普通高等教育“十二五”规划教材
大学本科数学类专业基础课程系列丛书

基础代数学选讲

郭聿琦　胡 洵　陈玉柱　编著

科学出版社

普通高等教育“十二五”规划教材

大学本科数学类专业基础课程系列丛书

基础代数学选讲

郭聿琦　胡　洵　陈玉柱　编著

科学出版社

北京

内 容 简 介

本书定位在“抽象代数”的基础之上，对相对基础的“多项式代数”和“线性代数”作出高观点和高能力下的审视，给出必要的、自然的、适当的加宽和加深，以夯实学生的知识基础，提高学生的数学素养. 本书共分8讲，内容包括：数域上的多项式，(并涉及由其定义的)多项式函数，线性相关性（线性代数的核心概念），关于线性空间和线性变换的其他基本事项(联系更一般的模和模同态概念)，线性空间的直和分解(模的特殊情形)，初等变换，初等矩阵与矩阵的等价标准形的应用开发，矩阵分块运算的应用开发，自然数集与数学归纳法，非 Klein 意义上的“高观点下的初等数学”. 全书语言简练，逻辑严密，注重培养学生的逻辑推理和抽象思维能力.

本书可作为高等院校数学类专业师生的教材，也可供其他科研工作者参考.

图书在版编目（CIP）数据

基础代数学选讲/郭聿琦，胡洵，陈玉柱编著. —北京：科学出版社，2016. 2
(大学本科数学类专业基础课程系列丛书)
普通高等教育“十二五”规划教材
ISBN 978-7-03-047122-2

Ⅰ. ①基… Ⅱ. ①郭… ②胡… ③陈… Ⅲ. ①代数-高等学校-教材
Ⅳ. ①O15

中国版本图书馆 CIP 数据核字 (2016) 第 012129 号

责任编辑：胡海霞／责任校对：蒋　萍
责任印制：霍　兵／封面设计：迷底书装

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

大厂书文印刷有限公司 印刷
科学出版社发行　各地新华书店经销
*
2016 年 2 月第　一　版　开本：787 × 1092　1/16
2016 年 2 月第一次印刷　印张：17
字数：390 000

定价：45.00 元

前　言

高校数学类专业为该专业本科生高年级开设的“代数学选讲”课程，平行于“分析学选讲”和“几何学选讲”等非传统课程.

据悉，国内各类高校中的大多数数学类专业已稳定开设此类课程二十余年. 中国科学技术大学龚昇教授生前就曾开设过“微积分学选讲”和“线性代数选讲”等课程；哈尔滨工业大学吴从炘教授也多次为本科生高年级开设“分析学选讲”课程（科学出版社 2011 年出版的《一元微积分深化引论》就是他开设此类课程的结晶之一）. 海外高校数学类本科的“××-学文献选读”类课程早已是本科高年级的传统课程，其内容除自编外，还有引自相关文献的，学生也承担某些内容的报告，这类课程强调课堂讨论. 笔者认为，上述海内外两种课程的共性，就应该是我们本书的写作“宗旨”.

本书为“代数学选讲”课程所编著，其素材大部分来源于作者在兰州大学、云南大学和西南大学开设“代数学选讲”十余次的手稿，其中也有部分内容是在国内近五十所院校为青年教师、研究生和七个数学基地班的学生，以及五次全国性高校教学研讨班做过的系列演讲内容. 该课程位于若干代数学基础课程（诸如“高等代数”“抽象代数”）之后. 它的开设宗旨定位在，对相对基础的内容做出高观点和高能力下的审视，给出必要的、自然的、适当的加宽和加深，以夯实学生的知识基础，提高学生的数学修养（特别是逻辑推理能力和抽象思维能力，这两种能力是代数学尤其善于承担培养的修养侧面），这对学生步入社会工作，或者继续深造，都至关重要.

“基础代数学选讲”主要涉及代数学中最基础的“多项式代数”和“线性代数”（联系到上述宗旨，这里的审视是在“抽象代数学”观点下的）. 目前，所见到的选讲类教材多局限于习题的分类解答，仅有微观处理，并无宏观审视，有浓厚的考研应试教育色彩，不吻合于上述宗旨. 这里除了紧扣我们的宗旨，在内容上也处处展示着我们几十年来在代数学教学上的研究成果，对内容的加宽和加深也本着必要、自然和适当的原则，在内容的整合过程中，“高等代数”教材里的已有事实，在需要时，也予以罗列，但一般地，不再提供证明过程. 凡此种种，读者皆能从本书各讲、节的标题上见其一斑.

