信息安全数学基础

第五章 多项式环与有限域

熊 虎

信息与软件工程学院

xionghu.uestc@gmail.com

第五章 多项式环与有限域

5.1 多项式环

定义5.1.1　设F是一个域，我们称

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

（$a_i\in F$, n是非负整数）是F上的一元多项式，其中x是未定元。

如果$a_n\neq 0$，则称a_nx^n为$f(x)$ 的首项，n 是多项式 $f(x)$的次数，记为$\deg(f(x))=n$。如果$a_n=1$，则称$f(x)$为首一多项式。如果$f(x)=a_0\neq 0$，则约定$\deg(f(x))=0$。即为零次多项式。

F上的全体一元多项式的集合用$F[x]$表示。当a_i全为0时，

$f(x)=0$，称为零多项式。对于零多项式，不定义多项式的次数。

5.1 多项式环

多项式环运算

对于$F[x]$中的任意两个多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,\ a_i\in F,$$

$$g(x)=b_nx^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0,\ b_i\in F,$$

定义$F[x]$上的加法和乘法分别如下：

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

$$f(x)g(x)=c_{2n}x^{2n}+\cdots+c_1x+c_0,\ c_i=\sum_{k=0}^{i}a_kb_{i-k}$$

上面系数的加法和乘法是定义在F上的。

显然如此定义的加法和乘法是封闭的，因此是合理的。
加法和乘法显然都满足结合律和交换律，分配律也满足。

5.1 多项式环

例5.1.1　域$GF(2)$上的两个多项式（$GF(2)$ 的两个元素表示为0，1）：

$$f(x)=x^6+x^4+x^2+x+1,\ g(x)=x^7+x+1,$$

则

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

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

5.1 多项式环

定理5.1.1 $F[x]$是具有单位元的整环。

证明：首先，加法和乘法都满足结合律和交换律，同时分配律也满足。

$F[x]$构成加法交换群，零元素即零多项式，任意多项式

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

的加法逆元为

$$-f(x) = -a_n x^n + (-a_{n-1}x^{n-1}) + \cdots + (-a_1 x) + (-a_0),$$

也可以写为$-f(x) = -a_n x^n - a_{n-1}x^{n-1} - \cdots - a_1 x - a_0.$

$F[x]$的单位元为$f(x) = 1$（$a_0 = 1$ ，其他的 a_i 全为0）。由于F无零因子，可证$F[x]$无零因子。故$F[x]$是具有单位元的整环。

定义5.1.2 对于$f(x)$, $g(x)\in F[x]$, $f(x)\neq 0$，如果存在$q(x)\in F[x]$，使 $g(x)=q(x)f(x)$，
则称$f(x)$ **整除** $g(x)$，记为

$$f(x)|g(x),$$

$f(x)$称为 $g(x)$ 的**因式**。如果

$$(f(x))^k|g(x),$$

但 $(f(x))^{k+1}$ 不能整除$g(x)$，则称$f(x)$是$g(x)$ 的***k*重因式**。

5.1 多项式环

多项式整除的性质

多项式整除具有下列性质：其中 $c \neq 0 \in F$ 。

1） $f(x)|0$；

2） $c|f(x)$（因为 $f(x) = c(c^{-1}f(x))$）；

3）如果 $f(x)|g(x)$，则 $cf(x)|g(x)$；

4）如果 $f(x)|g(x)$，$g(x)|h(x)$，则 $f(x)|h(x)$；

5）如果 $f(x)|g(x)$，$f(x)|h(x)$，则对任意 $u(x), v(x) \in F[x]$，有 $f(x)|u(x)g(x)+v(x)h(x)$；

