Pure Mathematics 理论数学, **2025**, **15**(4), 430-444
Published Online April 2025 in Hans. https://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2025.154144

Hans汉斯

一元多项式环与中国剩余定理

王传夷，刘雨喆*

贵州大学数学与统计学院，贵州 贵阳

收稿日期：2025年3月12日；录用日期：2025年4月16日；发布日期：2025年4月29日

摘 要

本文对一般环R上的一元多项式环$R[x]$展开了研究. 首先，本文引入了$R[x]$中的一元多项式之间左(或右) 带余除法以及左(或右)辗转相除法，并给出了两个多项式能够进行左(或右)带余除法以及左(或右)辗转相除法的条件. 其次，本文通过左(或右)辗转相除法引入了一元多项式有序对$(f(x), g(x))$伪互素这一概念，并证明了伪互素蕴含了理想的互素. 再者，利用伪互素的概念，本文在非交换一元多项式环$R[x]$证明了一类左$R[x]$-模同态φ^{Π}的存在性. 在本文的最后部分，我们提供了一个关于φ^{Π}的理论应用，并指出φ^{Π}在R为交换幺环的情况下就是$R[x]$上的中国剩余定理.

关键词

环，一元多项式环的表示，模同态基本定理，互素，辗转相除法

Monadic Polynomial Ring and the Chinese Remainder Theorem

Chuanyi Wang, Yuzhe Liu*

School of Mathematics and Statistics, Guizhou University, Guiyang Guizhou

Received: Mar. 12^{th}, 2025; accepted: Apr. 16^{th}, 2025; published: Apr. 29^{th}, 2025

* 通讯作者。

文章引用: 王传夷, 刘雨喆. 一元多项式环与中国剩余定理[J]. 理论数学, 2025, 15(4): 430-444.
DOI: 10.12677/pm.2025.154144

Abstract

This paper conducts a study on the monadic polynomial ring $R[x]$ over a ring R. First of all, we introduce the left (or right) division with remainder and the left (or right) Euclidean algorithm between two univariate polynomials in $R[x]$, and provide a condition under which two polynomials can perform left (or right) division with remainder and left (or right) Euclidean algorithm. Secondly, by utilizing the left (or right) Euclidean algorithm, the paper introduces the concept of pseudo-coprimality for ordered pairs of univariate polynomials $(f(x), g(x))$, and proves that pseudo-coprimality implies the coprimality of ideals. Furthermore, by using pseudo-coprime, the paper demonstrates the existence of a left $R[x]$-module homomorphism φ^{Π} in the non-commutative univariate polynomial ring $R[x]$. In the final part of the paper, we provide a theoretical application φ^{Π} and point out that it corresponds to the Chinese Remainder Theorem on $R[x]$ when R is a commutative ring with unity.

Keywords

Rings, Representations of Monadic Polynomial Rings, Homomorphism Theorem, Coprime, Euclidean Algorithm

1. 引言

所谓环的表示, 指的是将环R中的元素通过环同态h映射到给定Abel群M的自同态环上End M或其相反环$(\text{End } M)^{\text{op}}$, 然后通过End M或$(\text{End } M)^{\text{op}}$中的元素来刻画$R$中的元素. 它的一个等价叙述是用$R$对$M$发起一个左侧作用$R \times M \to M$或右侧作用$M \times R \to M$, 该作用习惯上被称为左$R$-作用或右$R$-作用, 并使之满足一些特殊作用规则. 因此环的表示也被称为左R-模或右R-模, 见 [1]. 基于此, 抽象代数领域发展了一个新的数学分支, 即代数的表示理论, 这其中包括了经典的同调理论 [1–3], 后续发展出来的相对同调理论 [4], Gorenstein同调理论 [5–7], 代数的箭图表示理论 [8], 以及gentle/skew-gentle/string代数的几何表示理论 [9–12]等, 这些理论重点研究了环/代数的表示(见

第2节)及其同调性质, 并产生了丰富的研究成果. 在实际应用方面, 则发展了包括交换代数、Lie代数、Hopf代数以及它们的表示理论, 其在数论与密码学、物理、张量等都占据着主要的地. 其中, 菲尔兹奖得主Atiyah所著的教材 [13]被公认是学习、研究交换代数的经典教材之一. 其内容囊括了交换环上的中国剩余定理, Hilbert基定理, 素谱空间, 环上拓扑等经典研究成果. 其中, 剩余类环与中国剩余定理在实际应用中也广受关注, 其被广泛地在密码学中使用. 例如, 文献 [14,15, 等]中所述的同态加密算法与Paillier解密的加速算法, 它们的数学原理都使用了中国剩余定理, 并指出该定理可以有效提升加密算法的速度.

本文的内容聚焦于给定环R上的一元多项式环$R[x]$以及模同态基本定理, 并在此基础上构造一个形如

$$\varphi^{\Pi}: R[x] \to \prod_{i\in I} R[x]/\langle f_i(x)\rangle \tag{1}$$

的左$R[x]$-模同态. 然后通过模同态基本定理得到一个形如

$$R[x]/\mathrm{Ker}(\varphi^{\Pi}) \cong \mathrm{Im}(\varphi^{\Pi}) \tag{2}$$

的特殊的模同构, 并指出这个特殊模同构是经典中国剩余定理在非交换一元多项式环$R[x]$上的推广.

本文共分为三个章节, 其结构陈述如下.

在第一章, 本文对群、环、环的表示以及模同态基本定理进行了基本的复习与回顾, 这些概念可以在经典教材 [2,3]中翻阅.