本书适合作高校数学类专业“代数学选讲”的教材（当然，使用时可有所取舍）、相关教师的参考书，以及数学专业本科生考研的参考书.

本书的撰写得到兰州大学教务处、兰州大学萃英学院（国家“基础学科拔尖人才培养试验计划”的兰州大学执行单位）和数学与统计学院的大力支持和鼓励，特别地，得到兰州大学教务处“兰州大学教材基金”资助和兰州大学萃英学院出版基金的资助，我们在此表示衷心的感谢. 本书的另两位作者胡洵、陈玉柱（在读博士生）参加了笔者在兰州大学为 2010 级、2011 级和 2012 级萃英班开设的“代数学选讲”课程的教学工作，担任助教，主持讨论课

和习题课, 为本书搜集并整理大量的有关资料. 本书的打印、校对, 除了后两位作者胡洵、陈玉柱, 张迪博士、博士生梁星亮和刘祖华等也有所参与; 另外, 西南大学王正攀教授和访问学者冯爱芳副教授, 通读了本书, 提出不少中肯的修改建议, 作者在此也向他们一并致以诚挚的谢意.

关于选讲类课程的建设和教材的撰写, 当然 "仁者见仁, 智者见智", 不妥之处, 欢迎批评指正.

郭聿琦

2015 年 9 月于兰州大学

目　录

第1讲 数域上的多项式, (并涉及由其定义的) 多项式函数

除了个别情形, 我们这里, 原则上只涉及数域上的一元多项式.

1.1 关于不可约多项式的一个基本事实与若干特殊的不可约多项式

1.1.1 基本事实

引理 1.1.1 令 $\mathbb{F}$ 为一数域, $p(x), f(x) \in \mathbb{F}[x]$, $p(x)$ 首 1 (本质上不需要这一假设) 不可约. 则 $p(x)$ 和 $f(x)$ 在 $\mathbb{C}$ 上有公根 c, 即

$$p(c) = 0 = f(c)$$

当且仅当

$$p(x) \mid f(x).$$

因此, 关于任意 $b \in \mathbb{C}$, $p(b) = 0$ 意味着 $f(b) = 0$.

证明 充分性显然. 下证必要性.

由 $p(x)$ 为首 1 不可约多项式, 有

$$(p(x), f(x)) = \begin{cases} 1, \\ p(x), \quad 即\ p(x) \mid f(x). \end{cases}$$

若 $(p(x), f(x)) = 1$, 则存在 $u(x), v(x) \in \mathbb{F}[x]$, 使得

$$u(x)p(x) + v(x)f(x) = 1.$$

从而

$$0 = u(c)p(c) + v(c)f(c) = 1,$$

矛盾. 所以 $p(x) \mid f(x)$. □

推论 1.1.1 (1) 当引理 1.1.1 中的 $f(x)$ 也在 $\mathbb{F}$ 上不可约时, $p(x)$ 与 $f(x)$ $\mathbb{F}$-相伴.

(2) 任意数域 $\mathbb{F}$ 上两个不可约多项式不相伴当且仅当它们在 $\mathbb{C}$ 上无公根; 从而, $\mathbb{F}$ 上任两个多项式 (在 $\mathbb{F}$ 上) 的互素性不因域的扩大而改变.

推论 1.1.2 任意数域 $\mathbb{F}$ 上的不可约多项式在 $\mathbb{C}$ 上都无重根.

1.1.2　一类特殊的不可约多项式

定理 1.1.1　令 $\mathbb{F}$ 为一数域, $p(x)\in\mathbb{F}[x]$, $p(x)$ 首 1(本质上不需要这一假设) 不可约. 则存在 $c\in\mathbb{C}$, 使得

$$p(c)=0=p(1/c) \tag{1.1}$$

当且仅当关于任意 $b\in\mathbb{C}\setminus\{0\}$, 有

$$p(b)=0 \Longleftrightarrow p(1/b)=0.$$

证明　充分性显然. 下证必要性.

令

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

显然, $a_0\neq 0$.

情形 1　当 $n=1$, 即 $p(x)=x+a_0$ 时, 由假设知, $p(x)=x\pm 1$.