6）如果 $f(x)|g(x)$，$g(x)|f(x)$，则 $f(x) = cg(x)$ 。

5.1 多项式环

例5.1.2　$Z[x]$中有 $(x+1)|(x^2-1)$，$(x-1)|(x^n-1)$ (n是正整数)。

与整数一样，$F[x]$也可以作带余除法。即对于$f(x)$，$g(x)\in F[x]$，$f(x)\neq 0$，则存在 $q(x)$，$r(x)\in F[x]$，使

$$g(x)=q(x)f(x)+r(x),\ r(x)=0 \text{ 或 } \deg(r(x))<\deg(f(x))$$

例5.1.3　$GF(2)$ 上多项式

$$f(x)=x^2+x+1,\ g(x)=x^5+x^3+x^2+x+1$$

则 $g(x)=(x^3+x^2+x+1)f(x)+x$ 。

5.1 多项式环

最大公因子

定义5.1.3 $f(x)$, $g(x) \in F[x]$ 为不全为零多项式。设 $d(x) \neq 0 \in F[x]$，如果 $d(x)|f(x)$, $d(x)|g(x)$，则称 $d(x)$ 是$f(x)$的一个公因式。

如果公因式 $d(x)$是首一多项式，而且 $f(x)$, $g(x)$的任何公因式都整除 $d(x)$，则称$d(x)$是$f(x)$, $g(x)$的最大公因式，记为 $(f(x), g(x))$ 。

如果$(f(x), g(x)) = 1$，则称 $f(x)$, $g(x)$互素。

5.1 多项式环

定理5.1.2 （欧几里德算法）对于多项式 $f(x)$, $g(x)$,其中 $\deg(f(x)) \leq \deg(g(x))$。反复进行欧几里德除法，得到下列方程式：

$$
\begin{aligned}
&g(x) = q_1(x)f(x) + r_1(x),\ \deg(r_1(x)) < \deg(f(x)),\\
&f(x) = q_2(x)r_1(x) + r_2(x),\ \deg(r_2(x)) < \deg(r_1(x)),\\
&r_1(x) = q_3(x)r_2(x) + r_3(x),\ \deg(r_3(x)) < \deg(r_2(x)),\\
&\cdots\\
&r_{m-2}(x) = q_m(x)r_{m-1}(x) + r_m(x),\ \deg(r_m(x)) < \deg(r_{m-1}(x)),\\
&r_{m-1}(x) = q_{m+1}(x)r_m(x)
\end{aligned}
$$

于是 $r_m(x) = (f(x), g(x))$。

5.1 多项式环

证明：

由上述除法过程可见，$r_m(x)$整除 $r_{m-1}(x), r_{m-2}(x), \cdots,$ $r_1(x)$， $f(x)$， $g(x)$ 。$r_m(x)$ 是 $f(x)$， $g(x)$ 的公因式。设 $h(x)$也是 $f(x)$， $g(x)$ 的公因式， 则 $h(x)$ 整除$g(x), f(x), r_1(x), \cdots,$ $r_{m-2}(x)$， $r_{m-1}(x), r_m(x)$ 。故 $r_m(x)$是 $f(x)$， $g(x)$的最大公因式。

5.1 多项式环

例5.1.4　求$GF(2)[x]$上多项式

$$f(x)=x^5+x^3+x+1,\ g(x)=x^3+x^2+x+1$$

的最大公因式。

由欧几里德算法得：

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

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

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

故 $(f(x),g(x))=x+1$。

5.1 多项式环

定理5.1.3 对于多项式 $f(x)$，$g(x)$，其中 $\deg(f(x)) \leq \deg(g(x))$，而且 $h(x)=(f(x),g(x))$。则存在 $a(x)$，$b(x)$使

$$a(x)f(x)+b(x)g(x)=h(x),$$

其中 $\deg(a(x)) \leq \deg(g(x))$，$\deg(b(x)) \leq \deg(g(x))$。

在欧几里德算法中，从上到下依次将 $r_1(x), r_2(x), \cdots$，$r_{m-1}(x), r_m(x)$ 用 $f(x)$，$g(x)$表示便得到该定理。

