DOI：10.19789/j.1004-9398.2026.02.007　　**Open Access**
文献引用：林开亮，王丽．从中国剩余定理看线性空间关于线性变换的分解[J]．首都师范大学学报（自然科学版），2026，47(2)：46-49. LIN K L，WANG L. Decomposition theorem from the viewpoint of Chinese remainder theorem[J]. Journal of Capital Normal University（Natural Science Edition），2026，47(2)：46-49.

从中国剩余定理看线性空间关于线性变换的分解*

林开亮[1]，王　丽[2**]

（1. 西北农林科技大学理学院，陕西 杨凌　712100；2. 河南理工大学数学与信息科学学院，河南 焦作　454003）

摘要：根子空间分解定理与准素空间分解定理是线性代数中的2个重要定理。基于多项式版本的中国剩余定理，本文给出了这2个定理的统一推广。

关键词：中国剩余定理；线性变换；线性空间分解定理
中图分类号：O156　　**文献标志码**：A

Decomposition theorem from the viewpoint of Chinese remainder theorem*

LIN Kailiang[1]，WANG Li[2**]

（1. Northwest A & F University，College of Science，Yangling Shaanxi　712100；2. Henan Polytechnic University，School of Mathematics and Information Science，Jiaozuo Henan　454003）

Abstract：The root subspace decomposition theorem and the primary space decomposition theorem are two important theorems in linear algebra. Based on the polynomial version of the Chinese remainder theorem，a unified generalization of these two theorems is presented in this paper.

Keywords：Chinese remainder theorem；linear transformation；decomposition theorem
CLC：O156　　**DC**：A

0　引　言

高等代数的一个重要结果是线性空间关于给定线性变换的根子空间分解定理，见北京大学经典教材《高等代数》[1]211中的定理12。

定理1[1]　设V是数域F上的线性空间，A是V上的线性变换。设A的特征多项式为$f(X)$，且在$F[X]$中可以分解为

$$f(X)=(X-\lambda_1)^{r_1}\cdots(X-\lambda_n)^{r_n},$$

式中$\lambda_1,\cdots,\lambda_n\in F$互异。则$V$可以分解为不变子空间的直和$V=V_1\oplus\cdots\oplus V_n$，其中$V_i=\left\{v\in V\mid(A-\lambda_i I)^{r_i}v=0\right\}$是$A$的属于特征值$\lambda_i$的根子空间（或称广义特征子空间）。

利用多项式版本的中国剩余定理可以更好地理解此定理，得出如下结果。

定理2（中国剩余定理的线性代数版本）　设A是域F上向量空间V的线性变换，对任意的$g\in F[X]$，记

收稿日期：2024-11-09
*2024年河南省教改项目（2024SJGLX0286）；河南理工大学课程思政重点项目《高等代数》（2022-1）；2023年河南理工大学青年骨干教师项目（2023XQG-11）
**通信作者：wanglimath@hpu.edu.cn

$\ker(g)=\ker(g(A))=\{v\in V: g(A)v=0\}$。

设 $f=\prod_{i=1}^{n} f_i$，其中 $f_1,\cdots,f_n\in F[X]$ 两两互素，则有向量空间的直和分解

$$\ker(f)=\bigoplus_{i=1}^{n}\ker(f_i)。\tag{1}$$

而且对每个 $i=1,\cdots,n$，存在 $e_i\in F[X]$ 使得

$$e_i(A)=P_i,\tag{2}$$

式中 P_i 是式(1)所确定的从 $\ker(f)$ 到 $\ker(f_i)$ 的投影。

文献[2]中，定理2被称为“中国剩余定理的线性变换版本”，其证明比较简洁。本文给出一个更详尽的阐述，以更好地理解中国剩余定理本质。

1　相关引理

引理1　设 $f_1,\cdots,f_n\in F[X]$，令 $f=\prod_{i=1}^{n} f_i$，且对每个 $i=1,\cdots,n$，令 $g_i=\prod_{\substack{1\leqslant j\leqslant n\\ j\neq i}} f_j$，则

$$\gcd(g_1,\cdots,g_n)\cdot\operatorname{lcm}(f_1,\cdots,f_n)=cf,\tag{3}$$

式中 $c\in F$ 使得 cf 的首项系数为1，gcd，lcm 分别表示最大公因式与最小公倍式。

证明　令 $d=\gcd(g_1,\cdots,g_n)$，根据欧几里德算法[2,3]，存在 $u_1,\cdots,u_n\in F[X]$ 使得

$$d=u_1g_1+\cdots+u_ng_n。$$

令 h 是 $f_1,\cdots,f_n$ 的一个公倍式，于是有 $h=q_1f_1,\cdots,h=q_nf_n$，其中 $q_1,\cdots,q_n\in F[X]$。从而

$$dh=(u_1g_1+\cdots+u_ng_n)h=$$
$$u_1g_1h+\cdots+u_ng_nh=u_1g_1q_1f_1+\cdots+u_ng_nq_nf_n=$$
$$u_1q_1(g_1f_1)+\cdots+u_nq_n(g_nf_n)=$$
$$u_1q_1f+\cdots+u_nq_nf=(u_1q_1+\cdots+u_nq_n)f。$$