在第二章, 本文将第一章的内容平行到一元多项式环$R[x]$(不需要$R[x]$的交换条件), 并引入了左(或右)带余除法和左(或右)辗转相除法, 以此引入了“伪互素有序对”(见定义3.8), 并通过推论3.10指出了它与经典意义下的互素的关联. 由于中国剩余定理在交换幺环上表现为一类特殊满同态通过第一同构定理诱导出的同构, 这成为本文引入伪互素的动机, 即, 如果建立非交换环R上的一元多项式环$R[x]$上的中国剩余定理, 并在后续的工作中将之平行到 [8, Chap I]中介绍的有限维代数上. 通过引入伪互素, 本文在第三章证明了如下定理：

定理1.1 (定理3.12)**.** 令R是含幺环. 如果一元多项式环$R[x]$上存在一族主理想$(\langle f_i(x)\rangle)_{i\in I}$使得对任意$i \neq j \in I$, 有序对$(f_i(x), f_j(x))$是伪互素有序对, 则形如(1)中所示的左$R[x]$-模同态是满同态.

在第三章, 本文就R是交换幺环的情况下讨论了φ^{Π}的核

$$\mathrm{Ker}(\varphi^{\Pi}) := \{h(x) \in R[x] \mid \varphi^{\Pi}(h(x)) = 0\},$$

并以此复现了可交换一元多项式环上的中国剩余定理, 见定理4.5.

2. 环的表示及其同态基本定理

环其表示是代数领域中的最重要、最基本的概念. 一个环R的表示本质上是一种环同态$R \to S$, 该同态将所需研究的环R中的元素以保持运算的方式映射为已获研究的环S中的元素, 因此它是使

用S中的元素来刻画R中的“元素类”的一种表示行为. 文章的这一部分将复习环及其表示对概念, 并给出模同构基本定理的证明. 这些概念可以在许多经典的近世代数教材中找到, 例如 [2, Chaps 1, 2]等.

2.1. 环

一个环 (ring) 是由集合R与映射$+,\cdot : R\times R\to R$构成的三元组$(R,+,\cdot)$, 并使得下面条件满足:

(1) $(R,+)$是Abel群 (“+”被称为环R上的加法 (addition));

(2) $(R,\cdot)$是半群 (“$\cdot$”被称为环R上的乘法 (multiplication));

(3) 对任意$a,b,c\in R$, 有$a(b+c)=ab+ac, (b+c)a=ba+ca$.

两个环R和S之间的映射$h: R\to S$如果对任意$r_1,r_2\in R$, 有: $h(r_1+r_2)=h(r_1)+h(r_2)$以及$h(r_1r_2)=h(r_1)h(r_2)$, 则称h是一个环同态 (homomorphism of rings).

例2.1. (1) 对任意给定的Abel群M, 令$\mathrm{End}(M)$表示全体M上的群自同态构成的集合. 则$\mathrm{End}(M)$是一个环, 其中, 环上的加法和乘法按下面公式给出:

- $\forall\varphi,\phi\in\mathrm{End}\,M$, $\varphi+\phi$是映射$\varphi+\phi: M\to M, m\mapsto\varphi(m)+\phi(m)$;
- $\forall\varphi,\phi\in\mathrm{End}\,M$, $\varphi\phi$是映射$\varphi\phi: M\to M, m\mapsto\varphi(\phi(m))$.

$\mathrm{End}(M)$称为Abel群M的自同态环 (endomorphism).

(2) 给定环R, 它的子集S在沿用R上的加法和乘法, 如果对任意$s_1,s_2\in S$, 有$s_1+s_2\in S$以及$s_1s_2\in S$, 则S也是一个环. 这个环称为R的一个子环 (subring).

2.2. 环的表示

定义2.2. 定义在环R上的一个左R-模 (left R-module) 或左R-表示 (left R-representation) M指的是附带环同态

$$h: R\to\mathrm{End}\,M, r\mapsto h_r$$

的Abel群M. 进一步地, 如果M存在子群N使得对任意$r\in R$和$x\in N$有$(h(r))(x)\in N$, 则h自然诱导了另一个环同态

$$R\to\mathrm{End}\,N, r\mapsto(h_r: N\to N),$$

附带该环同态的子群N称为M的一个左R-子模 (left R-submodule), 记作$N\le M$.

注记2.3. 上述定义可以等价地写为左R-模M是附带了满足下述条件的映射$\mu: R\times M\to M$的Abel群.

(M1) $\forall m\in M$: $1m=m$;

(M2) $\forall r\in R$, $m_1,m_2\in M$: $r(m_1+m_2)=rm_1+rm_2$;

(M3) $\forall r_1,r_2\in R$, $m\in M$: $(r_1+r_2)m=r_1m+r_2m$;

(M4) $\forall r_1,r_2\in R$, $m\in M$: $(r_1r_2)m=r_1(r_2m)$.

映射μ被称为环R对Abel群M的左R-作用 (left R-action), 它等价于环同态

$$h : R \to \operatorname{End} M, r \mapsto (r : m \mapsto \mu(r, m) := rm).$$

从(M1)–(M4)的观点看, 左R-模M是线性空间的推广, 且M的左R-子模N看作是M的子集, 使之在沿用M上的左R-作用的情况下, 依然是左R-模. 类似地, 可以定义右R-模.

在本文的第一章中, 所考虑的均为左R-模, 并且本文的第一章的结论对右R-模均有对偶的版本. 因此, 为了方便起见, 本文的第一章中提到的左R-模在不引起混淆的情况下均简称R-模或模.

例2.4. (1) 环R的一个左理想 (left ideal) I 指的是R的子环使得$rI := \{rx \mid x \in I\} \subseteq I$ 对任意$r \in R$成立. 则I是一个左R-模, 其中, R对I的左R-作用由环R上的乘法按$R \times I \to I, (r, x) \mapsto rx$自然给出. 显然, I是R的子模.

(2) 给定环R上的两个模M和N, 使得$N \leq M$. 则集合$M/N := \{m + N \mid m \in M\}$ 按加法$\forall m_1, m_2 \in M$: $(m_1 + N) + (m_2 + N) := (m_1 + m_2) + N$ 成Abel群. 且左R-作用$R \times M/N \to M/N, (r, m + N) \mapsto rm + N$ 指出M/N是一个R-模, 称为左R-商模 (left quotient R-module), 简称商模.