特别地，当 $f(x)$，$g(x)$互素时，存在 $a(x)$，$b(x)$ 使 $a(x)f(x)+b(x)g(x)=1$。

5.1 多项式环

多项式的分解

定义5.1.4 设 $p(x) \in F[x]$ 为首一多项式，且 $\deg(p(x)) \geq 1$，如果$p(x)$在$F[x]$内的因式仅有零次多项式 $cp(x)$（$c \neq 0 \in F$），则称$p(x)$是$F[x]$内的一个不可约多项式，否则称为可约多项式。

例**5.1.5** $Z[x]$上多项式 x^2+1不可约。$GF(2)[x]$ 上多项式 x^2+1可约：$x^2+1=(x+1)^2$ 。

5.1 多项式环

$GF(2)[x]$五次以内的不可约多项式

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

定理5.1.4 （因式分解唯一定理）$F[x]$上的多项式

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

可分解为

$$f(x) = a_n(p_1(x))^{k_1}(p_2(x))^{k_2}\cdots(p_r(x))^{k_r}, (k_1, k_2, \cdots, k_r > 0)$$

其中 $p_1(x)$, $\cdots$, $p_r(x)$ 是两两不同的首一不可约多项式。除 $p_1(x)$, $\cdots$, $p_r(x)$的排列次序外，上述分解是唯一的。

5.1 多项式环

证明：首先证明存在这样的分解。

如果 $f(x)$不可约，则定理正确。

如果 $f(x)$可约，则存在 $g(x)$，$h(x)$，使

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

其中 $0 < \deg(g(x))$,$\deg(h(x)) < \deg(f(x))$。对$g(x)$，$h(x)$ 继续分解，一直可以把 $f(x)$ 分解成互不相同的不可约多项式的幂的乘积。

再证这样的分解除排列次序外是唯一的。设还存在另一分解：

$$f(x) = a_n(q_1(x))^{l_1}(q_2(x))^{l_2}\cdots(q_s(x))^{l_s}.$$

5.1 多项式环

于是

$$(p_1(x))^{k_1}(p_2(x))^{k_2}\cdots(p_r(x))^{k_r}=(q_1(x))^{l_1}(q_2(x))^{l_2}\cdots(q_s(x))^{l_s}.$$

由上式可知，$p_1(x)|(q_1(x))^{l_1}(q_2(x))^{l_2}\cdots(q_s(x))^{l_s}$.

由于$p_1(x)$是不可约多项式，则 $p_1(x)$ 整除右边某个不可约多项式。不失一般性，设 $p_1(x)|q_1(x)$，由于 $p_1(x)$, $q_1(x)$ 都不可约得

$$p_1(x)=cq_1(x)(c\in F),$$

而 $p_1(x)$, $q_1(x)$都是首一多项式，所以 $p_1(x)=q_1(x)$。等式两边分别约去 $p_1(x)$和 $q_1(x)$，我们有

$$(p_1(x))^{k_1-1}(p_2(x))^{k_2}\cdots(p_r(x))^{k_r}=(q_1(x))^{l_1-1}(q_2(x))^{l_2}\cdots(q_s(x))^{l_s}.$$

上述过程进行下去，可以得到两个分解除不可约因式排列次序外是相同的。

5.1 多项式环

定理5.1.5 一个多项式 $f(x)\in F[x]$含有因式$x-a(a\in F)$，当且仅当 $f(a)=0$。

证明：由欧几里德除法，有

$$f(x)=q(x)(x-a)+r\text{，其中 } r\in F\text{。}$$

于是$(x-a)|f(x)$当且仅当 $r=0$ 当且仅当 $f(a)=0$。

5.1 多项式环

例5.1.6　分解$GF(2)[x]$上多项式：

$$f(x)=x^5+x^4+x^3+x^2+x+1。$$

由于$f(1)=0$，所以$f(x)$有因式$x+1$。运用多项式除法得

$$f(x)=(x+1)(x^4+x^2+1)\quad。$$

通过试探得

$$(x^4+x^2+1)=(x^2+x+1)^2\ 。$$

故

$$f(x)=(x+1)(x^2+x+1)^2。$$

实际上在$GF(2)[x]$上有

$$(f(x)+g(x))^2=(f(x))^2+(g(x))^2$$

5.1 多项式环

因此x^4+x^2+1也可这样分解：

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

多项式环里与整数环具有相似的性质，因此多项式运算的特点与我们在第1章里讨论的整除可以类比。

第五章 多项式环与有限域

5.2 多项式剩余类环

定义5.2.1 设 $f(x) \in F[x]$是首一多项式．对于$a(x)$, $b(x) \in F[x]$，如果$f(x)$ 除 $a(x), b(x)$ 得相同的余式，即