情形 2　当 $n\geqslant 2$ 时, 由

$$0=p(1/c)=(1/c)^n+a_{n-1}(1/c)^{n-1}+\cdots+a_1(1/c)+a_0,$$

有

$$0=c^np(1/c)=1+a_{n-1}c+\cdots+a_1c^{n-1}+a_0c^n.$$

记

$$f(x)\stackrel{d}{=}a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+1.$$

则 $f(c)=p(c)=0$. 根据引理 1.1.1, $p(x)\mid f(x)$. 又 $\partial(p(x))=\partial(f(x))$, 因此,

$$f(x)=d\cdot p(x),\quad d\in\mathbb{F},\quad d\neq 0.$$

若

$$0=p(b)=b^n+a_{n-1}b^{n-1}+\cdots+a_1b+a_0,$$

则 $b\neq 0$ (因为 $a_0\neq 0$), 且

$$0=(1/b)^np(b)=1+a_{n-1}(1/b)+\cdots+a_1(1/b)^{n-1}+a_0(1/b)^n=f(1/b).$$

从而, $p(1/b)=0$. □

当 $\partial(p(x))\geqslant 2$ 时, 由 $\mathbb{Q}\subseteq\mathbb{F}\subseteq\mathbb{C}$, 且 $p(x)$ 不可约知, ± 1 不为 $p(x)$ 的根. 因此, $p(x)$ 的根成对出现, 从而 $p(x)$ 为偶次, 再根据 Vieta 定理, $a_0=1$, 即 $p(x)=f(x)$. 总之有如下结论.

推论 1.1.3　数域 $\mathbb{F}$ 上的不可约多项式, 除了一次的 $p(x)=x+1, x-1$ 及其 $\mathbb{F}$-相伴多项式, 具式 (1.1) 性质的不可约多项式为偶次, 且其 $n+1$ 个系数关于其 $n/2$ 次项系数是中心对称的. 反之亦然.

1.1.3 另一类特殊的不可约多项式

定理 1.1.2 令 $\mathbb{F}$ 为一数域, $p(x) \in \mathbb{F}[x]$, $p(x)$ 首 1(本质上不需要这一假设) 不可约. 则存在 $c \in \mathbb{C}$, 使得

$$p(c) = 0 = p(-c) \tag{1.2}$$

当且仅当关于任意 $b \in \mathbb{C}$, 有

$$p(b) = 0 \Longleftrightarrow p(-b) = 0.$$

证明 充分性显然. 下证必要性.

令

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x_1 + a_0 = g_1(x) + g_2(x),$$

其中, $g_1(x)$ 为 $p(x)$ 的偶次项之和, $g_2(x)$ 为 $p(x)$ 的奇次项之和. 则

$$p(x) + p(-x) = 2g_1(x), \quad p(x) - p(-x) = 2g_2(x).$$

从而, $g_1(c) = g_2(c) = 0$. 根据引理 1.1.1,

$$p(x) \mid g_1(x), \quad p(x) \mid g_2(x), \quad \partial(g_1(x)), \partial(g_2(x)) \leqslant n.$$

(1) 若 $n = 1$, 则 $p(x) = x + a_0$. 由题设

$$c + a_0 = 0 = -c + a_0,$$

从而 $c = a_0 = 0$. 于是 $p(x) = x$, 只有零根.

(2) 若 $n \geqslant 2$, $g_2(x) \neq 0$, 则

$$p(x) = p_2(x), \quad a \in \mathbb{F} \setminus \{0\}$$

有因式 x, 因此 $p(x)$ 可约, 矛盾. 于是, $g_2(x) = 0$, 这指出 $p(x) = g_1(x)$, 即 $p(x)$ 只含偶次项. 从而, 关于任意 $b \in \mathbb{C}$, 有

$$p(b) = 0 \Longleftrightarrow p(-b) = 0. \qquad \square$$

由定理的证明过程可得如下结论.

推论 1.1.4 除了一次的 $p(x) = x$ 及其 $\mathbb{F}$-相伴多项式, 具式 (1.2) 性质的不可约多项式 $p(x)$ 只含偶次项. 反之亦然.

1.1.4 矩阵的最小多项式

定理 1.1.3 令 $\boldsymbol{A}$ 为数域 $\mathbb{F}$ 上一个 n 阶矩阵. 若 $\boldsymbol{A}$ 的特征多项式为

$$\Delta_{\boldsymbol{A}}(x) = \prod_{i=1}^{l} p_i^{r_i}(x),$$

其中, $p_i(x)$ 在 $\mathbb{F}$ 上首 1 不可约, $r_i \geqslant 1$, $p_i(x) \neq p_j(x)$, $i, j = 1, 2, \cdots, l$, $i \neq j$. 则 $\boldsymbol{A}$ 的最小多项式为

$$m_{\boldsymbol{A}}(x) = \prod_{i=1}^{l} p_i^{r_i'}(x),$$

其中, $1 \leqslant r_i' \leqslant r_i$, $i = 1, 2, \cdots, l$.

