普通高等教育“九五”国家教委重点教材

数论讲义

下 册

第二版

柯召 孙琦 编著

高等教育出版社

普通高等教育“九五”国家教委重点教材

数论讲义

下　册

第　二　版

柯召　孙琦　编著

高等教育出版社

图书在版编目(CIP)数据

数论讲义.下/柯召,孙琦编著.—2版.—北京:
高等教育出版社,2003.5
ISBN 7-04-009190-9

Ⅰ.数… Ⅱ.①柯…②孙… Ⅲ.数论-高等学校
-教材 Ⅳ.0156

中国版本图书馆CIP数据核字(2002)第097156号

责任编辑 文小西 **封面设计** 于文燕 **责任绘图** 黄建英
版式设计 马静如 **责任校对** 胡晓琪 **责任印制** 杨 明

出版发行	高等教育出版社	**购书热线**	010-64054588
社 址	北京市东城区沙滩后街55号	**免费咨询**	800-810-0598
邮政编码	100009	**网 址**	http://www.hep.edu.cn
传 真	010-64014048		http://www.hep.com.cn

经 销	新华书店北京发行所
排 版	高等教育出版社照排中心
印 刷	人民教育出版社印刷厂

开 本	850×1168 1/32	**版 次**	1987年3月第1版 2003年5月第2版
印 张	8.625	**印 次**	2003年5月第1次印刷
字 数	210 000	**定 价**	13.30元

本书如有缺页、倒页、脱页等质量问题,请到所购图书销售部门联系调换。

内 容 提 要

本书是根据作者多年教学经验和科研成果写成的。内容除通常的初等数论教材中所包括的基本内容外，还包括三次、四次互反律，代数数论初步，有限域上某些不定方程的基础知识，第二版中还增加了素性判别和整数分解等内容。作者在介绍熟知的经典结果时，也注意介绍新的证明方法和近代进展，并尽可能介绍它们的应用。本书第二版仍分上、下两册出版，上册前五章可作为初等数论课教学内容，上册第六章及下册可作为选修课教学内容。

本书可供数学专业、计算机专业及信息安全、数字信号处理、组合数学方面的学生和研究生用作教材或参考书，也可供从事上述这些方面的教学、科研人员参考。

目　录

第七章　有限域上的多项式

有限域上的多项式是数论所研究的重要内容之一.本章着重讨论有限域上多项式的不可约问题,多项式的周期和本原多项式,以及有限域上的置换多项式,等等.这些内容在某些应用学科中也很有用.

§1　F_p 上的不可约多项式

设 p 是一个素数,$F_p=\mathbf{Z}/(p)=\{0,1,\cdots,p-1\}$ 表示元素个数为 p 的有限域.熟知,其运算为整数模 p 的运算.对于系数在 F_p 上的多项式,我们可以像整数那样引入同余概念.设 $f(x)$ 是 F_p 上的一个 $n(n>0)$ 次多项式,F_p 上的多项式 $f_1(x),f_2(x)$ 满足 $f(x)\mid f_1(x)-f_2(x)$,则称 $f_1(x),f_2(x)$ 对模 $f(x)$ 同余,记为

$$f_1(x)\equiv f_2(x)\pmod{f(x)}.$$

我们知道,如果存在一个 F_p 上的 $n(n>0)$ 次不可约多项式 $m(x)$,取 $m(x)$ 为模,对 F_p 上的全体多项式进行等价分类,那么它的剩余系

$$a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0,a_i\in F_p,i=0,1,\cdots,n-1 \tag{1}$$

含有 p^n 个不同的多项式.

(1) 叫做模 $m(x)$ 的一组**完全剩余系**,除去 0 叫做模 $m(x)$ 的一组**缩系**.对于一般的 F_p 上的 n 次多项式 $f(x)$,(1)也是模 $f(x)$ 的一组**完全剩余系**,其中与 $f(x)$ 互素的全体多项式叫做模

$f(x)$的一组**缩系**.

我们定义(1)中的加法和乘法与多项式的相同,但所得和、积要用 $m(x)$去除.在这样的定义下,运算是封闭的.在这两个运算下,$m(x)$的剩余系(1)构成一个含 p^n 个元素的有限域,它是 F_p 的一个扩域,记为 F_{p^n}.那么,只要证明,对任意素数 p 和正整数 n,存在 F_p 上的 n 次不可约多项式,也就证明了存在元素个数为 p^n 的有限域.我们还知道任一有限域的元素个数一定是某个素数 p 的方幂,而且在同构意义下,元素个数相等的有限域是惟一的.

