=x^3+x,\\
r_2(x)=q_4(x)\cdot r_3(x)+r_4(x), & q_4(x)=x^2, & r_4(x)=1.
\end{array}$$

从而,

$$\begin{aligned}
r_4(x) &= q_4(x)\cdot(q_3(x)\cdot r_2(x)+r_1(x))+r_2(x)\\
&= (x^3+1)\cdot(q_2(x)\cdot r_1(x)+r_0(x))+q_4(x)\cdot r_1(x)\\
&= (x^4+x^3+x^2+x+1)\cdot(q_1(x)\cdot r_0(x)+g(x))+(x^3+1)\cdot r_0(x)\\
&= (x^5+x^3)\cdot(q_0(x)\cdot g(x)+f(x))+(x^4+x^3+x^2+x+1)\cdot g(x)\\
&= (x^5+x^3)\cdot f(x)+(x^{10}+x^6+x^4+x^3+x^2+x+1)\cdot g(x).
\end{aligned}$$

因此, $s(x)=x^5+x^3$, $t(x)=x^{10}+x^6+x^4+x^3+x^2+x+1.$

定理11.3.7 设$p(x)$ 是域$\mathbf{K}$ 上多项式环$\mathbf{K}[x]$ 中的不可约多项式. 则当多项式$a(x)$, $b(x)$ 满足$p(x) \mid a(x) \cdot b(x)$ 时, 有$p(x) \mid a(x)$, 或$p(x) \mid b(x)$.

证 假设$p(x) \mid a(x)$ 不成立, 则$(a(x), p(x)) = 1$. 根据多项式广义欧几里得除法(定理11.3.6), 可找到多项式$s(x)$, $t(x)$ 使得

$$s(x) \cdot a(x) + t(x) \cdot p(x) = 1.$$

两端同乘$b(x)$, 有$s(x) \cdot (a(x) \cdot b(x)) + (t(x) \cdot s(x)) \cdot p(x) = b(x)$. 因此,

$$p(x) \mid s(x) \cdot (a(x) \cdot b(x)) + (t(x) \cdot s(x)) \cdot p(x) = b(x).$$

证毕

11.4 多项式同余

本节考虑域$\mathbf{K}$ 上多项式环$\mathbf{K}[x]$ 中的多项式同余.

定义11.4.1 给定$\mathbf{K}[X]$ 中一个首一多项式$m(x)$. 两个多项式$f(x)$, $g(x)$叫做模$m(x)$ **同余**, 如果$m(x) \mid f(x) - g(x)$. 记作

$$f(x) \equiv g(x) \pmod{m(x)}.$$

否则, 叫做模$m(x)$ **不同余**. 记作$f(x) \not\equiv g(x) \pmod{m(x)}$.

定理11.4.1 设$m(x)$ 是域$\mathbf{K}$ 上多项式. 则$a(x)$, $b(x) \in \mathbf{K}[x]$ 使得

$$a(x) \equiv b(x) \pmod{m(x)}$$

的充要条件是存在多项式$s(x)$ 使得

$$a(x) = b(x) + s(x) \cdot m(x).$$

证 如果$a(x) \equiv b(x) \pmod{m(x)}$, 则根据多项式同余的定义, 我们

$$m(x) \mid a(x) - b(x).$$

又根据整除的定义, 存在多项式$s(x)$ 使得$a(x) - b(x) = s(x) \cdot m(x)$. 故

$$a(x) = b(x) + s(x) \cdot m(x).$$

反过来, 如果存在多项式$s(x)$ 使得$a(x) = b(x) + s(x) \cdot m(x)$, 则有

$$a(x) - b(x) = s(x) \cdot m(x).$$

根据多项式整除的定义, 我们有 $m(x) \mid a(x) - b(x)$.
再根据多项式同余的定义, 我们得到 $a(x) \equiv b(x) \pmod{m(x)}$. 证毕

模多项式同余具有等价关系的性质.

定理11.4.2 设$m(x)$ 是域K 上多项式. 则模多项式$m(x)$ 同余是等价关系, 即

i). (自反性) 对任一多项式$a(x)$, $a(x) \equiv a(x) \pmod{m(x)}$.

ii). (对称性) 若$a(x) \equiv b(x) \pmod{m(x)}$, 则$b(x) \equiv a(x) \pmod{m(x)}$.

iii). (传递性) 若$a(x) \equiv b(x) \pmod{m(x)}$, $b(x) \equiv c(x) \pmod{m(x)}$, 则$a(x) \equiv c(x) \pmod{m(x)}$.

证 我们运用定理11.4.1 来给出证明.