证明 令 $\mathbb{C}$ 为复数域. 首先证明 $m_{\boldsymbol{A}}(x)$ 与 $\Delta_{\boldsymbol{A}}(x)$ 在域 $\mathbb{C}$ 中有相同的根. 显然, $m_{\boldsymbol{A}}(x)$ 的根均为 $\Delta_{\boldsymbol{A}}(x)$ 的根. 若 x_0 为 $\Delta_{\boldsymbol{A}}(x)$ 在域 $\mathbb{C}$ 中的根, 则由 $\boldsymbol{A}$ 也为域 $\mathbb{C}$ 上的矩阵知, x_0 为 $\boldsymbol{A}$ 在 $\mathbb{C}$ 上的一个特征值, 即存在 $\boldsymbol{\alpha} \in \mathbb{C}^n \setminus \{\boldsymbol{\theta}\}$ ($\boldsymbol{\theta}$ 表示零向量), 使得 $\boldsymbol{A}\boldsymbol{\alpha} = x_0\boldsymbol{\alpha}$. 令

$$m_{\boldsymbol{A}}(x) = x^r + \cdots + c_1 x + c_0.$$

则

$$\begin{aligned}\boldsymbol{\theta} = m_{\boldsymbol{A}}(\boldsymbol{A})\boldsymbol{\alpha} &= (\boldsymbol{A}^r + \cdots + c_1\boldsymbol{A} + c_0\boldsymbol{E})\boldsymbol{\alpha} \\ &= x_0^r\boldsymbol{\alpha} + \cdots + c_1 x_0\boldsymbol{\alpha} + c_0\boldsymbol{\alpha} = m_{\boldsymbol{A}}(x_0)\boldsymbol{\alpha}.\end{aligned}$$

因此, $m_{\boldsymbol{A}}(x_0) = 0$, 即 x_0 为 $m_{\boldsymbol{A}}(x)$ 在 $\mathbb{C}$ 中的一个根.

从而, $\mathbb{F}$ 上 $\Delta_{\boldsymbol{A}}(x)$ 的任意不可约因子 $p_i(x)$ 与 $m_{\boldsymbol{A}}(x)$ 在 $\mathbb{C}$ 上有公根, $i = 1, 2, \cdots, l$. 根据引理 1.1.1, $p_i(x)$ 均为 $m_{\boldsymbol{A}}(x)$ 的因子, $i = 1, 2, \cdots, l$. 再由 $m_{\boldsymbol{A}}(x) \mid \Delta_{\boldsymbol{A}}(x)$ 知,

$$m_{\boldsymbol{A}}(x) = \prod_{i=1}^{l} p_i^{r_i'}(x),$$

其中, $1 \leqslant r_i' \leqslant r_i$, $i = 1, 2, \cdots, l$. □

下面将证明域 $\mathbb{F}$ 上矩阵 $\boldsymbol{A}$ 在 $\mathbb{F}$ 上的最小多项式 $m_{\boldsymbol{A}}(x)$ 不随域的扩大而改变.

定理 1.1.4 令 $\mathbb{F}$ 为一数域, $\boldsymbol{A} \in \mathbb{F}^{n \times n}$, $\mathbb{F}_1$ 为 $\mathbb{F}$ 的扩域, 则

$$m_{\boldsymbol{A}}^{\mathbb{F}}(x) = m_{\boldsymbol{A}}^{\mathbb{F}_1}(x),$$

其中, $m_{\boldsymbol{A}}^{\mathbb{F}_1}(x)$ 表示 $\boldsymbol{A}$ 在 $\mathbb{F}_1$ 上的最小多项式.

为此, 我们要回顾 λ-矩阵 (即域 $\mathbb{F}$ 上的多项式矩阵) 及其标准形的有关概念和事实.

令 $\mathbb{F}$ 为一数域. 则 $\mathbb{F}$ 上的 λ-矩阵指的是 $\mathbb{F}$ 上多项式环 $\mathbb{F}[x]$ 上的多项式矩阵. $\mathbb{F}$ 上关于 x 的 $m \times n$ 多项式矩阵的全体所构成的集合记为 $\mathbb{F}[x]^{m \times n}$.