下面,我们分几个定理来证明任给整数 $n>0$ 和素数 p,存在 F_p 上的 n 次不可约多项式.

定理 1　如果有一个 F_p 上的 n 次不可约多项式 $m(x)$,那么它一定是 $x^{p^n}-x$ 的因式.

证　设 n 次不可约多项式 $m(x)$的缩系是

$$f_1(x),f_2(x),\cdots,f_{p^n-1}(x).$$

设 $m(x)\nmid f(x)$,与整数缩系的性质类似,此时

$$f_1(x)f(x),f_2(x)f(x),\cdots,f_{p^n-1}(x)f(x)\ (\mathrm{mod}\ m(x))$$

也是一缩系.所以有

$$\prod_{i=1}^{p^n-1}f_i(x)\equiv\prod_{i=1}^{p^n-1}(f(x)f_i(x))\ (\mathrm{mod}\ m(x)),$$

$$f(x)^{p^n-1}\equiv 1\ (\mathrm{mod}\ m(x)). \tag{2}$$

或对 F_p 上任意一个多项式 $f(x)$,都有

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

取 $f(x)=x$,就得到

$$x^{p^n}\equiv x\ (\mathrm{mod}\ m(x)).$$

证完

定理 2　设 $\psi(x)$是一个 l 次不可约多项式,且

$$x^{p^n}\equiv x\ (\mathrm{mod}\ \psi(x)),$$

则 $l\leqslant n$.

证 设 $f(x)=\sum_{i=0}^{t}a_ix^i$，$a_i\in F_p$，由

$$(f(x))^{p^n}=\Big(\sum_{i=0}^{t}a_ix^i\Big)^{p^n}=\sum_{i=0}^{t}a_i^{p^n}(x^{p^n})^i$$

$$=\sum_{i=0}^{t}a_i(x^{p^n})^i=f(x^{p^n}),$$

所以

$$(f(x))^{p^n}=f(x^{p^n})\equiv f(x)\ (\mathrm{mod}\ \psi(x)).$$

对于模 $\psi(x)$，有 p^l 个不同的多项式．由于同余方程

$$X^{p^n}-X\equiv 0\ (\mathrm{mod}\ \psi(x))$$

根的个数不超过 p^n，故 $p^l\leqslant p^n$，$l\leqslant n$． 证完

仿第一章§6的引理证明方法，易证下面的定理．

定理3 设$(n,l)=d$，则$(x^{p^n-1}-1,x^{p^l-1}-1)=x^{p^d-1}-1$．

定理4 在定理2的条件下，则有 $l\mid n$．

证 可设 $l>1$，由 $\psi(x)\mid(x^{p^n}-x,x^{p^l}-x)$，可得

$$\psi(x)\mid(x^{p^n-1}-1,x^{p^l-1}-1),$$

再由定理3得 $\psi(x)\mid x^{p^d-1}-1$，这里 $d=(n,l)$，故 $d\leqslant l$．另一方面，由定理2，$l\leqslant d$，于是 $l=d$，即得 $l\mid n$． 证完

定理5 在 F_p 上，多项式 $x^{p^n}-x$ 无重因式．

证 在特征为 p 的域 F_p 上，多项式 $f(x)$ 如果有重因式，仍有$(f(x),f'(x))$的次数大于零．设 $f(x)=x^{p^n-1}-1$，则 $f'(x)=(p^n-1)x^{p^n-2}=-x^{p^n-2}$，于是$(f(x),f'(x))=1$，故 $x^{p^n-1}-1$ 无重因式，由 $x\nmid x^{p^n-1}-1$，便知 $x^{p^n}-x$ 无重因式． 证完

定理6 设 F_p 上的 n 次不可约多项式的个数是 $\Phi_p(n)$（只相差一个常数因子的多项式不加区别），则

$$\Phi_p(n)=\frac{1}{n}\sum_{l\mid n}\mu(l)p^{\frac{n}{l}},\tag{3}$$

其中 $\mu(l)$ 是麦比乌斯函数.