2.3. 模同态基本定理

令R是环, M和N是R-模. 从M到N的左R-模同态 (left R-homomorphism) 指的是满足下述条件的映射$h : M \to N$:

(1) $\forall m_1, m_2 \in M$: $h(m_1 + m_2) = h(m_1) + h(m_2)$;

(2) $\forall r \in R, m \in M$: $h(rm) = rh(m)$.

特别地, 如果h是单射/满射/双射, 则称h是单同态/满同态/同构 (monomorphism / epimorphism / isomorphism). 关于模同态$h : M \to N$, 有下面两条基本性质.

引理2.5 ([2, Chap 2, Section 2.1]).

(1) $\operatorname{Ker}(h) := \{x \in M \mid h(x) = 0\} \leq M$

(2) $\operatorname{Im}(h) := \{y \in N \mid \exists x \in M$ 使得$h(x) = y\} \leq N$.

注记2.6. 引理2.5中的$\operatorname{Ker}(h)$和$\operatorname{Im}(h)$分别被称为模同态h的核 (kernel) 与像 (image).

定理2.7 (第一同态基本定理 [2, Chap 2, Section 2.1]). 模同态$h : M \to N$自然诱导的模同态

$$\bar{h} : M/\operatorname{Ker}(h) \to \operatorname{Im}(h), m + \operatorname{Ker}(h) \mapsto h(m)$$

是一个模同构.

此定理在交换代数上的版本可以参见 [13], 在Artin环或有限维代数上的版本可以参见 [8]

3. 一元多项式环的表示及其同态基本定理

同态基本定理在不同的环上可以导出不同的推论. 例如当环R是域$\mathbf{R}$时, $\mathbf{R}$-模就是线性空间, 此时$\mathbf{R}$-同态$h : M \to N$就是线性映射. 同态基本定理给出$\operatorname{Im}(h) \cong M/\operatorname{Ker}(h)$, 于是, $\operatorname{Im}(h) \oplus \operatorname{Ker}(h) \cong M$. 即得秩-零化度定理(Rank-Nullity Theorem)

3.1. 一元多项式环与左带余除法

定义3.1. 给定环R上一元多项式环 (one variable polynomial ring) 指的是形如

$$R[x] := \left\{ f(x) = \sum_{i=0}^{n} a_i x^i \mid a_1, \cdots a_n \in R, n \in \mathbf{N} \right\}$$

的集合, 其中, 对任意$f(x) = \sum_{i=0}^{n} a_i x^i, g(x) = \sum_{i=0}^{n} b_i x^i \in R[x]$, 其加法和乘法分别定义为$f(x) + g(x) := \sum_{i=0}^{n}(a_i + b_i)x^i$ 以及$f(x)g(x) := \sum_{i=0}^{2n}\left(\sum_{r+s=i} a_r b_s\right)x^i$; 此外, x称为此一元多项式环上的文字 (word).

特别地, 下面命题成立.

命题3.2. *$R[x]$是环. 进一步地, 如果R是含幺环, 则$R[x]$也是.*

对每个$R[x]$中的多项式$f(x) = \sum_{i=0}^{n} a_i x^n$, $a_n \neq 0$, 定义$\deg : R[x] \to \mathbf{N}, f(x) \mapsto n$, 并称$\deg(f(x))$是多项式$f(x)$的次数 (degree). 利用多项式的次数, 可以引入左带余除法.

定义3.3 (左带余除法)**.** 对多项式$f(x), g(x) \in R[x]$, 其中, $\deg(f(x)) \geqslant \deg(g(x))$, 如果存在$q(x)$, $r(x) \in R[x]$满足:

(1) $f(x) = g(x)q(x) + r(x)$;

(2) $\deg(r(x)) < \deg(g(x))$,

则称$f(x)$可以对$g(x)$作左带余除法. 对偶地, 可以定义右带余除法.

注意在$R[x]$上并不是任意两个多项式$f(x)$和$g(x)$都可以进行左带余除法的. 例如取实数域$\mathbf{R}$上的3阶下三角矩阵环$R = \begin{pmatrix} \mathbf{R} & & \\ \mathbf{R} & \mathbf{R} & \\ \mathbf{R} & \mathbf{R} & \mathbf{R} \end{pmatrix}$, 则对$R[x]$中的多项式

$$f(x) = \begin{pmatrix} 0 & & \\ 0 & & \\ 1 & 0 & \end{pmatrix} x \text{ 和} g(x) = \begin{pmatrix} 0 & & \\ 1 & 0 & \\ & & 0 \end{pmatrix} x,$$

易见$g(x)$无法对$f(x)$作左带余除法, 同时$f(x)$也无法对$g(x)$作左带余除法. 当R的性质非常好时, 例如$R \in \{\mathbf{R}, \mathbf{C}, \mathbf{Z}\}$时, $R[x]$上的任意两个多项式总能作左带余除法. 下面命题给出两个多项式可以进行左带余除法的条件.

命题3.4. *设R是含幺环, $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$是$R[x]$中的两个多项式, 且$n, m, t$是满足$n - m = t \geqslant 0$的三个自然数. 如果$f(x)$对$g(x)$关于$c_{n-m}, c_{n-m+1}, \ldots, c_0 \in R$满足左因子条件, 即存在$c_{n-m}, c_{n-m+1}, \ldots, c_0 \in R$使得下面等式组成立:*

$$a_n = c_{n-m} b_m;$$

$$a_{n-1} = c_{n-m-1} b_m + c_{n-m} b_{m-1};$$

$$a_{n-2} = c_{n-m-2} b_m + c_{n-m-1} b_{m-1} + c_{n-m} b_{m-2};$$

$$\cdots\ \cdots\ \cdots;$$
$$a_{n-t}=c_0b_m+c_1b_{m-1}+c_2b_{m-2}+\cdots+c_{n-m}b_{m-t},$$

则$f(x)$可以对$g(x)$作左带余除法.