进而 $h=(u_1q_1+\cdots+u_nq_n)\frac{f}{d}$。表明 h 是 $\frac{f}{d}$ 的倍式。注意到 $\frac{f}{d}$ 是 $f_1,\cdots,f_n$ 的公倍式，就表明将 $\frac{f}{d}$ 的首项系数归一化之后，即可得到 $f_1,\cdots,f_n$ 的最小公倍式。

注　引理1有一个整数类比，见文献[4]。

设 $f,g,h\in F[X]$，若 $f\mid(g-h)$，记为 $g\equiv h\pmod f$。有如下引理。

引理2　设 $f_1,\cdots,f_n\in F[X]$ 两两互素，令 $f=\prod_{i=1}^{n} f_i$，且对每个 $i=1,\cdots,n$，令 $g_i=\prod_{\substack{1\leqslant j\leqslant n\\ j\neq i}} f_j$，则存在 $u_1,\cdots,u_n\in F[X]$ 使得

$$1=u_1g_1+\cdots+u_ng_n,\tag{4}$$

且对任意的 $i\neq j$ 有

$$u_ig_iu_jg_j\equiv 0\pmod f,\tag{5}$$

对每个 $i=1,\cdots,n$，有

$$(u_ig_i)^2\equiv u_ig_i\pmod f。\tag{6}$$

证明　由于 $f_1,\cdots,f_n\in F[X]$ 两两互素，从而有 $\operatorname{lcm}(f_1,\cdots,f_n)=cf, c\in F$ 使得 cf 的首项系数为1。从而由引理1中的对偶关系(3)，有 $\gcd(g_1,\cdots,g_n)=1$，进而由欧几里的算法可知，存在 $u_1,\cdots,u_n\in F[X]$ 使得式(4)成立。设 $i\neq j$，则

$$u_ig_iu_jg_j=u_iu_jg_ig_j=$$
$$u_iu_j\left(\prod_{\substack{1\leqslant k\leqslant n\\ k\neq i}} f_i\right)\left(\prod_{\substack{1\leqslant l\leqslant n\\ l\neq j}} f_i\right)=u_iu_j\left(\prod_{\substack{1\leqslant k\leqslant n\\ k\neq i,j}} f_i\right)f。$$

从而式(5)成立。为证明式(6)，只需对每个 $i=1,\cdots,n$，有

$$(u_ig_i)^2-u_ig_i=u_ig_i(u_ig_i-1)=$$
$$u_ig_i\left(-\sum_{\substack{1\leqslant j\leqslant n\\ j\neq i}} u_jg_j\right)=-\sum_{\substack{1\leqslant j\leqslant n\\ j\neq i}} u_ig_iu_jg_j。$$

由式(5)即得。

注　用环论的语言，引理2相当于说，若 $f_1,\cdots,f_n\in F[X]$ 两两互素，则式(4)诱导出商环 $F[X]/(f)$ 中“单位元1的一个正交幂等分解”。其整数版本可对照文献[5]。

由引理1不难推出 $f_1,\cdots,f_n$ 两两互素等价于 $g_1,\cdots,g_n$ 的最大公因式为1[6]。

引理3　设 W 是域 F 上向量空间，$P_1,\cdots,P_n$ 是满足 $P_1+\cdots+P_n=I$ 的幂等变换，当 $i\neq j$ 时，$P_iP_j=0$。则

$$W=\bigoplus_{i=1}^{n}\operatorname{Im}(P_i),\tag{7}$$

并且 P_i 是式(7)所确定的从 W 到子空间 $\operatorname{Im}(P_i)$ 的投影。

证明　对任意的 $v\in W$，显然有

$$v=Iv=(P_1+\cdots+P_n)v=P_1v+\cdots+P_nv。$$

从而

$$W=\sum_{i=1}^{n}\operatorname{Im}(P_i)。$$

下面证明上式右端的和为直和。设 $v_i\in\operatorname{Im}(P_i)$ 使得 $v_1+\cdots+v_n=0$。由于 $P_i^2=P_i$，令 $v_i=P_iw_i$，则有 $v_i=P_iw_i=P_i^2w_i=P_i(P_iw_i)=P_iv_i$，从而上式即为

$$P_1v_1 + \cdots + P_nv_n = 0,$$

用P_i作用于上式两边,得到$P_i^2v_i = 0$, 注意$P_i^2v_i = P_iv_i = v_i$, 从而得到$v_i = 0$。这就证明了式(7),并且$v = Iv = (P_1 + \cdots + P_n)v = P_1v + \cdots + P_nv$。立即得到$P_i$是$W$到子空间$\mathrm{Im}(P_i)$的投影。