1. (自反性) 对任一多项式$a(x)$, 我们有$a(x) = a(x) + 0 \cdot m(x)$, 所以

$$a(x) \equiv a(x) \pmod{m(x)}.$$

2. (对称性) 若$a(x) \equiv b(x) \pmod{m(x)}$, 则存在多项式$s(x)$ 使得

$$a(x) = b(x) + s(x) \cdot m(x),$$

从而有 $b(x) = a(x) + (-s(x)) \cdot m(x)$.

因此, $b(x) \equiv a(x) \pmod{m(x)}$.

3. (传递性) 若$a(x) \equiv b(x) \pmod{m(x)}$, $b(x) \equiv c(x) \pmod{m(x)}$, 则分别存在多项式$s_1(x)$, $s_2(x)$使得

$$a(x) = b(x) + s_1(x) \cdot m(x), \qquad b(x) = c(x) + s_2(x) \cdot m(x),$$

从而 $a(x) = c(x) + (s_1(x) + s_2(x)) \cdot m(x)$.

因为$s_1(x) + s_2(x)$ 是整数, 所以

$$a(x) \equiv c(x) \pmod{m(x)}.$$

证毕

模多项式同余有运算性质.

定理11.4.3 设$m(x)$ 是域K 上多项式. 设$a_1(x),\ a_2(x),\ b_1(x),\ b_2(x)$ 是四个多项式. 如果 $a_1(x) \equiv b_1(x) \pmod{m(x)}$, $a_2(x) \equiv b_2(x) \pmod{m(x)}$,

则i) $a_1(x) + a_2(x) \equiv b_1(x) + b_2(x) \pmod{m(x)}$;

ii) $a_1(x) \cdot a_2(x) \equiv b_1(x) \cdot b_2(x) \pmod{m(x)}$.

证 依题设, 根据定理11.4.1, 分别存在多项式$s_1(x),\ s_2(x)$ 使得

$$a_1(x) = b_1(x) + s_1(x) \cdot m(x), \quad a_2(x) = b_2(x) + s_2(x) \cdot m(x),$$

从而

$$\begin{aligned} a_1(x) + a_2(x) &= b_1(x) + b_2(x) + (s_1(x) + s_2(x)) \cdot m(x), \\ a_1(x) \cdot a_2(x) &= b_1(x) \cdot b_2(x) + (s_1(x) \cdot m(x)) \cdot b_2(x) + b_1(x) \cdot (s_2(x) \cdot m(x)) \\ &\quad +(s_1(x) \cdot m(x))(s_2(x) \cdot m(x)) \\ &= b_1(x) \cdot b_2(x) + (s_1(x) + s_2(x) + s_1(x) \cdot s_2(x) \cdot m(x)) \cdot m(x). \end{aligned}$$

(交换性)

因为$s_1(x) + s_2(x),\ s_1(x) + s_2(x) + s_1(x) \cdot s_2(x) \cdot m(x)$ 都是多项式, 所以根据定理11.4.1, 我们有 $a_1(x) + a_2(x) \equiv b_1(x) + b_2(x) \pmod{m(x)}$,

及 $a_1(x) \cdot a_2(x) \equiv b_1(x) \cdot b_2(x) \pmod{m(x)}$. 即定理成立. 证毕

根据定理11.3.1, 任一多项式$f(x)$ 都与其被$m(x)$ 除的余式$r(x)$ 模$m(x)$ 同余, 该余式$r(x)$ 叫做$f(x)$ 模$m(x)$ 的最小余式, 记为$(f(x) \pmod{m(x)})$.

设$p(x)$ 是$\mathbf{K}[X]$ 中的多项式, 则$(p(x)) = \{f(x) \mid f(x) \in \mathbf{K}[x],\ p(x) \mid f(x)\}$ 是$\mathbf{K}[X]$ 中的理想. 由此得到商环$R/(p(x))$. 该商环上的运算法则为:

加法:

$$f(x) + g(x) = ((f+g)(x) \pmod{p(x)}). \tag{11}$$

乘法:

$$f(x) \cdot g(x) = ((fg)(x) \pmod{p(x)}). \tag{12}$$

定理11.4.4 设K 是一个域. $p(x)$ 是$\mathbf{K}[X]$ 中的不可约多项式. 则商环$\mathbf{K}[X]/(p(x))$ 对于加法运算(11) 和乘法(12)运算法则构成一个域.

证 我们只需证明$\mathbf{K}[X]/(p(x))$ 中的非零元$f(x) \pmod{p(x)}$ 为可逆元. 事实上, 对于满足$f(x) \not\equiv 0 \pmod{p(x)}$ 的多项式$f(x)$, 有$(f(x), p(x)) = 1$. 根据定理11.3.6, 存在多项式$s(x)$, $t(x)$ 使得

$$s(x) \cdot f(x) + t(x) \cdot p(x) = 1.$$

从而,

$$s(x)f(x) \equiv 1 \pmod{p(x)}.$$

这说明$f(x) \pmod{p(x)}$ 为可逆元, $s(x) \pmod{p(x)}$ 为其逆元. 证毕

下面三个例子将用于AKS 算法的证明.