$$a(x) = q_1(x)f(x) + r(x),$$

$$b(x) = q_2(x)f(x) + r(x),$$

则称$a(x)$和 $b(x)$关于模$f(x)$同余，记为

$$a(x) \equiv b(x) \mod f(x)$$

多项式剩余类环

由定义可见, $a(x) \equiv b(x) \mod f(x)$ 当且仅当

$$a(x) - b(x) = g(x)f(x), g(x) \in F[x],$$

$$\text{或 } f(x)|a(x) - b(x)$$

令$\overline{a(x)}$是$F[x]$中和$a(x)$关于$f(x)$同余的全体多项式集合。与整数情形相似，我们可以把$F[x]$划分成剩余类．这些剩余类的集合记为 $F[x] \mod f(x)$。

多项式剩余类环

例**5.2.1** $GF(2)[X] \mod (x^2+1) = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$

定义多项式剩余类的加法和乘法分别如下：

$$\overline{a(x)} + \overline{b(x)} = \overline{a(x)+b(x)}$$

$$\overline{a(x)}\,\overline{b(x)} = \overline{a(x)b(x)}$$

多项式剩余类环

定理5.2.1 设$f(x) \in F[x]$是一个首一多项式，且$def(f(x)) > 0$，则$F[x] \mod f(x)$构成具有单位元的交换环，称为多项式剩余类环。

多项式剩余类环可能存在零因子，例如

$$GF(2)[X] \mod (x^2+1)$$

中就是零因子，因为

$$\overline{x+1x+1} = \overline{x^2+1} = \overline{0}$$

$GF(2)[X] \mod (x^2+1)$存在零因子，是因为x^2+1是可约多项式。在不可约多项式的情形，我们有下面的定理

多项式剩余类环

定理5.2.2 如果 $f(x)$ 是 F 上的首一不可约多项式，则 $F[x] \mod f(x)$ 构成域。

证明 在定理5.2.1的基础上只需证明 $F[x] \mod f(x)$ 的每个非零元都有乘法逆元，则 $F[x] \mod f(x)$ 是域。

对于任意

$$\overline{g(x)} \neq \overline{0} \in F[x] \mod f(x)$$

由于 $f(x)$ 是首一不可约多项式，则

$$(g(x), f(x)) = 1$$

多项式剩余类环

于是存在$a(x), b(x) \in F[x]$，使

$$a(x)g(x) + b(x)f(x) = 1$$

所以

$$\begin{aligned}
\overline{1} &= \overline{a(x)g(x) + b(x)f(x)} \\
&= \overline{a(x)}\;\overline{g(x)} + \overline{b(x)}\;\overline{f(x)} \\
&= \overline{a(x)}\;\overline{g(x)} + \overline{b(x)}\;\overline{0} \\
&= \overline{a(x)}\;\overline{g(x)} \\
&= \overline{1}
\end{aligned}$$

这表明$a(x)$是$g(x)$的逆元。

定理证毕

多项式剩余类环、域

我们下面讨论多项式环的理想与多项式剩余类环的关系。
很容易验证：对于任意$f(x) \in F[x]$，

$$I = \{g(x)f(x) | g(x) \in F[x]\}$$

是$F[x]$的理想。

由定理4.4.2，我们得到I的全体陪集是$F[x]$关于I的商环。而I的全体陪集正好是剩余类的集合 $F[x] \mod f(x)$ ，所以$F[x] \mod f(x)$构成一个环，是$F[x]$关于

$$I = \{g(x)f(x) | g(x) \in F[x]\}$$

的商环。

多项式剩余类环、域

定理5.2.3 域 F上的多项式 $F[x]$主理想整环。

证明 $F[x]$是有单位元的交换环，设 I是$F[x]$中任意理想。如果 $I=\{0\}$，则 I显然是主理想。否则I中一定有一个最低次数的多项式 $f(x)$。我们下面证明I是由 $f(x)$生成的理想。对于任意 $g(x)\in I$，有 $g(x)=q(x)f(x)+r(x), r(x)=0$