注 引理3的逆命题也成立[7-8]。

2 定理2的证明与评述

证明 令$f = \prod_{i=1}^{n} f_i$, 且对每个$i = 1, \cdots, n$, 令$g_i = \prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} f_j$, 则由引理2知,存在$u_1, \cdots, u_n \in F[X]$使得

$$1 = u_1(X)g_1(X) + \cdots + u_n(X)g_n(X), \quad (8)$$

且对任意的$i \neq j$有

$$u_i(X)g_i(X)u_j(X)g_j(X) \equiv 0 \ (\mathrm{mod} f(X)), \quad (9)$$

对每个$i = 1, \cdots, n$, 有

$$(u_i(X)g_i(X))^2 \equiv u_i(X)g_i(X) \ (\mathrm{mod} f(X)), \quad (10)$$

令$X = A$,由式(8~10)可得

$$I = u_1(A)g_1(A) + \cdots + u_n(A)g_n(A), \quad (11)$$

且对任意的$i \neq j$有

$$u_i(A)g_i(A)u_j(A)g_j(A) \equiv 0 \ (\mathrm{mod} f(A)), \quad (12)$$

对每个$i = 1, \cdots, n$, 有

$$(u_i(A)g_i(A))^2 \equiv u_i(A)g_i(A) \ (\mathrm{mod} f(A)), \quad (13)$$

由于多项式同余,$g(x) \equiv h(x)(\mathrm{mod} f(x))$指的是$f(x) \mid g(x) - h(x)$,即存在$q(x) \in F(x)$使得$g(x) - h(x) = q(x)f(x)$。所以,$g(A) \equiv h(A)(\mathrm{mod} f(A))$意味着存在$q(x) \in F(x)$使得$g(A) - h(A) = q(A)f(A)$。

令$W = \ker(f)$,

$$P_i = u_i(A)g_i(A), \quad i = 1, \cdots, n,$$

则式(11~13)意味着在W上有

$$I = P_1 + \cdots + P_n,$$

且对任意的$i \neq j$有$P_iP_j = 0$, 对每个$i = 1, \cdots, n$, 有$P_i^2 = P_i$。即$P_1, \cdots, P_n$满足引理3的条件。由于P_i为投影,证明式(1)等价于证明

$$v \in \ker(f_i) \Leftrightarrow v \in \ker(f) \text{且} P_iv = v。$$

充分性:若$v \in \ker(f_i)$, 则$v \in \ker(f)$。为证明$P_iv = v$, 注意$v = Iv = (P_1 + \cdots + P_n)v$。显然当$j \neq i$时,$f_i \mid g_j$, 从而若$v \in \ker(f_i)$, 则$v \in \ker(g_j)$, 于是当$j \neq i$时有$P_jv = u_j(A)g_j(A)v = 0$, 这就得到$v = (P_1 + \cdots + P_n)v = P_iv$。

必要性:设$v \in \ker(f)$且$P_iv = v$, 则

$$f_i(A)v = f_i(A)P_iv = f_i(A)u_i(A)g_i(A)v = u_i(A)f(A)v = 0。$$

定理2可以视为对文献[9]的补充。若取f是A的极小多项式,并令$f = \prod_{i=1}^{n} f_i$是f的准素分解,则得到线性空间V关于线性变换A的准素分解,参见文献[7]。

以上证明将几何分解式(1)建立在代数分解式(4)的基础上。充分揭示了孟道骥教授[10]193所说的:“在研究线性变换的不变子空间的时候,就会不可避免地与多项式理论联系起来。特别地,中国剩余定理是非常重要的。”从抽象代数的观点来看,定理2可视为模论中的中国剩余定理的特例。加州伯克利大学的伍鸿熙教授曾说,他从数学大师陈省身那里学到的最重要的一点,就是从整体而非局部地去把握问题,不考虑复杂的技术细节,即抓住关键点。陈省身先生对待问题的人生哲学,就是每件事情都有一个关键点。如果你抓住了这个关键点,那么剩下的迟早会解决[11]。

对于定理2而言,关键点在哪里呢?简单说,多项式f_i两两互素的条件给出了多项式环中的一个单位分解式(4),给出多项式环模主理想(f)所得商环的一个正交幂等单位分解,得到线性空间$W = \ker(f)$上的单位变换的一个正交幂等分解,进而得到空间W的一个直和分解。

定理2有许多具体的应用。例如,可以由此引出求Fibonacci数列通项的一个算子方法[12],并且这个方法可以推广到求解常系数线性差分方程与微分方程,参见文献[2,13-14]。