$\mathbb{F}$ 上矩阵的许多概念和结果都可以推广到 $\mathbb{F}$ 上的多项式矩阵中.

定义 1.1.1 称数域 $\mathbb{F}$ 上 $m \times n$ 多项式矩阵的下述变换为多项式矩阵的初等变换:

(1) k 乘以矩阵的第 l 行 (列), 记为 $[l(k)]$ $(\{l(k)\})$, $k \in \mathbb{F}$, $k \neq 0$, $l = 1, 2, \cdots, m$ ($l = 1, 2, \cdots, n$);

(2) 将矩阵的第 s 行 (列) 的 $\varphi(x)$ 倍加到第 t 行 (列) 上, 记为 $[t + s(\varphi(x))]$ $(\{t + s(\varphi(x))\})$, $\varphi(x) \in \mathbb{F}[x]$, $s, t = 1, 2, \cdots, m$ ($s, t = 1, 2, \cdots, n$), $s \neq t$;

(3) 交换矩阵的第 s, t 行 (列), 记为 $[s, t]$ $(\{s, t\})$, $s, t = 1, 2, \cdots, m$ ($s, t = 1, 2, \cdots, n$).

注 1.1 $\mathbb{F}$ 上多项式矩阵的初等变换与 $\mathbb{F}$ 上矩阵的初等变换仅在第二种变换上有所不同.

定义 1.1.2 令 $\boldsymbol{A}(x),\boldsymbol{B}(x)\in\mathbb{F}[x]^{m\times n}$. 称 $\boldsymbol{A}(x)$ 与 $\boldsymbol{B}(x)$ 等价, 如果 $\boldsymbol{A}(x)$ 可经由有限次行和列的初等变换得到 $\boldsymbol{B}(x)$.

$\mathbb{F}$ 上多项式矩阵的等价关系, 具有自反性、对称性和传递性. 因此, $\boldsymbol{A}(x)$ 与 $\boldsymbol{B}(x)$ 等价, 可以说成 $\boldsymbol{A}(x)$, $\boldsymbol{B}(x)$ 两者等价.

定义 1.1.3 令 $\boldsymbol{A}(x)\in\mathbb{F}[x]^{m\times n}$. 若 $\boldsymbol{A}(x)$ 等价于 $\mathbb{F}[x]^{m\times n}$ 上的如下形式的多项式矩阵

$$\begin{pmatrix} d_1(x) & & & & & & \\ & d_2(x) & & & & & \\ & & \ddots & & & & \\ & & & d_r(x) & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}, \tag{1.3}$$

其中, $r=r_{\boldsymbol{A}(x)}$, $d_k(x)$ 为 $\mathbb{F}$ 上的首 1 多项式, $k=1,2,\cdots,r$, 且 $d_k(x)\mid d_{k+1}(x)$, $k=1,2,\cdots,r-1$, 则称式 (1.3) 为 $\boldsymbol{A}(x)$ 的一个等价标准形.

定义 1.1.4 令 $\boldsymbol{A}(x)\in\mathbb{F}[x]^{m\times n}$, $r_{\boldsymbol{A}(x)}=r$, $r\geqslant 1$. 关于正整数 k, $k=1,2,\cdots,r$, $\boldsymbol{A}(x)$ 中有非零的 k 阶子式 (根据秩的定义), 称 $\boldsymbol{A}(x)$ 中所有 k 阶子式的首 1 的最大公因式 $D_k(x)$ 为 $\boldsymbol{A}(x)$ 的 k 阶行列式因子.

引理 1.1.2 等价的非零多项式矩阵有相同的各阶行列式因子, 从而有相同的秩.

根据引理 1.1.2, 容易验证如下推论.

推论 1.1.5 令 $\boldsymbol{A}(x)\in\mathbb{F}[x]^{m\times n}$, $r_{\boldsymbol{A}(x)}=r$, $r\geqslant 1$. 若 $D_1(x),D_2(x),\cdots,D_r(x)$ 为 $\boldsymbol{A}(x)$ 的各阶行列式因子, 式 (1.3) 是 $\boldsymbol{A}(x)$ 的一个等价标准形, 则

$$\begin{aligned} &d_1(x)=D_1(x),\\ &d_k(x)=\frac{D_k(x)}{D_{k-1}(x)},\quad k=2,3,\cdots,r. \end{aligned}$$

推论 1.1.6 数域 $\mathbb{F}$ 上的多项式矩阵的等价标准形存在且唯一.