证　如果 $l \mid n$，由 $x^{p^l}-x \mid x^{p^n}-x$，可知对任一 l 次不可约多项式 $\psi(x)$，有 $\psi(x) \mid x^{p^n}-x$，因 $x^{p^n}-x$ 无重因式，再由定理 4，$x^{p^n}-x$ 正好是全体 l 次（$l \mid n$）不可约多项式的乘积，故有

$$p^n = \sum_{l \mid n} l\Phi_p(l).$$

再由反演公式得

$$\Phi_p(n) = \frac{1}{n}\sum_{l \mid n}\mu(l)p^{\frac{n}{l}},$$

这便证明了(3)式成立.　　证完

定理 7　$\Phi_p(n)>0$，这里 $n \geqslant 1$.

证　设 $n = q_1^{l_1}\cdots q_s^{l_s}$，$l_i \geqslant 0$，$i=1,2,\cdots,s$，$q_1<q_2<\cdots<q_s$，便有

$$n\Phi_p(n) = p^n - \sum_{q_i} p^{\frac{n}{q_i}} + \sum_{1 \leqslant i<j \leqslant s} p^{\frac{n}{q_i q_j}} - \cdots + (-1)^s p^{\frac{n}{q_1\cdots q_s}}. \tag{4}$$

设 $n>1$，由于

$$\frac{n}{q_1\cdots q_s} + 1 \leqslant \frac{n}{q_2\cdots q_s},$$

而(4)中各项，除 $p^{\frac{n}{q_1\cdots q_s}}$ 外，其余各项中 p 的幂指数都不小于 $\frac{n}{q_2\cdots q_s}$，所以对(4)式模 $p^{\frac{n}{q_1\cdots q_s}+1}$，得

$$n\Phi_p(n) \equiv (-1)^s p^{\frac{n}{q_1\cdots q_s}} \pmod{p^{\frac{n}{q_1\cdots q_s}+1}}.$$

这就证明了必须有 $\Phi_p(n)>0$.　　证完

Chowla 曾经猜想，设 $N_n(p)$ 代表 F_p 上不可约多项式 x^n+x+a（$1 \leqslant a \leqslant p-1$）的个数，则对于给定的 $n \geqslant 2$，有 $p_0(n)$ 存在，当 $p \geqslant p_0(n)$ 时，$N_n(p)>0$.

如果我们设 F_p 上所有不同的首项系数为 1 的 l 次不可约多

项式的乘积为 $P_{l,p}(x)$，前面已证明了

$$x^{p^n} - x = \prod_{l \mid n} P_{l,p}(x),$$

故由反演公式得

$$P_{n,p}(x) = \prod_{l \mid n} (x^{p^{\frac{n}{l}}} - x)^{\mu(l)}.$$

例 1 设 $p=2, n=2$，故 $\Phi_2(2)=1$，

$$P_{2,2}(x) = \frac{x^4 - x}{x^2 - x} = x^2 + x + 1.$$

这就是 F_2 上的惟一的二次不可约多项式.

例 2 设 $p=2, n=3$，故 $\Phi_2(3)=2$，

$$P_{3,2}(x) = \frac{x^8 - x}{x^2 - x} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$
$$= (x^3 + x + 1)(x^3 + x^2 + 1),$$

即 $x^3 + x + 1, x^3 + x^2 + 1$ 是 F_2 的两个三次不可约多项式.

因为 F_p 上的 n 次不可约多项式的个数是有限的，对于 F_p 上任意给定的 n 次多项式 $f(x)$，如果可约，那么至少有一个次数不大于 $\frac{n}{2}$ 的不可约因式，因此 $f(x)$ 可经有限步分解为不可约因式的乘积. 下面举一个例子.

例 3 $p=2, n=7$，故 $\Phi_2(7)=18$.