对偶地, 如果$f(x)$对$g(x)$关于$c_{n-m},c_{n-m+1},\ldots,c_0\in R$满足右因子条件 (即将上面等式组的$b_*$和$c_*$交换即可), 则$f(x)$可以对$g(x)$作右带余除法.

Proof. 本证明只证明可作左代余除法的情形, 可作右带余除法的情况对偶.

由于存在c_{n-m}使得$a_n=c_{n-m}b_m$可知:

$$c_{n-m}g(x)=\sum_{i=0}^{m}c_{n-m}b_ix^i=\left(\sum_{i=0}^{m-1}c_{n-m}b_ix^i\right)+a_nx^m,$$

于是,

$$f(x)-c_{n-m}x^{n-m}g(x)=\sum_{i=0}^{n-m-1}a_ix^i+\sum_{i=n-m}^{n-1}(a_i-c_{n-m}b_{i-(n-m)})x^i.$$

不妨设$a_i-c_{n-m}b_{i-(n-m)}\neq 0$, 则上式等号右侧的多项式的次数为$n-1$.

若$n-1\geqslant m$, 则有$\deg(f(x)-c_{n-m}x^{n-m}g(x))>\deg(g(x))$. 同理, 根据$c_{n-m-1}b_m=a_{n-1}-c_{n-m}b_{m-1}$, 可知:

$$c_{n-m-1}g(x)=\sum_{i=0}^{m}c_{n-m-1}b_ix^i=\left(\sum_{i=0}^{m-1}c_{n-m-1}b_ix^i\right)+(a_{n-1}-c_{n-m}b_m)x^m,$$

于是,

$$\begin{aligned}&f(x)-c_{n-m}x^{n-m}g(x)-c_{n-m-1}x^{n-m-1}g(x)\\=&\sum_{i=0}^{n-m-1}a_ix^i+\sum_{i=n-m}^{n-1}(a_i-c_{n-m}b_i)x^i-\sum_{i=n-m-1}^{n-1}c_{n-m-1}b_{i-(n-m-1)}x^i\\=&\sum_{i=0}^{n-m-2}a_ix^i+(a_{n-m-1}-c_{n-m-1}b_0)x^{n-m-1}\\&+\sum_{i=n-m-1}^{n-2}(a_i-c_{n-m}b_i-c_{n-m-1}b_{i-(n-m-1)})x^i.\end{aligned}$$

注意当$a_i-c_{n-m}b_{i-(n-m)}=0$时, 可取$c_{n-m-1}=0$.

重复上述步骤, 得到一系列多项式

$$\begin{aligned}
-q_1(x)g(x) &= -c_{n-m}x^{n-m}g(x);\\
-q_2(x)g(x) &= -c_{n-m}x^{n-m}g(x) - c_{n-m-1}x^{n-m-1}g(x);\\
&\cdots \qquad \cdots,\\
-q_{t+1}(x)g(x) &= -c_{n-m}x^{n-m}g(x) - c_{n-m-1}x^{n-m-1}g(x) - \cdots - c_0 g(x).
\end{aligned}$$

令$q(x) = q_{t+1}(x)$, 此时, $r(x) = f(x) - q(x)g(x)$是一个次数小于$\deg(g(x))$的多项式, 从而得到左带余除法式

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

上式的存在性表明了此命题的成立. □

带余除法的一个进一步的概念是辗转相除法.

定义3.5 (辗转相除法)**.** 对多项式$f(x), g(x) \in R[x]$, 其中, $\deg(f(x)) \geqslant \deg(g(x))$, 如果存在$q_i(x)$, $r_i(x) \in R[x]$ $(-1 \leqslant i \leqslant k$, 且$r_{-1}(x) = f(x), r_0(x) = g(x), r_1(x), \ldots, r_k(x) \neq 0)$, 使得:

(1) $\deg(g(x)) > \deg(r_1(x)) > \deg(r_2(x)) > \cdots > \deg(r_k(x))$;

(2) 对任意$-1 \leqslant t \leqslant k-2$有左带余除法

$$r_t(x) = r_{t+1}(x)q_{t+2}(x) + r_{t+2}(x), \tag{3}$$

(3) $r_k(x)$是$r_{k-1}(x)$的因式, 即存在$q_{k+1}(x)$使得$r_k(x)q_{k+1}(x) = r_{k-1}(x)$,

则称$f(x)$可以对$g(x)$作左辗转相除法. 对偶地, 可以定义右辗转相除法.

在$\mathbf{Z}[x]$, $\mathbf{Q}[x]$, $\mathbf{R}[x]$, $\mathbf{C}[x]$等形式的一元多项式环中, 总可以进行左辗转相除法和右辗转相除法. 但对一般环R, $R[x]$上的两个多项式$f(x)$对$g(x)$如果满足左(或右)因子条件, 则根据命题3.4, 这两个多项式可以进行左(或右)带余除法, 即有$f(x) = q(x)g(x) + r(x)$或$f(x) = g(x)q(x) + r(x)$). 然而, $g(x)$对$r(x)$未必满足左(或右)因子条件, 此时$f(x)$对$g(x)$无法进行左(或右)辗转相除法.

3.2. 一元多项式环的表示

根据定义2.2, 环R上的一元多项式环$R[x]$的表示是从$R[x]$到Abel群M的自同态环$\operatorname{End} M$的环同态$h : R[x] \to \operatorname{End} M$, 该同态由$x$的像$x \mapsto h_x$完全决定. 换言之, $R[x]$-模M可以被理解为在事先给定Abel群M上的自同态$H = h_x$的情况下的左$R[x]$-作用$R[x] \times M \to M$, $(f(x), m) \mapsto H(m)$. 当$R = \mathbf{R}$时, M同时也是R-线性空间, 且H是阶为$\dim M$的方阵, 其对应于$R[x] = \mathbf{R}[x]$的文字x. 在下文中, 记号$R[x]f(x)$表示集合$R[x]f(x) = \{\varphi(x)f(x) \mid \varphi(x) \in R[x]\}$. $\mathbf{Z}f(x)$, $f(x)R[x]$可以被类似地定义 (注意$\mathbf{Z}$上的交换性自然导致了$\mathbf{Z}f(x) = f(x)\mathbf{Z}$).