定义 1.1.5 令 $\boldsymbol{A}(x)\in\mathbb{F}[x]^{m\times n}$, $r_{\boldsymbol{A}(x)}=r$, $r\geqslant 1$. 称 $\boldsymbol{A}(x)$ 的等价标准形 (1.3) 的 r 个非零元素 $d_1(x),d_2(x),\cdots,d_r(x)$ 为 $\boldsymbol{A}(x)$ 的不变因子.

注 1.2 由引理 1.1.1 知, 多项式的首 1 的最大公因式不因域的扩大而改变. 因此, 多项式矩阵的行列式因子与不变因子也不因域的扩大而改变.

令 $\mathbb{F}$ 为一数域, $\boldsymbol{A}\in\mathbb{F}^{n\times n}$. 我们特别考察 $\mathbb{F}$ 上一特殊的多项式矩阵, 即 $\boldsymbol{A}$ 的特征矩阵 $x\boldsymbol{E}-\boldsymbol{A}$.

定义 1.1.6 令 $\boldsymbol{A}\in\mathbb{F}^{n\times n}$. 则 $x\boldsymbol{E}-\boldsymbol{A}$ 的 (n 个) 不变因子、(n 个) 行列式因子 (因为 $x\boldsymbol{E}-\boldsymbol{A}$ 的秩为 n) 也分别称为 $\boldsymbol{A}$ 的不变因子和行列式因子.

推论 1.1.7　令 $\boldsymbol{A} \in \mathbb{F}^{n\times n}$. 则

$$\Delta_{\boldsymbol{A}}(x) = D_n(x) = d_1(x)d_2(x)\cdots d_n(x),$$

其中, $D_n(x)$ 为 $\boldsymbol{A}$ 的第 n 个行列式因子, $d_1(x), d_2(x), \cdots, d_n(x)$ 为 $\boldsymbol{A}$ 的所有不变因子. 因此,

$$\sum_{i=1}^{n} \partial(d_i(x)) = n.$$

定理 1.1.5　令 $\boldsymbol{A}, \boldsymbol{B} \in \mathbb{F}^{n\times n}$. 则 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 相似当且仅当它们的特征矩阵 $x\boldsymbol{E} - \boldsymbol{A}$ 与 $x\boldsymbol{E} - \boldsymbol{B}$ 等价.

于是, 我们有如下结论.

推论 1.1.8　令 $\boldsymbol{A}, \boldsymbol{B} \in \mathbb{F}^{n\times n}$. 则 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 相似当且仅当它们有完全相同的行列式因子, 也当且仅当它们有完全相同的不变因子.

任一矩阵 $\boldsymbol{A} \in \mathbb{F}^{n\times n}$ 的特征多项式 $|x\boldsymbol{E} - \boldsymbol{A}|$ 为 $\mathbb{F}$ 上一首 1 多项式. 反过来, $\mathbb{F}$ 上任一首 1 多项式

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}[x], \tag{1.4}$$

总是 $\mathbb{F}$ 上如下 n 阶方阵的特征多项式 (容易计算):

$$\boldsymbol{C} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}. \tag{1.5}$$

定义 1.1.7　式 (1.5) 中的 $\boldsymbol{C}$ 称为式 (1.4) 的友阵.

推论 1.1.9　$\mathbb{F}$ 上任意首 1 多项式是其友阵的特征多项式.

定理 1.1.6　$\mathbb{F}$ 上首 1 多项式 $f(x)$ 的友阵 $\boldsymbol{C}$ 的最小多项式也为 $f(x)(= \Delta_{\boldsymbol{C}}(x))$.

证明　见注 3.27.　□

由友阵 $\boldsymbol{C}$ 的行列式因子的计算可知, 下面推论成立.

推论 1.1.10　$\mathbb{F}$ 上首 1 多项式 $f(x)$ 的友阵 $\boldsymbol{C}$ 的全部不变因子为

$$1, \cdots, 1, d_n(x)(= \Delta_{\boldsymbol{C}}(x) = m_{\boldsymbol{C}}(x) = f(x)).$$

令 $\boldsymbol{A} \in \mathbb{F}^{n\times n}$, $\boldsymbol{A}$ 的不变因子为

$$1, \cdots, 1, d_{k+1}(x), d_{k+2}(x), \cdots, d_n(x),$$

其中, $d_i(x)$ 首 1, $\partial(d_i(x)) \geqslant 1$, $i = k+1, \cdots, n$, $d_i(x) \mid d_{i+1}(x)$, $i = k+1, \cdots, n-1$. 又令 $\boldsymbol{C}_i$ 为 $d_i(x)$ 的 $\partial(d_i(x))$ 阶友阵, $i = k+1, \cdots, n$.