先把具有奇数项且常数项为 1 的全部 7 次多项式列出（因为常数项为零或项数为偶数时，显然可约），共 $\binom{6}{5} + \binom{6}{3} + \binom{6}{1} = 32$ 个. 其中 $x^2 + x + 1$ 的倍式是

$x^7 + x^6 + x^5 + x^4 + x^3 + x + 1$, $x^7 + x^6 + x^4 + x^3 + x^2 + x + 1$,
$x^7 + x^6 + x^5 + x^3 + 1$, $x^7 + x^6 + x^3 + x^2 + 1$,
$x^7 + x^5 + x^4 + x + 1$, $x^7 + x^4 + x^2 + x + 1$,
$x^7 + x^5 + 1$, $x^7 + x^2 + 1$;

$x^3 + x + 1$ 的倍式是

$x^7+x^6+x^5+x+1$，　　$x^7+x^6+x^4+x^3+1$，

$x^7+x^5+x^4+x^2+1$，　　$x^7+x^5+x^3+x^2+1$；

x^3+x^2+1 的倍式是

$x^7+x^6+x^2+x+1$，　　$x^7+x^4+x^3+x+1$；

剩下 18 个正好是全部 F_2 上 7 次不可约多项式，用它们的系数来表示，例如 10000011 表示多项式 x^7+x+1，它们是

10000011，10001001，10001111，10010001，
10011101，10100111，10101011，10111001，
10111111，11000001，11001011，11010011，
11010101，11100101，11101111，11110001，
11110111，11111101.

(2) 式是费马小定理的推广. 下面，我们把欧拉函数和欧拉定理推广到 F_p 上的多项式环 $F_p[x]$ 中去.

定义　$\varphi(p,f(x))$ 为 $f(x)$ 的一组完全剩余系中与 $f(x)$ 互素的多项式的个数.

我们有以下的定理.

定理 8　设 $f(x)$ 是 F_p 上的 n 次多项式，其标准分解为

$$f(x)=p_1^{l_1}(x)\cdots p_k^{l_k}(x),$$

$p_i(x)$ 为不可约多项式，且 $p_i(x)$ 的次数 $\partial^\circ(p_i(x))=n_i$ $(i=1,\cdots,k)$，则有

① $\varphi(p,f(x))=p^n\prod_{i=1}^{k}\left(1-\frac{1}{p^{n_i}}\right)$；

② 如果 $(g(x),f(x))=1$，则 $g(x)^{\varphi(p,f(x))}$[①] $\equiv 1 \pmod{f(x)}$.

证　首先证明 $(g(x),h(x))=1$ 时，$\varphi(p,g(x)h(x))=\varphi(p,g(x))\cdot\varphi(p,h(x))$. 因为任一次数 $<\partial^\circ(g(x)h(x))$ 的多

① 为方便排版，本书用两种方式表示一个多项式的幂，例如，$p^l(x)$ 也可表为 $p(x)^l$.

项式 $q(x)$，若$(q(x),g(x)h(x))=1$，则有惟一对多项式 $u(x)$，$v(x)$满足 $q(x)\equiv u(x)\pmod{g(x)}$，$q(x)\equiv v(x)\pmod{h(x)}$，其中$\partial^\circ(u(x))<\partial^\circ(g(x))$，$(u(x),g(x))=1$，$\partial^\circ(v(x))<\partial^\circ(h(x))$，$(v(x),h(x))=1$. 如果 $q_1(x)\neq q(x)$，$\partial^\circ(q_1(x))<\partial^\circ(g(x)h(x))$，那么 $q_1(x)$所对应的一对$\{u_1(x),v_1(x)\}$与$\{u(x),v(x)\}$不同，否则推出 $q_1(x)\equiv q(x)\pmod{g(x)h(x)}$，则有 $q_1(x)=q(x)$与所设不合. 反之，任给一对$\{u(x),v(x)\}$，则由孙子剩余定理，同余式组

$$X\equiv u(x)\pmod{g(x)},X\equiv v(x)\pmod{h(x)}$$

有惟一解 $q(x)$模 $g(x)h(x)$. 因为$(u(x),g(x))=1$ 和$(v(x),h(x))=1$，故$(q(x),g(x)h(x))=1$，于是 $g(x)h(x)$的缩系与二元集$\{u(x),v(x)\}$(其中 $u(x)$和 $v(x)$分别过 $g(x)$和 $h(x)$的缩系)一一对应，这就证明了 $\varphi(p,g(x)h(x))=\varphi(p,g(x))\varphi(p,h(x))$.