或 $def(r(x))<def(f(x))$ ，

由于I是理想，

$$r(x)=g(x)-q(x)f(x)\in I,$$

因为$f(x)$次数的最低性得 $r(x)=0$ ，所以$g(x)=q(x)f(x)$，

则 $g(x)\in(f(x))$，故 $I=(f(x))$ 。

故 $F[x]$ 是一个主理想整环。

第五章 多项式环与有限域

有限域

定义**5.3.1** 有限个元素构成的域称为有限域或**Galois**（伽罗瓦）域。域中元素的个数称为有限域的阶。

我们曾指出，当p是素数时，模p剩余类集合

$$\{\overline{0}, \overline{1}, \overline{2}..., \overline{p-1}\}$$

构成p阶有限域$GF(p)$并指出这也是最简单的一种有限域。

q阶有限域的所有非零元构成q-1阶乘法交换群。在乘法群中，元素a 的阶n是使$a^n = 1$的最小正整数。a生成一个n阶循环群：$\{1, a^1, a^2, ..., a^{n-1}\}$ 。

有限域

我们将域中非零元素关于乘法群的阶定义为域中非零元素的阶。

由关于群的讨论我们有，n阶有限群的任意元素a均满足 $a^n=1$，所以 $a^{q-1}=1$。

如果把零元也考虑进来，则q阶有限域的所有元素满足 $a^q=a$ 或 $a^q-a=0$。

那么q阶有限域可以看成是方程

$$x^q-x=0$$

的根的集合。

有限域

定义5.3.2 q阶有限域中阶为$q-1$的元素称为本原域元素，简称本原元。

本原元的意义是很明显的。如果q阶有限域中存在本原元a，则所有非零元构成一个由a生成的$q-1$阶循环群。那么q阶有限域就可以表示为

$$\{0, 1, a^1, a^2, ..., a^{q-2}\}。$$

有限域

定理5.3.1　有限域中一定含有本原元。

实际上，当$q > 2$时，阶有限域的本原元多于一个．如果a是一个本原元，对于$1 \le n \le q-1$，只要

$$(n, q-1) = 1,$$

由群中的结论，则a^n的阶也是$q-1$，即a^n也是本原元．我们指出,q阶有限域中共有$\varphi(q-1)$个本原元（φ是欧拉函数）。

有限域

假设a是域中的一个非零元，使

$$na = \overbrace{a + a + \cdots + a}^{n} = 0$$

的最小正整数n是a的加法阶．如果不存在这样的n，则加法阶是无限大。

例5.3.1 $GF(7)$ 非零元素的加法阶：

$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
7	7	7	7	7	7

有限域

定理5.3.2 在一个无零因子环R里所有非零元的加法阶都相同．当加法阶有限时，它是一个素数。

证明 如果R的每一个非零元的阶都是无限大，那么定理正确。

如果R的一个非零元a的阶有限，假设为n。设b是另一个非零元，则

$$(na)b = a(nb) = 0\ ,$$

由于R无零因子，可得$nb = 0$ 可以断定n是使$nb = 0$的最小正整数，否则假定$m < n$ 使得$mb = 0$，于是

$(mb)a = b(ma) = 0 \Rightarrow ma = 0$，

与n是a的阶矛盾．故n也是$\boldsymbol{b}$的阶。

有限域

下面证 n是一个素数。

假设n不是素数，则

$n = n1n2$，其中 $n1, n2 < n$，

显然

$n1a \neq 0, n2a \neq 0$ ，

但是有

$(n1a)(n2a) = ((n1n2)a)a = (na)a = 0$ ，

这与R无零因子矛盾，故 n是素数。

域的性质

定义5.3.3　域中非零元的加法阶称为环的特征，当加法阶为无限大时，称特征为0。

推论　域的特征或者是0，或者是一个素数。有限域的特征是素数。

例**5.3.2** $GF(p)$的特征为 p，因为

$$p\overline{1} = \underbrace{\overline{1}+\overline{1}+\cdots+\overline{1}}^{p} = \overline{0}$$