例11.4.1 设n 是正整数, S 是有单位元环R 的子集. 设$p(x)$ 是R 上的多项式, 满足$p(x) \mid p(x^n)$. 如果在多项式环$R[x]$ 中, 对所有的$b \in S$, 都有

$$(x+b)^n \equiv x^n + b \pmod{p(x)}.$$

则对任意整数$k \geq 0$, 有 $(x+b)^{n^k} \equiv x^{n^k} + b \pmod{p(x)}$.

证 我们对k 作数学归纳法. $k=0$ 时, 结论显然成立.

$k=1$ 时, 就是假设条件 $(x+b)^n \equiv x^n + b \pmod{p(x)}$. 结论成立.

假设k 时, 结论成立, 即 $(x+b)^{n^k} \equiv x^{n^k} + b \pmod{p(x)}$.

两端作n 次方, 有 $(x+b)^{n^{k+1}} \equiv (x^{n^k} + b)^n \pmod{p(x)}$.

根据假设, 用x^{n^k} 代替x, 有

$$(x^{n^k}+b)^n \equiv (x^{n^k})^n + b \equiv x^{n^{k+1}} + b \pmod{p(x^{n^k})}.$$

但由假设, 有$p(x) \mid p(x^n)$, 进而 $p(x^n) \mid p(x^{n^2}),\ \ldots,\ p(x^{n^{k-1}}) \mid p(x^{n^k})$.

因此, $p(x) \mid p(x^{n^k})$, $(x^{n^k}+b)^n \equiv (x^{n^k})^n + b \equiv x^{n^{k+1}} + b \pmod{p(x)}$.

故 $(x+b)^{n^{k+1}} \equiv (x^{n^k})^n + b \equiv x^{n^{k+1}} + b \pmod{p(x)}$.

这就是说, 对于$k+1$ 结论成立. 根据数学归纳法原理, 结论对任意的$k \geq 1$ 成立. 证毕

例11.4.2 设$n, r \geq 2$ 是整数, S 是环$R = \mathbf{Z}/n\mathbf{Z}$ 的子集. 如果在多项式环$R[x]$ 中, 对所有的$b \in S$, 都有

$$(x+b)^n \equiv x^n + b \pmod{x^r - 1}.$$

则对任意整数$k \geq 0$, 有

$$(x+b)^{n^k} \equiv x^{n^k} + b \pmod{x^r - 1}.$$

证 在例11.4.1 中取$p(x) = x^r - 1$ 即得结论. 证毕

例11.4.3 设$n, m, r \geq 2$ 是整数. 如果$m \equiv n \pmod r$, 则对任意多项式$g(x)$, 有

$$g(x^m) \equiv g(x^n) \pmod{x^r - 1}.$$

证 不妨设$m \geq n$. 因为$m \equiv n \pmod r$, 所以存在整数$k \geq 0$ 使得$m = k \cdot r + n$.

$k = 0$时, 结论显然成立. $k \geq 1$时, 设$g(x) = \sum_{i=0}^{N} b_i x^i$, 则

$$g(x^m) - g(x^n) = \sum_{i=0}^{N} b_i x^{in}((x^r)^{ik} - 1) = (x^r - 1) \sum_{i=0}^{N} b_i x^{in}((x^r)^{ik-1} + \cdots + x^r + 1).$$

因此, 结论成立. 证毕

11.5 本原多项式

本节考虑$\mathbf{F}_p$ 上的不可约多项式$p(x)$, 及其所生成的有限域.

定理11.5.1 设p 是素数. 设$p(x)$ 是$\mathbf{F}_p[X]$ 中的n 次不可约多项式, 则

$$\mathbf{F}_p[X]/(p(x)) = \{a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \mid a_i \in \mathbf{F}_p\}.$$

记为$\mathbf{F}_{p^n}$. 这个域的元素个数为p^n.