现在计算 $\varphi(p,p_i^{l_i}(x))$. $\partial^\circ(p_i^{l_i}(x))=n_il_i$，次数小于 n_il_i 的多项式共 $p^{l_in_i}$ 个，记次数小于 n_il_i 又是 $p_i(x)$的倍式 $p_i(x)q_i(x)$的多项式的个数为 N，那么 $\varphi(p,p_i^{l_i}(x))=p^{l_in_i}-N$，而 N 等于次数小于 $n_il_i-n_i$ 的多项式 $q_i(x)$的个数 $p^{l_in_i-n_i}$，所以

$$\varphi(p,p_i^{l_i}(x))=p^{l_in_i}-p^{l_in_i-n_i}=p^{l_in_i}\left(1-\frac{1}{p^{n_i}}\right).$$

故

$$\varphi(p,f(x))=\prod_{i=1}^{k}p^{l_in_i}\left(1-\frac{1}{p^{n_i}}\right)=p^n\prod_{i=1}^{k}\left(1-\frac{1}{p^{n_i}}\right).$$

这就证明了①.

如果$(g(x),f(x))=1$，设 $f_1(x),\cdots,f_t(x)$($t=\varphi(p,f(x))$)是 $f(x)$的一组缩系，与整数的情形类似，$g(x)f_1(x),\cdots,g(x)f_t(x)$亦过 $f(x)$的一组缩系，则

$$\prod_{i=1}^{t}g(x)f_i(x)\equiv\prod_{j=1}^{t}f_i(x)\pmod{f(x)},$$

即得

$$g(x)^{\varphi(p,f(x))}\equiv 1 \pmod{f(x)}.$$

这便证明了②.　　证完

我们还可以引入 F_p 上多项式的 m 次剩余的概念.

定义　设 $\varphi(x)$ 是 F_p 上的 n 次不可约多项式，$m>1$，设 $(f(x),\varphi(x))=1$，若有 F_p 上一多项式 $g(x)$ 存在，使

$$g(x)^m\equiv f(x) \pmod{\varphi(x)},$$

则 $f(x)$ 称为 F_p 上模 $\varphi(x)$ 的 m **次剩余**，否则称为 m **次非剩余**.

定理 9　设素数 $p>2$，$\varphi(x)$ 是 F_p 上的 n 次不可约多项式，$(f(x),\varphi(x))=1$，则 $f(x)$ 是 F_p 上模 $\varphi(x)$ 的二次剩余的充分必要条件是

$$f(x)^{\frac{p^n-1}{2}}\equiv 1 \pmod{\varphi(x)}. \tag{5}$$

证　设 $(f(x),\varphi(x))=1$，若有 F_p 上的多项式 $g(x)$ 存在，使

$$g(x)^2\equiv f(x) \pmod{\varphi(x)},$$

而 $(g(x),\varphi(x))=1$，由(2)式得

$$f(x)^{\frac{p^n-1}{2}}\equiv g(x)^{p^n-1}\equiv 1 \pmod{\varphi(x)},$$

故(5)成立.

反之，设(5)式成立. 我们先来证明在 $\varphi(x)$ 的缩系中恰有 $\frac{p^n-1}{2}$ 个二次剩余. 因为 $\partial^\circ(\varphi(x))=n$，不妨设 $\varphi(x)$ 的缩系是(1)中除去 0 的 p^n-1 个多项式. (1)中次数为 $k(k=0,1,\cdots,n-1)$，首项系数为 $1,2,\cdots,\frac{1}{2}(p-1)$ 的多项式有 $\frac{1}{2}(p-1)p^k$ 个，所有这样的多项式共有

$$\sum_{k=0}^{n-1}\frac{1}{2}(p-1)p^k=\frac{1}{2}(p-1)\frac{p^n-1}{p-1}=\frac{p^n-1}{2}$$