我们可以发现一个有趣的现象，$GF(p)$的特征等于$|GF(p)|$

域的性质

定义5.3.4 如果一个域F不再含有真子集作为F的子域，则称F为素域。

定理5.3.3 阶为素数的有限域必为素域。

证明 如果阶为素数q的域F有真子域，那么这个真子域一定是F构成的加法群的真子群，这个子群的阶一定是q的因子。而素数q除1和q外无其他因子，因子1对应$\{0\}$这个子群，它不是域；因子q对应F全体。可见F无真子域，F是素域。

有限域

引理　在特征为p的域中，下列子集

$$\{0,1,1+1,\ldots,\overbrace{1+1+\cdots+1}^{p-1}\}$$

构成p阶素子域，而且这一素子域与$GF(p)$同构。

证明　设

$$S=\{0,1,1+1,\ldots,\overbrace{1+1+\cdots+1}^{p-1}\}$$

建立S与$GF(p)$ 的下列映射

$$0\to\overline{0},1\to\overline{1},1+1\to\overline{1+1}\ ,\ \ldots,\ \overbrace{1+1+\cdots+1}^{p-1}=\overline{p-1}$$

很容易看出这是一个同构映射，因此S是一个p阶有限域

域的性质

定理5.3.4 1）素数p阶域的特征为p。

2）任何素数p阶域与$GF(p)$同构。

证明

1）设素数p阶域F的特征为q。则由引理，F含有一个与$GF(p)$同构的q阶素子域S，而又由定理5.3.3，F是素域，所以$F=S, p=q$。

2）由1和引理显然。

由于任何素数p阶域都与$GF(p)$同构，这样我们可以用$GF(p)$代表任意素数p阶域，并且将$GF(p)$中的元素简单记为$\{0,1,2,...,p-1\}$。

有限域

定理5.3.5 有限域的阶必为其特征之幂。

一般有限域记为$GF(p^m)$，其中p是域的特征,m是正整数。由于特征总是素数，则有限域的阶总为素数的幂。

有限域的构作

定理5.3.6 如果$f(x)$是$GF(p)$上的m 次首一不可约多项式，则$GF(p)[x] \bmod f(x)$构成p^m阶有限域$GF(p^m)$。

证明 当$f(x)$是p阶域$GF(p)$上的m次首一不可约多项式时，$GF(p)[x] \bmod f(x)$构成p^m个元素的域，这个域的特征为p，所以$GF(p)[x] \bmod f(x)$构成p^m阶有限域$GF(p^m)$。

有限域

定理5.3.7 任意 $GF(p^m)$有限域都同构.

这个定理的证明超出本书的范围．由于该定理，任意p^m阶有限域都可记为$GF(p^m)$，不必加以区分，这与任意素数域都记为$GF(p)$同理。

有兴趣的读者可以参阅胡冠章老师编著的《应用近世代数》第三版**P171**定理**4.3.1**的证明

有限域

例5.3.3 $GF(2)[x] \bmod (x3+x+1)$构成有限域$GF(23)$.

$GF(23)$ 的8个元素：

$$\{\overline{0},\overline{1},\overline{x},\overline{x+1},\overline{x^2},\overline{x^2+1},\overline{x^+x},\overline{x^2+x+1}\}$$

为了表示简单，可以去掉上面的横线，但其剩余类的含义没有改变：

$$\{0,1,x,x+1,x^2,x^2+1,x^2+x,x^2+x+1\}\cdot$$

- 谢谢