证 根据定理11.4.4, $\mathbf{F}_p[X]/(p(x))$ 构成一个域, 且元素形式为

$$a_{n-1}x^{n-1} + \cdots + a_1x + a_0, \qquad a_i \in \mathbf{F}_p.$$

因为$|\mathbf{F}_p| = p$, 所以$|\mathbf{F}_{p^n}| = p^n$. 证毕

例11.5.1 设$p(x) = x^8 + x^4 + x^3 + x + 1$ 是$\mathbf{F}_2[X]$ 中的8 次不可约多项式. 我们有

$$\mathbf{F}_{2^8} = \mathbf{F}_2[X]/(x^8+x^4+x^3+x+1) = \{a_7x^7+\cdots+a_1x+a_0 \mid a_i \in \{0,1\}\}.$$

对于$f(x) = x^6 + x^3 + x + 1,\ g(x) = x^5 + x^2 + x + 1 \in \mathbf{F}_2[X]$, 有

$$f(x) + g(x) = x^6 + x^3 + x^5 + x^2 \pmod{p(x)},$$

$$f(x) \cdot g(x) = x^6 + x^3 + 1 \pmod{p(x)}.$$

进一步, 设$p(x)$ 是$\mathbf{F}_p[X]$ 中的n 次不可约多项式. 考察序列$\{x^k \pmod{p(x)}\}_{k\in\mathbf{N}}$ 的性质.
因为序列$\{x^k \pmod{p(x)}\}_{k\in\mathbf{N}}$ 中不同元素个数为p^n-1的个数, 因此存在k, l 使得

$$x^k \equiv x^l \pmod{p(x)}.$$

不妨设$k>l$, 则有

$$x^{k-l} \equiv 1 \pmod{p(x)}.$$

定义11.5.1 设p 是素数. 设$f(x)$ 是$\mathbf{F}_p[X]$ 中的多项式. 则使得

$$x^e \equiv 1 \pmod{f(x)}$$

成立的的最小正整数e 叫做$f(x)$ 在$\mathbf{F}_p$ 上的**指数**, 记作$\mathrm{ord}_p(f(x))$.
如果$\mathrm{ord}_p(f(x)) = p^n-1$, 则称$f(x)$ 为$\mathbf{F}_p$ 上的**本原多项式**.
注 n 次多项式$f(x)$ 在$\mathbf{F}_p$ 上的指数$\mathrm{ord}_p(f(x))$ 实际上是$\mathbf{F}_p$ 上序列$u=\{u_k = x^k \pmod{f(x)} \mid k\geq 1\}$ 的最小周期$p(u(f(x)))$ (参见定义B.0.1), 且$p(u(f(x)))\leq p^n-1$. 使得$p(u(f(x)))=p^n-1$ 的n 次多项式为本原多项式. 进一步, 当$f(x)$ 是不可约多项式时, 该最小周期$p(u(f(x)))$ 是p^n-1 的因子.

定理11.5.2 设p 是素数. 设$f(x)$, $g(x)$ 是$\mathbf{F}_p$ 上的多项式, 则

(i) 若整数d 使得$x^d \equiv 1 \pmod{f(x)}$. 则$\mathrm{ord}_p(f(x)) \mid d$.

(ii) 如果$g(x) \mid f(x)$, 则

$$\mathrm{ord}_p(g(x)) \mid \mathrm{ord}_p(f(x)).$$

(iii) 如果$(f(x), g(x)) = 1$, 则

$$\mathrm{ord}_p(f(x) \cdot g(x)) = [\mathrm{ord}_p(f(x)), \mathrm{ord}_p(g(x))].$$

(iv) 如果$f(x)$ 是$\mathbf{F}_p$ 上中的n 次不可约多项式, 则

$$\mathrm{ord}_p(f(x)) \mid p^n - 1.$$

证 (i) 令$e = \mathrm{ord}_p(f(x))$. 若$e \nmid d$, 根据欧几里得除法(定理1.1.9), 存在整数s, r 使得$d = s \cdot e + r$, $\quad 0 \le r < e$. 当$r \neq 0$ 时, 有

$$x^r \equiv x^r (x^e)^s = x^d \equiv 1 \pmod{f(x)}.$$

这与e 的最小性矛盾.

(ii) 令$e = \mathrm{ord}_p(f(x))$, $e' = \mathrm{ord}_p(g(x))$. 根据定义, 我们有

$$x^e \equiv 1 \pmod{f(x)}.$$

又$g(x) \mid f(x)$, 所以

$$x^e \equiv 1 \pmod{g(x)}.$$

因此, $e' \mid e$.

(iii) 令$e = \mathrm{ord}_p(f(x))$, $e' = \mathrm{ord}_p(g(x))$, $e'' = \mathrm{ord}_p(f(x) \cdot g(x))$. 由(ii) 我们有$e \mid e''$, $e' \mid e''$, 根据定理1.4.5, 有$[e, e'] \mid e''$.