引理3.6. *对任意$f(x) \in R[x]$:*

(1) *集合$\mathbf{Z}f(x) + R[x]f(x)$是$R[x]$的左理想, 也是左$R[x]$-模.*

(2) *对偶地, 集合$f(x)\mathbf{Z} + f(x)R[x]$是$R[x]$的右理想, 也是右$R[x]$-模.*

Proof. 本证明只给出(1)的证明, (2)的证明对偶. 简便起见, 令$\mathbf{Z}f(x)+R[x]f(x)=I$. 首先, 易见$I$是Abel群. 再者, 任取$h(x)\in R[x]$, 有$h(x)(zf(x)+g(x)f(x))=h(x)(z+g(x))\cdot f(x)\in R[x]f(x)\subseteq \mathbf{Z}f(x)+R[x]f(x)$, 因此, I是左理想. 根据例2.4 (1), 可知I是左$R[x]$-模. □

当R是含幺环时, 根据命题3.2, $R[x]$也是. 此时, 还有$\mathbf{Z}f(x)+R[x]f(x)=R[x]f(x)=f(x)\mathbf{Z}+f(x)R[x]$. 于是, 引理3.6变为$R[x]f(x)$是$R[x]$-模.

3.3. 一元多项式环上的模同态基本定理

推论3.7. *对任意Abel群M和N以及群同态$\mathcal{A}\in \operatorname{End}M$和$\mathcal{B}\in\operatorname{End}N$, 如果存在Abel群的满同态$h: M\to N$使得*

$$h(\mathcal{A}(m))=\mathcal{B}(h(m)),$$

则对任意环R上的一元多项式环$R[x]$, 由$(x,m)\mapsto\mathcal{A}(m)$ $(m\in M)$ 和$(x,n)\mapsto\mathcal{A}(n)$ $(n\in N)$ 分别诱导的左$R[x]$-作用$R\times M\to M$和$R\times N\to N$必能使$\mathbf{Z}$-模同构

$$M/\operatorname{Ker}(h)\cong N$$

同时也是$R[x]$-模同构.

Proof. 注意每个Abel群都是一个$\mathbf{Z}$-模, 所以由定理2.7, 可知$M/\operatorname{Ker}(h)\cong N$是$\mathbf{Z}$-模同构. 再者, $(x,m)\mapsto\mathcal{A}(m)$诱导的左$R[x]$-作用$R\times M\to M$定义了$M$是$R[x]$-模, 且, 同理$N$也是$R[x]$-模, 因此由已知条件得$h(xm)=h(\mathcal{A}(m))=\mathcal{B}(h(m))=xh(m)$, $\forall m\in M$, 从而对任意一元多项式$f(x)=\sum_{i=0}^{n}r_ix^i\in R[x]$, 有

$$\begin{aligned}h(f(x)m)&=h\left(\sum_{i=0}^{n}r_i\mathcal{A}^i(m)\right)=\sum_{i=0}^{n}r_ih(\mathcal{A}^i(m))\\&=\sum_{i=0}^{n}r_i\mathcal{B}^i(h(m))=\left(\sum_{i=0}^{n}r_ix^i\right)h(m)=f(x)h(m).\end{aligned}$$

这表明h是$R[x]$-模同态, 因此, 由定理2.7, 可知$M/\operatorname{Ker}(h)\cong N$是$R[x]$-模同构. □

定义3.8 (伪互素)**.** 设$f(x),g(x)\in R[x]$可以作左辗转相除法, 并沿用定义3.5中的记号. 此时, 如果$\deg(r_k(x))=0$, 也即$r_k(x)=r\in R$, 则称$(f(x),g(x))$是几乎伪互素有序对 (或在不引起混淆时，称$f(x)$和$g(x)$是几乎伪互素的). 进一步地, 如果R是含幺环, 且r是R的单位 (unit), 即存在r'使得$rr'=r'r=1$, 则称$(f(x),g(x))$伪互素有序对 (或在不引起混淆时，称$f(x)$和$g(x)$伪互素的).

下面引理表明“$f(x)$和$g(x)$ (几乎)伪互素”与“$g(x)$和$f(x)$ (几乎)伪互素”不同.

引理3.9. *令R是环.*

(1) *设$f(x),g(x)\in R[x]$几乎伪互素, 则存在$u(x),v(x)\in R[x]$以及$r\in R$, 使得*

$$f(x)u(x)+(f(x)\delta_{k\bmod 2,1}+g(x)\delta_{k\bmod 2,\,0})+g(x)v(x)=r,$$

其中, 对任意整数r,s, $\delta_{r,s}$是*Kronecker*符号.

(2) 进一步地, 如果R是含幺环且$f(x),g(x)\in R[x]$伪互素, 则:

- 存在$u(x),v(x)\in R[x]$以及单位$r\in R$, 使得$rf(x)u(x)+g(x)v(x)=1$;
- 存在$u(x),v(x)\in R[x]$以及单位$r\in R$, 使得$f(x)u(x)+g(x)v(x)r=1$.