个，设为 $f_1(x),f_2(x),\cdots,f_{\frac{p^n-1}{2}}(x)$，现在我们来证明

$$f_1(x)^2,f_2(x)^2,\cdots,f_{\frac{p^n-1}{2}}(x)^2 \tag{6}$$

是 $\varphi(x)$的全部二次剩余.设 $f(x)$为 $\varphi(x)$的任一个二次剩余,则有 F_p 上的$g(x)$满足

$$f(x)\equiv g(x)^2\equiv(-g(x))^2(\mathrm{mod}\ \varphi(x)),$$

因 $g(x)$和 $-g(x)$的首项系数总有一个在 1 与 1/2($p-1$)之间,故 $f(x)$必与(6)中某个 $f_j(x)^2$ 模 $\varphi(x)$同余,且(6)中无两个多项式模 $\varphi(x)$同余,这就说明(6)给出了 $\varphi(x)$的全部二次剩余.因为同余方程

$$X^{\frac{p^n-1}{2}}\equiv 1\ (\mathrm{mod}\ \varphi(x)) \tag{7}$$

在 F_p 上模 $\varphi(x)$解的个数$\leqslant\frac{p^n-1}{2}$,故(6)也给出了(7)的全部解.这就证明了,如果 $f(x)$满足(5),即 $f(x)$是同余式(7)的一个解,则 $f(x)$是模 $\varphi(x)$的二次剩余. 证完

§2 F_p 上多项式的次数和原根

和整数的情形类似,我们可以引入 F_p 上的多项式的次数和原根的定义.以下我们均讨论 F_p 上的多项式.

定义 设 $\varphi(x)$是 F_p 上的一个 n 次不可约多项式,而$(f(x),\varphi(x))=1$,l 为使

$$f(x)^l\equiv 1\ (\mathrm{mod}\ \varphi(x))$$

的最小的正整数,则 l 叫做$f(x)$对**模** $\varphi(x)$**的次数**.如果 $l=p^n-1$,则 $f(x)$叫做**模** $\varphi(x)$**的原根**.

仿照第五章关于整数的次数和原根的几个定理,容易推出以下几个定理.

定理 1 设 $\varphi(x)$是 F_p 上的一个 n 次不可约多项式,$f(x)$对模 $\varphi(x)$的次数是 l,则 $l\mid p^n-1$.

定理 2 设 $f(x)$对模 $\varphi(x)$的次数是 l,则

$$1,f(x),f(x)^2,\cdots,f(x)^{l-1}$$

对模 $\varphi(x)$ 两两不同余.

定理 3　设 $f(x)$ 对模 $\varphi(x)$ 的次数是 l，$m>0$，则 $f^m(x)$ 对模 $\varphi(x)$ 的次数是 $\frac{l}{(m,l)}$.

定理 4　设 $l \mid p^n-1$，$\varphi(x)$ 为 F_p 上 n 次不可约多项式，则次数为 l、模 $\varphi(x)$ 互不同余的多项式的个数是 $\varphi(l)$ 个. 这里 $\varphi(l)$ 为欧拉函数.

推论　恰有 $\varphi(p^n-1)$ 个模 $\varphi(x)$ 互不同余的原根.

于是，设 $f(x)$ 是模 $\varphi(x)$ 的一个原根，则

$$f(x),\cdots,f(x)^{p^n-1}$$

给出模 $\varphi(x)$ 的**一组缩系**.

以上这些性质，也可用有限域的概念给出. 设 $\varphi(x)=x^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0$ 是 F_p 上一个 n 次不可约多项式，设 $\varphi(x)$ 的剩余系为

$$a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0,$$
$$a_i\in F_p,i=0,1,\cdots,n-1. \tag{1}$$

在 §1 的开始部分，我们曾指出，在(1)中引入模 $\varphi(x)$ 的加法和乘法，(1)构成含 p^n 个元素的有限域. 这样(1)中的元素已不是通常 F_p 上的多项式. 为了与 F_p 上的多项式区别，我们用一个新的记号 α 来代替(1)中的 x，于是得到 p^n 个元素的集

$$a_{n-1}\alpha^{n-1}+a_{n-2}\alpha^{n-2}+\cdots+a_1\alpha+a_0,$$
$$a_i\in F_p,i=0,1,\cdots,n-1. \tag{2}$$

设 $f_1(x),f_2(x)\in(1)$，$f_1(\alpha),f_2(\alpha)\in(2)$，则在 F_p 上分别有惟一的 $v(x)$ 和 $u(x)$，使

$$f_1(x)+f_2(x)\equiv v(x)\pmod{\varphi(x)},$$
$$f_1(x)f_2(x)\equiv u(x)\pmod{\varphi(x)}.$$

(2) 中元素的加法和乘法，分别规定为

$$f_1(\alpha)+f_2(\alpha)=v(\alpha)$$