又由

$$x^{[e,e']} \equiv (x^e)^{\frac{[e,e']}{e}} \equiv 1 \pmod{f(x)}, \quad x^{[e,e']} \equiv (x^{e'})^{\frac{[e,e']}{e'}} \equiv 1 \pmod{g(x)},$$

得到

$$x^{[e,e']} \equiv 1 \pmod{f(x) \cdot g(x)}.$$

从而, $e'' \mid [e, e']$. 故

$$\mathrm{ord}_p(f(x) \cdot g(x)) = [\mathrm{ord}_p(f(x)), \mathrm{ord}_p(g(x))].$$

访问主页
标题页
目录页
第 47 页 共 77 页
返回
全屏显示
关闭
退出

(iv) 根据定理11.5.1, $\mathbf{F}_p[X](f(x))$ 中有p^n-1 个元素:

$$a_1(x),\ a_2(x),\ \ldots,\ a_{p^n-2}(x),\ a_{p^n-1}(x),$$

且

$$x\cdot a_1(x),\ x\cdot a_2(x),\ \ldots,\ x\cdot a_{p^n-2}(x),\ x\cdot a_{p^n-1}(x)$$

是这些元素的一个置换, 因此有

$$(x\cdot a_1(x))(x\cdot a_2(x))\cdots,(x\cdot a_{p^n-1}(x))\equiv a_1(x)\cdot a_2(x)\cdots a_{p^n-1}(x)\ (\mathrm{mod}\ f(x)).$$

变形得到

$$(a_1(x)\cdot a_2(x)\cdots a_{p^n-1}(x))(x^{p^n-1}-1)\equiv 0\ (\mathrm{mod}\ f(x)).$$

因为$((a_1(x)\cdot a_2(x)\cdots a_{p^n-1}(x)),f(x))=1$, 所以

$$x^{p^n-1}\equiv 1\ (\mathrm{mod}\ f(x)).$$

最后, 由(i) 得到$\mathrm{ord}_p(f(x))\mid p^n-1$. 证毕

定理11.5.3 设p 是素数. 设$f(x)$ 是$\mathbf{F}_p$ 上的本原多项式, 则$f(x)$ 是$\mathbf{F}_p$ 上的不可约多项式,

证 若$f(x)$ 是$\mathbf{F}_p$ 上的可约多项式, 则存在非常数多项式$f_1(x)$, $f_2(x)$ 使得$f(x) = f_1(x) \cdot f_2(x)$. 不妨设$(f_1(x), f_2(x)) = 1$. 令$n = \deg\ f(x)$, $n_1 = \deg\ f_1(x)$, $n_2 = \deg\ f_2(x)$. 根据定理11.5.2, 我们有

$$\mathrm{ord}_p(f(x)) = [\mathrm{ord}_p(f_1(x)), \mathrm{ord}_p(f_2(x))] \leq (p^{n_1}-1)(p^{n_2}-1) < (p^{n_1+n_2}-1).$$

这与$f(x)$ 是本原多项式矛盾. 定理成立. 证毕

类似于模p 原根的判别方法(定理5.2.2), 也有$\mathbf{F}_p$ 上本原元多项式的判别方法.

定理11.5.4 设p 是素数, n 正整数. 设$f(x)$ 是$\mathbf{F}_p[X]$ 中的n 次多项式. 如果

(i) $x^{p^n-1} \equiv 1 \pmod{f(x)}$.

(ii) 对于p^n-1 的所有不同素因数是$q_1, \ldots, q_s$,

$$x^{\frac{p^n-1}{q_i}} \not\equiv 1 \pmod{f(x)}, \quad i = 1, \ldots, s. \tag{13}$$

则$f(x)$ 是n 次本原多项式.

证 令$e = \mathrm{ord}_p(f(x))$. 由假设条件(i), 有$e \mid p^n-1$. 如果$e < p^n-1$, 则存在一个素数q_j 使得$q_j \mid \dfrac{p^n-1}{e}$. 即

$$\frac{p^n-1}{e} = u \cdot q_j, \quad \text{或} \quad \frac{p-1}{q_j} = u \cdot e.$$

进而

$$x^{\frac{p^n-1}{q_j}} = (x^e)^u \equiv 1 \pmod{f(x)}.$$

与假设(13)矛盾. 证毕

例11.5.2 在$\mathbf{F}_2[X]$ 中的不可约多项式和本原多项式.

2 次多项式x^2+x+1 是本原多项式.

3 次多项式x^3+x+1, x^3+x^2+1 都是本原多项式.

4 次多项式x^4+x+1, x^4+x^3+1 都是本原多项式, 但不可约多项式$x^4+x^3+x^2+x+1$ 不是本原多项式$(\mathrm{ord}_p(f(x))=5)$.

5 次多项式x^5+x^2+1, x^5+x^3+1, $x^5+x^3+x^2+x+1$, $x^5+x^4+x^2+x+1$, $x^5+x^4+x^3+x+1$, $x^5+x^4+x^3+x^2+1$ 都是本原多项式.