Proof. 本证明沿用定义3.5中的记号, 并假设k足够大. 并将公式组(3)改写为:

$$\begin{aligned}
r_k(x)&=r_{k-2}(x)-r_{k-1}(x)q_k(x)\in r_{k-2}(x)+r_{k-1}(x)R[x];\\
r_{k-1}(x)&=r_{k-3}(x)-r_{k-2}(x)q_{k-1}(x)\in r_{k-3}(x)+r_{k-2}(x)R[x];\\
r_{k-2}(x)&=r_{k-4}(x)-r_{k-3}(x)q_{k-1}(x)\in r_{k-4}(x)+r_{k-3}(x)R[x];\\
&\cdots\\
r_1(x)&=r_{-1}(x)-r_0(x)q_1(x)\in r_{-1}(x)+r_0(x)R[x],
\end{aligned}$$

就有:

$$\begin{aligned}
r_k(x)&\in r_{k-2}(x)+r_{k-1}(x)R[x]\\
&\subseteq r_{k-3}(x)R[x]+r_{k-2}(x)+r_{k-2}(x)R[x]\\
&\subseteq r_{k-4}(x)+r_{k-4}(x)R[x]+r_{k-3}(x)R[x]\\
&\subseteq\cdots\\
&\subseteq\begin{cases}r_{-1}(x)+r_{-1}(x)R[x]+r_0(x)R[x], & \text{如果}k\text{是奇数};\\ r_{-1}(x)R[x]+r_0(x)+r_0(x)R[x], & \text{如果}k\text{是偶数}.\end{cases}
\end{aligned}$$

这就证明了(1).

对于(2), 由R是含幺环可知

$$\begin{aligned}
&f(x)u(x)+f(x)\delta_{k\bmod 2,1}\in\{f(x)(1+u(x)),f(x)u(x)\}\subseteq f(x)R[x],\\
\text{以及}\quad&g(x)\delta_{k\bmod 2,\,0}+g(x)v(x)\in\{g(x)(1+v(x)),g(x)v(x)\}\subseteq g(x)R[x],
\end{aligned}$$

所以已证命题(1)中的表达式可以改写为$f(x)\tilde{u}(x)+g(x)\tilde{v}(x)=r$. 再根据$r$是单位, 可知存在$r'$使得$rr'=1=r'r$, 因此有$r'f(x)\tilde{u}(x)+g(x)\tilde{v}(x)=f(x)\tilde{u}(x)r'+g(x)\tilde{v}(x)'=1$, 这就证明了(2). □

当给定环R的子环R同时是左理想和右理想时, 则称它是双边理想（常常简称为理想）. 环R的元素r生成的双边理想可以表达为$\langle r\rangle:=\mathbf{Z}r+Rr+rR+RrR$. 环$R$的两个双边理想$I$和$J$如果满足$I+J=R$, 则称它们互素. 这里, $I+J$定义为集合$I+J:=\{x+y\mid x\in I,y\in J\}$, 它也是$R$的理想. 当$R$是含幺环时, 对一元多项式环$R[x]$中的两个多项式$f(x)$和$g(x)$, 如果它们是伪互素的, 则有$1\in Rf(x)R[x]+R[x]g(x)\subseteq R[x]$, 这意味着包含$Rf(x)R[x]+R[x]g(x)$的$R[x]$的最小理想就是$R[x]$自身. 于是得到下面推论.

推论3.10. 设R是含幺环. 如果$(f(x), g(x))$伪互素, 则:

(1) 存在$u(x), v(x) \in R[x]$使得$f(x)u(x) + g(x)v(x) = 1$;

(2) $\langle f(x)\rangle$和$\langle g(x)\rangle$互素.

Proof. 论断(1)是引理3.9的(2)的一个直接推论. 由引理3.9的(2), 可知$1 \in Rf(x)R[x] + R[x]g(x) \subseteq \langle f(x)\rangle + \langle g(x)\rangle$, 所以$\langle f(x)\rangle + \langle g(x)\rangle = R[x]$, 这就证明了(2). □

引理3.11. 令R是含幺环, I是指标集, $(f_i(x))_{i\in I}$是$R[x]$中的一族一元多项式, 使得对任意$i \neq j \in I$, $(f_i(x), f_j(x))$总是伪互素的. 对任意$t \in I$, 令$J_t = \bigcap_{r\neq t}\langle f_r(x)\rangle$, 则:

(1) J_t是$R[x]$的一个双边理想;

(2) $\langle f_t(x)\rangle$与J_t互素.

Proof. (1) 对任意环, 注意它的任意两个双边理想的交也是一个双边理想, 因此, 若任意n个双边理想的交是一个双边理想, 那么$n+1$个双边理想的交可以看成两个双边理想的交: 其一是这$n+1$个双边理想的其中n个, 剩下那个双边理想则是第二个. 于是根据归纳法可得(1).

(2) 设I的元素个数是n. 由推论3.10的(2)可知对任意$i \neq j \in I$, $\langle f_i(x)\rangle$和$\langle f_j(x)\rangle$互素. 所以, 对任意$r \neq t$, 有$\langle f_t(x)\rangle + \langle f_r(x)\rangle = R[x]$. 这表明$R[x]$的单位元1有$n-1$种分解$1 = \varphi_r(x) + \phi_r(x)$, $r \in I, r \neq t$, 其中, $\varphi_r(x) \in \langle f_t(x)\rangle$, $\phi_r(x) \in \langle f_r(x)\rangle$. 所以

$$\prod_{r\neq t}\phi_r(x) = \prod_{r\neq t}(1-\varphi_r(x)) = 1 + \widehat{\phi}(x). \tag{4}$$

有如下两点值得注意:

- $\widehat{\phi}(x) = 1 - \prod_{r\neq t}(1-\varphi_r(x)) \in \sum_{r\neq t}\Big(R[x]\varphi_r(x)R[x] + \varphi_r(x)R[x] + R[x]\varphi_r(x)\Big) \subseteq \langle f_t(x)\rangle$;
- $\prod_{r\neq t}\phi_r(x) \in \prod_{r\neq t}\langle f_r(x)\rangle \subseteq J_t$,

因此(4)式给出了:

$$1 = -\widehat{\phi}(x) + \prod_{r\neq t}\phi_r(x) \in \langle f_t(x)\rangle + J_t, \tag{5}$$

得$R[x] = \langle f_t(x)\rangle + J_t$. □

下面结论是本文的主定理.