由推论 1.1.8, 有如下定理.

定理 1.1.7 令 $\boldsymbol{A}\in\mathbb{F}^{n\times n}$. 则 $\boldsymbol{A}$ 相似于分块对角阵

$$\boldsymbol{F}=\begin{pmatrix}\boldsymbol{C}_{k+1} & & & \\ & \boldsymbol{C}_{k+2} & & \\ & & \ddots & \\ & & & \boldsymbol{C}_n\end{pmatrix}.$$

定义 1.1.8 令 $\boldsymbol{A}\in\mathbb{F}^{n\times n}$. 用 $\boldsymbol{A}$ 的非常数不变因子构造出来的与 $\boldsymbol{A}$ 相似的矩阵 $\boldsymbol{F}$ 称为 $\boldsymbol{A}$ 的 Frobenius 标准形, $d_i(x)$ 的友阵 $\boldsymbol{C}_i$ 称为相应于不变因子 $d_i(x)$ 的 Frobenius 块, $i=k+1,\cdots,n$.

Frobenius 标准形 $\boldsymbol{F}$ 也称为 $\boldsymbol{A}$ 的有理标准形, 这是因为 $\boldsymbol{F}$ 的元素是由 $\boldsymbol{A}$ 的元素经有理合成 (加、减、乘、除) 而得到的.

由于 $\boldsymbol{F}$ 的最小多项式是所有 $\boldsymbol{C}_i$ 的最小多项式的最小公倍式, $\boldsymbol{C}_i$ 的最小多项式为 $d_i(x)$, $i=k+1,k+2,\cdots,n$, 又

$$d_i(x)\mid d_{i+1}(x),\quad i=k+1,\cdots,n-1,$$

从而

$$m_{\boldsymbol{F}}(x)=[d_{k+1}(x),d_{k+2}(x),\cdots,d_n(x)]=d_n(x).$$

由相似矩阵有相同的最小多项式, 易知如下推论.

推论 1.1.11 令 $\boldsymbol{A}\in\mathbb{F}^{n\times n}$. 则

$$m_{\boldsymbol{A}}(x)=d_n(x),$$

其中, $d_n(x)$ 为 $\boldsymbol{A}$ 的第 n 个不变因子.

由注 1.2 和推论 1.1.11, 定理 1.1.4 得证.

下面给出定理 1.1.4 的第二种证明.

证明 由于 $m_{\boldsymbol{A}}^{\mathbb{F}}(x)\in\mathbb{F}[x]\subseteq\mathbb{F}_1[x]$, 当然有

$$m_{\boldsymbol{A}}^{\mathbb{F}_1}(x)\ \mid\ m_{\boldsymbol{A}}^{\mathbb{F}}(x).$$

令

$$\partial(m_{\boldsymbol{A}}^{\mathbb{F}_1}(x))=l,\quad \partial(m_{\boldsymbol{A}}^{\mathbb{F}}(x))=m.$$

则 $l\leqslant m$. 又 $m_{\boldsymbol{A}}^{\mathbb{F}}(x)$, $m_{\boldsymbol{A}}^{\mathbb{F}_1}(x)$ 均为 $\mathbb{F}_1$ 上首 1 多项式, 因此, 要证明 $m_{\boldsymbol{A}}^{\mathbb{F}_1}(x)=m_{\boldsymbol{A}}^{\mathbb{F}}(x)$, 只需证明 $l=m$. 于是, 由 $l\leqslant m$ 知, 只需证明 $l\geqslant m$.

为此, 先做如下准备.