6 次多项式x^6+x+1, x^6+x^5+1, $x^6+x^4+x^3+x+1$, $x^6+x^5+x^2+x+1$ 都是本原多项式, 但不可约多项式x^6+x^3+1 不是本原多项式$(\mathrm{ord}_p(f(x))=9)$.

例11.5.3 证明: $f(x) = x^8 + x^4 + x^3 + x^2 + 1$ 是$\mathbf{F}_2[X]$ 中的本原多项式.

解 因为$n = 8,\ 2^n - 1 = 255 = 3 \cdot 5 \cdot 17$,其素因数为$q_1 = 17,\ q_2 = 5,\ q_3 = 3$. 进而, $(2^n-1)/q_1 = 15,\ (2^n-1)/q_2 = 51, (2^n-1)/q_3 = 85,$. 根据定理11.5.4, 只需验证(13),即x^{255} 模$f(x)$ 是否同余于1 和$x^{15},\ x^{51},\ x^{85}$ 模$f(x)$ 是否都不同余于1:

$$\begin{aligned} x^{255} &\equiv 1, & x^{15} &\equiv x^5 + x^2 + x, \\ x^{51} &\equiv x^3 + x, & x^{85} &\equiv x^7 + x^6 + x^4 + x^2 + x \pmod{f(x)}, \end{aligned}$$

故$f(x)$ 是本原多项式. 证毕

例11.5.4 证明: $f(x)=x^8+x^4+x^3+x+1$ 不是$\mathbf{F}_2[X]$ 中的本原多项式.

解 因为$n=8,\ 2^n-1=255=3\cdot5\cdot17$,其素因数为$q_1=17,\ q_2=5,\ q_3=3$. 进而, $(2^n-1)/q_1=15,\ (2^n-1)/q_2=51, (2^n-1)/q_3=85,$. 根据定理11.5.5, 只需验证(13), 即x^{255} 模$f(x)$ 是否同余于1和$x^{15},\ x^{51},\ x^{85}$ 模$f(x)$ 是否都不同余于1:

$$\begin{aligned}
&x^{255}\equiv 1,\ \ x^{15}\equiv x^5+x^3+x^2+x+1,\\
&x^{51}\equiv 1,\quad x^{85}\equiv x^7+x^5+x^4+x^3+x^2+1\pmod{f(x)},
\end{aligned}$$

故$f(x)$ 不是本原多项式. 证毕

11.6 多项式理想

定理11.6.1 域K 上多项式环$\mathbf{K}[x]$ 是主理想环, 且理想$I=(a(x))$ 的表达式为

$$I=(a(x))=\{s(x)\cdot a(x)\mid s(x)\in\mathbf{K}[x]\}$$

证 设I 是$\mathbf{K}[x]$ 中的一个非零理想. 则存在非零多项式$b(x)\in I$. 设$a(x)$ 是I 中的次数最小的多项式, 则$I=(a(x))=\{s(x)\cdot a(x)\mid s(x)\in\mathbf{K}[x]\}$. 事实上, 对任意$b(x)\in I$, 存在多项式$s(x)$, $r(x)$ 使得

$$b(x)=s(x)\cdot a(x)+r(x),\quad 0\le\deg\ r(x)<\deg\ a(x).$$

这样, 由$b(x)\in I$ 及$(-s(x))\cdot a(x)\in I$, 得到$r(x)=b(x)+(-s(x))\cdot a(x)\in I$. 这与$a(x)$ 是I 中次数最小的多项式矛盾. 因此, $r(x)=0$, $b(x)=s(x)\cdot a(x)\in(a(x))$. 从而$I\subset(a(x))$. 又显然有$(a(x))\subset I$. 故$I=(a(x))$, $\mathbf{K}[x]$ 是主理想环. 证毕

推论 设$I = (a(x))$ 是多项式环$\mathbf{K}[x]$ 中的理想. 则多项式$b(x) \in I$ 的充要条件是$a(x) \mid b(x)$.

证 必要性. 设$b(x) \in I = (a(x))$, 则存在多项式$s(x)$ 使得$b(x) = s(x) \cdot a(x)$, 因此, $a(x) \mid b(x)$.

充分性. 设$a(x) \mid b(x)$, 则存在多项式$s(x)$ 使得$b(x) = s(x) \cdot a(x)$, 因此, $b(x) \in I = (a(x))$. 证毕

定理11.6.2 设$\mathbf{K}[x]$ 是域$\mathbf{K}$ 上多项式环. 如果$p(x)$ 是$\mathbf{K}[x]$ 中的不可约多项式, 则理想$P = (p(x))$ 是素理想.