3 结束语

本文所讲的定理1与2固然仅适用数学专业的高等代数课程,但其一个特殊情况也适用于普通专业的线性代数课程,即关于可对角化的矩阵/线性变换的基本定理[10]191。

本文所提到的中国剩余定理是古典的中国剩余定理[5]的多项式版本,最简单的情形即Lagrange插值公式。事实上,在高等代数和数值分析中都有重要的应用,用以证明高等代数中的一个基本结果[2,8],线性变换的属于不同特征值的特征向量线性无关。

在教学方面，即便基础课程如高等代数，经典的教材如北京大学版高等代数，基本的定理如根子空间分解定理，依然有改进的余地（读者可将文献[1]中第222页的定理12及其证明与本文对照）。理解数学的本质，分享数学的真与美是数学人永无止境的追求。教学与理解从来就没有最好，只有更好。教学尤其是基础课的教学非常倚重教师，关键就在于教师对课程的理解，本质上是对数学的理解。

©The editorial department of Journal of Capital Normal University（Natural Science Edition）2024. This is an open access article under the CC BY-NC-ND 4.0 license（https://creativecommons.org/licenses/by-nc-nd/4.0/）.

参 考 文 献

[1] 北京大学数学系前代数小组.高等代数[M].6版.北京：高等教育出版社，2025.
Compiled by the former Algebra Group of the Department of Mathematics, Peking University. Advanced algebra[M]. 6th. Beijing: Higher Education Press, 2025.

[2] 林开亮，王兢.中国剩余定理的若干应用[J].中央民族大学学报（自然科学版），2023，32(3)：28-33.
LIN K L, WANG J. Several applications of the Chinese remainder theorem[J]. Journal of Minzu University of China (Natural Science Edition), 2023, 32(3): 28-33.

[3] 王湘浩，谢邦杰.高等代数（修订本）[M].北京：人民教育出版社，1964.
WANG X H, XIE B J. Advanced algebra (revised edition)[M]. Beijing: People's Education Press, 1964.

[4] 华罗庚.数论导引[M].北京：科学出版社，1957.
HUA L G. Introduction to number theory[M]. Beijing: Science Press, 1957.

[5] 张贤科.初等数论[M].北京：高等教育出版社，2016.
ZHANG X K. Elementary number theory[M]. Beijing: Higher Education Press, 2016.

[6] 段炼.两两互素的充要条件及一相关问题[J].数学通报，1996，2：44-46.
DUAN L. Sufficient and necessary conditions for pairwise coprimality and a related problem[J]. Journal of Mathematics (China), 1996, (2): 44-46.

[7] 张贤科.高等线性代数[M].北京：高等教育出版社，2012.
ZHANG X K. Advanced linear algebra[M]. Beijing: Higher Education Press, 2012.

[8] HOFFMAN K, KUNZE R. Linear algebra[M].2nd. New Jersey: Prentice Hall, 1971.

[9] 丘维声.高等代数：下册[M].2版.北京：高等教育出版社，2003.
QIU W S. Advanced algebra[M]. 2nd. Beijing: Higher Education Press, 2003.

[10] 孟道骥.代数之管见：漫谈代数学习[M].北京：科学出版社，2016.
MENG D J. A Glimpse of algebra: ramblings on learning algebra[M]. Beijing: Science Press, 2016.

[11] 丘成桐，刘克峰，季理真.数学与数学人：纪念陈省身先生文集[M].杭州：浙江大学出版社，2005.
QIU C T, LIU K F, JI L Z. Mathematics and mathematicians: a collection in memory of professor Shiing-Shen Chern[M]. Hangzhou: Zhejiang University Press, 2005.

[12] 斯托加茨.心里有数的人生[M].李晓东，译.沈阳：万卷出版公司，2010.
STROGATZ. The calculus of friendship[M]. LI X D, translator. Shenyang: Wan Juan Publishing House, 2010.

[13] 林开亮.解常系数线性微分方程和递推关系的新方法：秦九韶和亥维赛的遗产[J].数学传播，2019，43(2)：63-79.
LIN K L. A new method for solving linear differential equations with constant coefficients and recurrence relations: The heritage of Qin Jiushao and Heaviside[J]. Math Media, 2019, 43(2): 63-79.

[14] 林开亮，王兢.求解常系数线性微分方程的代数方法[J].内蒙古师范大学学报（自然科学汉文版），2019，48(6)：577-582. DOI:10.3969/j.issn.1001-8735.2019.06.016.
LIN K L, WANG J. An algebraic method for solving linear differential equations with constant coefficients[J]. Journal of Inner Mongolia Normal University (Natural Science Edition in Chinese), 2019, 48(6): 577-582.

（责任编辑：马田田）