定理3.12 (非交换一元多项式环上的中国剩余定理)**.** 沿用引理3.11中的记号. 则

$$\varphi^{\Pi} = (\varphi_i)_{I\times 1} : R[x] \to \prod_{i\in I} R[x]/\langle f_i(x)\rangle$$

是左$R[x]$-满同态. 其中, $\varphi_i : R[x] \to R[x]/\langle f_i(x)\rangle$将$R[x]$中的一元多项式$h(x)$映射为陪集$h(x) +$

$\langle f_i(x)\rangle$.

Proof. 不妨设$I=\{1,2,\cdots,n\}$. 由引理3.11可知$\langle f_r(x)\rangle + J_r = R[x]$, 因此$R[x]$的单位元1有分解

$$(a_r(x)f_r(x)b_r(x)+c_r(x)f_r(x)+f_r(x)d_r(x))+g_r(x)=1, \tag{6}$$

其中, $g_r(x)\in J_r$, $a_r(x),b_r(x),c_r(x),d_r(x)\in R[x]$. 对任意$(h_r(x)+\langle f_r(x)\rangle)_{r\in I}\in\prod_{i\in I}R[x]/\langle f_i(x)\rangle$ 的任意分量$h_r(x)+\langle f_r(x)\rangle$的代表元素$h_r(x)$, 用它在式(6)两侧相乘, 得:

$$H_r(x):=h_r(x)\cdot\big(1-(a_r(x)f_r(x)b_r(x)+c_r(x)f_r(x)+f_r(x)d_r(x))\big)=h_r(x)g_r(x),$$

以及

$$\begin{aligned}\varphi_r(H_r(x))&=h_r(x)\cdot\big(1-(a_r(x)f_r(x)b_r(x)+c_r(x)f_r(x)+f_r(x)d_r(x))\big)+\langle f_r(x)\rangle.\\&=h_r(x)+\langle f_r(x)\rangle\end{aligned} \tag{7}$$

同时, 对任意$r\neq s\in I$, 有

$$\varphi_s(H_r(x))=h_r(x)g_r(s)+\langle f_s(x)\rangle\in\bigcap_{i\neq r}\langle f_i(x)\rangle+\langle f_s(x)\rangle\subseteq\langle f_s(x)\rangle. \tag{8}$$

进一步地, 式(7)和(8)给出了

$$\varphi_s(H_r(x))=\begin{cases}h_s(x), & \text{如果}r=s;\\ 0, & \text{其它情形.}\end{cases}$$

从而, 一元多项式$H(x)=\sum_{r\in I}H_r(x)$ 给出了$(h_r(x)+\langle f_r(x)\rangle)_{r\in I}$在映射$\varphi^{\Pi}$下的一个原像, 因此$\varphi^{\Pi}$是满同态. □

4. 主定理在交换幺环上的情形

交换幺环指的是同时是含幺环且乘法满足交换律的环. 在这一章中, 本文所讨论的环R均被假设为交换幺环, 则$R[x]$也是交换幺环.

4.1. Bezout定理

推论4.1 (Bezout定理)**.** 对$R[x]$中的两个多项式$f(x)$和$g(x)$.

(1) 如果$(f(x),g(x))$伪互素, 则存在$u(x),v(x)\in R[x]$使得

$$\begin{aligned}&u(x)f(x)+g(x)v(x)=u(x)f(x)+v(x)g(x)\\=\ &f(x)u(x)+v(x)g(x)=f(x)u(x)+g(x)v(x)=1.\end{aligned}$$

(2) 进一步地, $(f(x),g(x))$伪互素当且仅当$\langle f(x)\rangle$和$\langle g(x)\rangle$互素.

Proof. (1)和(2)的必要性由推论3.10的(1)直接得到. 下面证明(2)的充分性.

设$\langle f(x)\rangle$和$\langle g(x)\rangle$互素, 则$1\in R[x]=\langle f(x)\rangle+\langle g(x)\rangle$, 说明单位元1存在分解$1=\tilde{f}(x)+\tilde{g}(x)$, 其中, $\tilde{f}(x)\in\langle f(x)\rangle$, $\tilde{g}(x)\in\langle g(x)\rangle$. 由于$R[x]$是交换幺环, 因此$\langle f(x)\rangle=\{h(x)f(x)\mid h(x)\in R[x]\}$, 这表明$\tilde{f}(x)$形如$u(x)f(x)=f(x)u(x)$. 同理$\tilde{g}(x)$形如$v(x)g(x)=g(x)v(x)$. 因此$(f(x),g(x))$是伪互素有序对. □

上面推论自然诱导了互素的概念.

定义4.2. 设R是交换幺环, 则一元多项式环$R[x]$上的两个多项式$f(x)$和$g(x)$如能使得有序对$(f(x),g(x))$和$(g(x),f(x))$其中之一是伪互素的, 则称$f(x)$和$g(x)$互素.

4.2. 关于定理3.12中左$R[x]$-模同态的核

引理4.3. 在定理3.12中取R是交换幺环, 则对其有限指标集I的任意非空子集J, 有

$$\prod_{r\in J}\langle f_r(x)\rangle=\bigcap_{r\in J}\langle f_r(x)\rangle$$

Proof. 简便起见, 对任意$r\in J$, 将$\langle f_r(x)\rangle$记作X_r. 则求证式变为$\prod\limits_{r\in J}X_r=\bigcap\limits_{r\in J}X_r$. 首先, 由于所有的$X_r$都是双边理想, 所以，通过双边理想的定义可知“$\subseteq$”自然成立.