关于任意 $\boldsymbol{A}\in\mathbb{F}^{n\times n}$, 若

$$f(x)=a_rx^r+a_{r-1}x^{r-1}+\cdots+a_1x+a_0\in\mathbb{F}[x],$$

则

$$f(\boldsymbol{A}) \overset{d}{=} a_r\boldsymbol{A}^r + a_{r-1}\boldsymbol{A}^{r-1} + \cdots + a_1\boldsymbol{A} + a_0\boldsymbol{A}^0 \in \mathbb{F}^{n\times n}.$$

令 $\boldsymbol{D} = (d_{ij}) \in \mathbb{F}^{n\times n}$. 又记 $\boldsymbol{A}^k$ 的 (i,j) 元素为 $a_{ij}^{(k)}(\in \mathbb{F})$, $i,j = 1,2,\cdots,n$, $k = 0,1,\cdots,r$, 则

$$\boldsymbol{D} = f(\boldsymbol{A}) \Longleftrightarrow d_{ij} = a_r a_{ij}^{(r)} + a_{r-1}a_{ij}^{(r-1)} + \cdots + a_1 a_{ij}^{(1)} + a_0 a_{ij}^{(0)}, \quad i,j = 1,2,\cdots,n.$$

下面证明 $l \geqslant m$. 令

$$m_{\boldsymbol{A}}^{\mathbb{F}_1}(x) = x^l + c_{l-1}x^{l-1} + \cdots + c_1 x + c_0 \in \mathbb{F}_1[x].$$

则

$$\boldsymbol{O} = m_{\boldsymbol{A}}^{\mathbb{F}_1}(\boldsymbol{A}) = \boldsymbol{A}^l + c_{l-1}\boldsymbol{A}^{l-1} + \cdots + c_1\boldsymbol{A} + c_0\boldsymbol{A}^0.$$

上式等价于

$$a_{ij}^{(l)} + c_{l-1}a_{ij}^{(l-1)} + \cdots + c_1 a_{ij}^{(1)} + c_0 a_{ij}^{(0)} = 0, \quad i,j = 1,2,\cdots,n. \tag{1.6}$$

视 $\mathbb{F}$ 为 $\mathbb{F}$ 上的一个一维线性空间, (1) 为其自然基底, $\mathbb{F}_1$ 为 $\mathbb{F}$ 上一线性空间. 考察 $\mathbb{F}_1$ 的子空间

$$G[\alpha_l, \alpha_{l-1}, \alpha_{l-2}, \cdots, \alpha_1, \alpha_0],$$

其中, $\alpha_l = 1, \alpha_i = c_i, i = 0,1,\cdots,l-1$. 取 $G[\alpha_l, \alpha_{l-1}, \alpha_{l-2}, \cdots, \alpha_1, \alpha_0]$ 的一个基底 $(\beta_1, \beta_2, \cdots, \beta_k)$, $k \in \mathbb{Z}^+$, 其中 $\beta_1 = 1$, 则

$$\begin{aligned}
1 &= 1\beta_1 + 0\beta_2 + \cdots + 0\beta_k,\\
c_{l-1} &= b_{l-1,1}\beta_1 + b_{l-1,2}\beta_2 + \cdots + b_{l-1,k}\beta_k,\\
&\cdots\cdots\\
c_1 &= b_{11}\beta_1 + b_{12}\beta_2 + \cdots + b_{1k}\beta_k,\\
c_0 &= b_{01}\beta_1 + b_{02}\beta_2 + \cdots + b_{0k}\beta_k,
\end{aligned}$$

其中, $b_{ij} \in \mathbb{F}$, $i = 0,1,\cdots,l-1$, $j = 1,2,\cdots,k$.

将上述 $l+1$ 个等式代入式 (1.6), 并整理成关于 $\beta_1, \beta_2, \cdots, \beta_k$ 的表达式, 有

$$\begin{aligned}
&\left(a_{ij}^{(l)} + b_{l-1,1}a_{ij}^{(l-1)} + \cdots + b_{11}a_{ij}^{(1)} + b_{01}a_{ij}^{(0)}\right)\beta_1\\
&+ \left(b_{l-1,2}a_{ij}^{(l-1)} + \cdots + b_{12}a_{ij}^{(1)} + b_{02}a_{ij}^{(0)}\right)\beta_2 + \cdots\\
&+ \left(b_{l-1,k}a_{ij}^{(l-1)} + \cdots + b_{1k}a_{ij}^{(1)} + b_{0k}a_{ij}^{(0)}\right)\beta_k = 0, \quad i,j = 1,2,\cdots,n.
\end{aligned}$$

由 $\beta_1, \beta_2, \cdots, \beta_k$ 线性无关知, β_i 的系数均为零, $i = 1,2,\cdots,k$. 特别地, β_1 的系数为零, 即

$$a_{ij}^{(l)} + b_{l-1,1}a_{ij}^{(l-1)} + \cdots + b_{11}a_{ij}^{(1)} + b_{01}a_{ij}^{(0)} = 0, \quad i,j = 1,2,\cdots,n. \tag{1.7}$$