证 设$\mathbf{K}[x]$ 中的多项式$a(x)$, $b(x)$ 使得$a(x) \cdot b(x) \in P$, 则$p(x) \mid a(x) \cdot b(x)$. 根据定理11.3.7, 有$p(x) \mid a(x)$ 或$p(x) \mid b(x)$, 从而$a(x) \in P$ 或$b(x) \in P$. 这说明$P = (p(x))$ 是素理想. 证毕

11.7 多项式结式与判别式

定义11.7.1 设域K 上的多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,\ g(x)=b_mx^m+\cdots+b_1x+b_0.$$

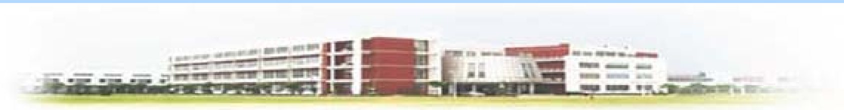
则称行列式

$$\begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \cdots & 0 & 0 & 0 \\ 0 & a_n & a_{n-1} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_1 & a_0 & 0 \\ 0 & 0 & 0 & \cdots & a_2 & a_1 & a_0 \\ b_m & b_{m-1} & b_{m-2} & \cdots & 0 & 0 & 0 \\ 0 & b_m & b_{m-1} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & b_1 & b_0 & 0 \\ 0 & 0 & 0 & \cdots & b_2 & b_1 & b_0 \end{vmatrix} \begin{array}{l} \left.\begin{array}{l} \\ \\ \\ \\ \\ \end{array}\right\} m\text{行} \\ \left.\begin{array}{l} \\ \\ \\ \\ \\ \end{array}\right\} n\text{行} \end{array} \tag{14}$$

为多项式$f(x)$, $g(x)$ 的结式, 记作$R(f,g)$.

这里, 行列式的前m 行是多项式$f(x)$ 的系数$a_n,\ a_{n-1},\ a_{n-2},\ \cdots,\ a_2,\ a_1,\ a_0$ 分别移位$0,\ 1,\ \ldots,\ m-1$ 得到, 其它项以0 补充. 行列式的后n 行是多项式$g(x)$ 的系数$b_m,\ b_{m-1},\ b_{m-2},\ \cdots,\ b_2,\ b_1,\ b_0$ 分别移位$0,\ 1,\ \ldots,\ n-1$ 得到, 其它项以0 补充.

访问主页
标题页
目录页
第 56 页 共 77 页
返回
全屏显示
关闭
退出



例如, 设域**K** 上$f(x)=a_4x^4+a_3x^3+a_2x^2+a_1x+a_0,\ g(x)=b_3x^3+b_2x^2+b_1x+b_0$. 则

$$R(f,g)=\begin{vmatrix} a_4 & a_3 & a_2 & a_1 & a_0 & 0 & 0 \\ 0 & a_4 & a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & 0 & a_4 & a_3 & a_2 & a_1 & a_0 \\ b_3 & b_2 & b_1 & b_0 & 0 & 0 & 0 \\ 0 & b_3 & b_2 & b_1 & b_0 & 0 & 0 \\ 0 & 0 & b_3 & b_2 & b_1 & b_0 & 0 \\ 0 & 0 & 0 & b_3 & b_2 & b_1 & b_0 \end{vmatrix} \begin{array}{l} \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} 3\text{行} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} 4\text{行} \end{array}$$

例11.7.1 设 $f(x)=x^3+1,\ g(x)=x^2+x+1$ 是域$\mathbf{F}_2$ 上多项式. 则

$$R(f,g)=\begin{vmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{vmatrix}=0.$$

解

$$R(f,g)=\begin{vmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{vmatrix}=\begin{vmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{vmatrix}=\begin{vmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{vmatrix}=0.$$

例11.7.2 设$f(x) = a_2x^2 + a_1x + a_0,\ g(x) = b_1x + b_0$ 是域K 上多项式. 则

$$R(f,g) = \begin{vmatrix} a_2 & a_1 & a_0 \\ b_1 & b_0 & 0 \\ 0 & b_1 & b_0 \end{vmatrix} = a_2b_0^2 + a_0b_1^2 - a_1b_0b_1. \tag{15}$$

设域K 上的多项式 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_2x^2+a_1x+a_0.$
则称

$$f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+2a_2x+a_1 \tag{16}$$

为 $f(x)$ 的导式.