另一方面, 任取$t\in J$, 则根据引理3.11及其证明中的式(5), 可知X_t与$\prod\limits_{r\neq t}X_r$互素. 所以$R[x]=X_t+\prod\limits_{r\neq t}X_r$. 上式表明$R[x]$的单位元1有分解$1=f(x)+g(x)$, $f(x)\in X_t, g(x)\in\prod\limits_{r\neq t}X_r$, 同时也表明对任意$\bigcap\limits_{r\neq t}X_r$中的一元多项式$h(x)$, 有

$$\begin{aligned}h(x)&=h(x)1=h(x)(f(x)+g(x))=h(x)f(x)+h(x)g(x)\\&\in\bigcap_{r\neq t}X_r\cdot X_t+\prod_{r\neq t}X_r\subseteq\bigcap_{r\neq t}X_r+\prod_{r\neq t}X_r=\prod_{r\neq t}X_r.\end{aligned}$$

因此也有“$\supseteq$”. □

命题4.4. 在定理3.12中取R是交换幺环, 则φ^{Π}同时是左且右的$R[x]$-模同态, 且它的核$\mathrm{Ker}(\varphi^{\Pi})$满足:

$$\mathrm{Ker}(\varphi^{\Pi})=\prod_{i\in I}\langle f_i(x)\rangle=\bigcap_{i\in I}\langle f_i(x)\rangle.$$

Proof. 根据引理4.3, 只需证

$$\mathrm{Ker}(\varphi^{\Pi})=\bigcap_{i\in I}\langle f_i(x)\rangle.$$

任取$h(x)\in\mathrm{Ker}(\varphi^{\Pi})$, 则对每个$i$, 有$h(x)+\langle f_i(x)\rangle=0+\langle f_i(x)\rangle$, 因此, 有$h(x)\in\langle f_i(x)\rangle$. 从而, $h(x)\in\bigcap\limits_{i\in I}\langle f_i(x)\rangle$. 这就得到了“$\subseteq$”. 反之, 任取$h(x)\in\bigcap\limits_{i\in I}\langle f_i(x)\rangle$, 则对每个$i$, 有$h(x)\in\langle f_i(x)\rangle$. 因此,

$\varphi(h(x)) = (0 + \langle f_i(x)\rangle)_{i\in I}$, 这就得到了“$\supseteq$”. □

4.3. 可交换一元多项式环上的中国剩余定理

定理4.5 (可交换一元多项式环上的中国剩余定理 [13]). *沿用定理3.12中的记号, 则有Abel群同构*

$$R[x]\Big/\prod_{i\in I}\langle f_i(x)\rangle = R[x]\Big/\bigcap_{i\in I}\langle f_i(x)\rangle \cong \prod_{i\in I} R[x]/\langle f_i(x)\rangle,$$

且该同构同时是左$R[x]$-模同构和右$R[x]$-模同构.

Proof. 由定理2.7可知

$$R[x]/\mathrm{Ker}(\varphi^{\Pi}) \cong \prod_{i\in I} R[x]/\langle f_i(x)\rangle.$$

再由引理4.3以及命题4.4可知上式已经与所要证明的同构相同. □

基金项目

本文由国家自然科学基金项目面上项目(12171207)；本文由国家自然科学基金项目青年项目(12401042)；贵州省科技厅重点项目(Grant No.ZD[2025]085)；贵州省科技厅科学计划项目(Grant No.ZK[2024]YiBan066)；以及贵州大学引进人才科研启动基金项目(贵大人基合字[2022]53, [2022]65号)资助.

参考文献

[1] Cartan, H. and Eilenberg, S. (1956) Homological Algebra. Princeton University Press.

[2] Rotman, J.J. (1979) An Introduction to Homological Algebra (2nd Edition). Academic Press.

[3] Weibel, C.A. (1994) An Introduction to Homological Algebra. Cambridge University Press. https://doi.org/10.1017/cbo9781139644136

[4] Enochs, E.E. and Jenda, O.M.G. (2011) Relative Homological Algebra. Walter de Gruyter.

[5] Bass, H. (1963) On the Ubiquity of Gorenstein Rings. *Mathematische Zeitschrift*, **82**, 8-28. https://doi.org/10.1007/bf01112819

[6] Brenner, S. and Butler, M.C.R. (1980) Generalizations of the Bernstein-Gelfand-Ponomarev Reflection Functors. In: Dlab, V. and Gabriel, P., Eds., *Lecture Notes in Mathematics*, Springer Berlin Heidelberg, 103-169. https://doi.org/10.1007/bfb0088461

[7] Mangeney, M., Peskine, C. and Szpiro, L. (1966-1967) Anneaux de Gorenstein, et torsion en algèbre commutative. Séminaire Samuel. Algèbre commutative, Anneaux de Gorenstein, et torsion en algèbre commutative, Tome 1 (1966-1967), Article No. 1. http://www.numdam.org/item/SAC_1966-1967__1__A1_0/

[8] Assem, I., Skowronski, A. and Simson, D. (2006) Elements of the Representation Theory of Associative Algebras. Cambridge University Press. https://doi.org/10.1017/cbo9780511614309

[9] Baur, K. and Coelho Simões, R. (2019) A Geometric Model for the Module Category of a Gentle Algebra. *International Mathematics Research Notices*, **2021**, 11357-11392. https://doi.org/10.1093/imrn/rnz150

[10] Baur, K. and Simões, R. (2024) A Geometric Model for the Module Category of String Algebra. https://arxiv.org/abs/2403.07810

[11] Haiden, F., Katzarkov, L. and Kontsevich, M. (2017) Flat Surfaces and Stability Structures. *Publications mathématiques de l'IHÉS*, **126**, 247-318. https://doi.org/10.1007/s10240-017-0095-y

[12] Opper, S., Plamondon, P.-G. and Schroll, S. (2018) A Geometric Model for the Derived Category of Gentle Algebras. http://arxiv.org/abs/1801.09659

[13] Atiyah, M.F. and Macdonald, I.G. (2018) Introduction to Commutative Algebra. CRC Press. http://rguir.inflibnet.ac.in:8080/jspui/handle/123456789/8941

[14] Dong, X., Zhang, W., Shah, M., Wang, B. and Yu, N. (2019) A Restrained Paillier Cryptosystem and Its Applications for Access Control of Common Secret. https://arxiv.org/abs/1912.09034

[15] Paillier, P. (1999) Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In: Stern, J., Ed., *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 223-238. https://doi.org/10.1007/3-540-48910-x_16