定义11.7.1 设域K 上的多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_2x^2+a_1x+a_0.$$

则称 $f(x)$ 与其导式 $f'(x)$ 的结式 $R(f,f')$ 为 $f(x)$ 的判别式, 记作 $\Delta(f)$, 即

$$\Delta(f)=\begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \cdots & 0 & 0 & 0 \\ 0 & a_n & a_{n-1} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_1 & a_0 & 0 \\ 0 & 0 & 0 & \cdots & a_2 & a_1 & a_0 \\ na_n & (n-1)a_{n-1} & (n-2)a_{n-2} & \cdots & 0 & 0 & 0 \\ 0 & na_n & (n-1)a_{n-1} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 2a_2 & a_1 & 0 \\ 0 & 0 & 0 & \cdots & 3a_3 & 2a_2 & a_1 \end{vmatrix} \tag{17}$$

例11.7.3 设 $f(x) = ax^2+bx+c$ 是域K 上多项式, 导式 $f'(x) = 2ax+b$. 则 $f(x)$ 的判别式 $\Delta(f) = a(4ac-b^2)$.

$$\Delta(f) = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = \begin{vmatrix} a & b & c \\ 0 & -b & -2c \\ 0 & 2a & b \end{vmatrix} = ab^2+4a^2c-2ab^2 = a(4ac-b^2). \tag{18}$$

这里先将第1 行的 (-2) 倍加到第2 行, 再作计算.

例11.7.4 设$f(x) = ax^3 + bx + c$ 是域K 上多项式, 导式$f'(x) = 3ax^2 + b$. 则$f(x)$ 的判别式$\Delta(f) = a^2(4b^3 + 27ac^2)$.

$$\Delta(f) = \begin{vmatrix} a & 0 & b & c & 0 \\ 0 & a & 0 & b & c \\ 3a & 0 & b & 0 & 0 \\ 0 & 3a & 0 & b & 0 \\ 0 & 0 & 3a & 0 & b \end{vmatrix} = \begin{vmatrix} a & 0 & b & c & 0 \\ 0 & a & 0 & b & c \\ 0 & 0 & -2b & -3c & 0 \\ 0 & 0 & 0 & -2b & -3c \\ 0 & 0 & 3a & 0 & b \end{vmatrix} = a^2(4b^3+27ac^2). \tag{19}$$

这里先将第1 行的(-3) 倍加到第3 行, 再将第2 行的(-3) 倍加到第4 行, 最后作计算.

定理11.7.1 设有域K 上的n 次多项式$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 和m 次多项式$g(x)=b_mx^m+\cdots+b_1x+b_0$. 则存在多项式

$$s(x),\ t(x)\in \mathbf{Z}[a_0,a_1,\ldots,a_n,b_0,b_1,\ldots,b_m][x],$$

使得

$$s(x)\cdot f(x)+t(x)\cdot g(x)=R(f,g). \tag{20}$$

证 对$f(x),\ g(x)$ 的结式作计算, 分别将第$n+m-1$ 列的x 倍加到第$n+m$ 列, 第$n+m-2$ 列的x^2 倍加到第$n+m$ 列,. . ., 第$n+m-j$ 列的x^j 倍加到第$n+m$ 列, . . ., 第1 列的x^{n+m-1} 倍加到第$n+m$ 列, 得到

$$R(f,g)=\begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \cdots & 0 & 0 & x^{m-1}\cdot f(x) \\ 0 & a_n & a_{n-1} & \cdots & 0 & 0 & x^{m-2}\cdot f(x) \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_1 & a_0 & x\cdot f(x) \\ 0 & 0 & 0 & \cdots & a_2 & a_1 & f(x) \\ b_m & b_{m-1} & b_{m-2} & \cdots & 0 & 0 & x^{n-1}\cdot g(x) \\ 0 & b_m & b_{m-1} & \cdots & 0 & 0 & x^{n-2}\cdot g(x) \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & b_1 & b_0 & x\cdot g(x) \\ 0 & 0 & 0 & \cdots & b_2 & b_1 & g(x) \end{vmatrix} \tag{21}$$

再对第$n+m$ 作Laplace 展开, 整理得到$s(x),\ t(x)$ 使得(20) 成立. 证毕

定理11.7.2 设有域K 上的n 次多项式$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 和m 次多项式$g(x)=b_mx^m+\cdots+b_1x+b_0$. 如果$f(x)$, $g(x)$ 在域F 中分别有根$\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n$ 和$\beta_1,\ \beta_2,\ \ldots,\ \beta_m$. 则$f(x)$ 与$g(x)$ 的结式$R(f,g)$ 满足

$$R(f,g)=a_n^m b_m^n\prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j). \tag{22}$$

推论1 设$f(x)$, $g(x)$ 是域K 上的多项式. 则$f(x)$ 和$g(x)$ 有公因式的充要条件是$f(x)$ 与$g(x)$ 的结式$R(f,g)=0$.

推论2 设$f(x)$, $g(x)$ 是域K 上的多项式. 则$f(x)$ 和$g(x)$ 有互质的充要条件是$f(x)$ 与$g(x)$ 的结式$R(f,g)\neq 0$.