数学名著译丛

抽象代数学

卷 3

域论及伽罗瓦理论

N. 贾柯勃逊 著

科学出版社

数学名著译丛

抽象代数学

卷 3

域论及伽罗瓦理论

N. 贾柯勃逊 著

李忠侯 俞曙霞 李世余 译

科 学 出 版 社

1987

内 容 简 介

本书是作者根据他在几所大学里讲授的抽象代数学讲义编成的. 全书分三卷. 本卷是卷 3,主要叙述域论及伽罗瓦 (Galois) 理论, 是一本对于发展代数数论与代数几何具有重大价值的著作.

在这一卷中,作者阐述了理解近世代数数论、环论与代数几何学所需的主要基本域论的知识,着重讨论了有限维域扩张及伽罗瓦理论、域的一般结构理论、赋值论和关于阿贝尔 (Abel) 扩张的结果,同时指出了域的现代理论与引导它发展的古典问题之间的联系. 并论述了域论对分析学具有重要意义的部分.

本书可供数学研究工作者、高等院校数学系教师和学生参考.

N. Jacobson
LECTURES IN ABSTRACT ALGEBRA
III. THEORY OF FIELDS AND GALOIS THEORY
Springer-Verlag, 1964

数学名著译丛
抽象代数学
卷 3
域论及伽罗瓦理论
N. 贾柯勃逊 著
李忠侯 俞曙霞 李世余 译
责任编辑 苏芳霞
科学出版社出版
北京朝阳门内大街 137 号
中国科学院印刷厂印刷
新华书店北京发行所发行 各地新华书店经售
*
1987 年 8 月第 一 版 开本: 850×1168 1/32
1987 年 8 月第一次印刷 印张: 10 1/8
印数: 0001—6,000 字数: 265,000
统一书号: 13031·3591
本社书号: 5234·13—1
定价: 2.90 元

序

本卷是著者十多年前开始编写的一套代数学教科书的最后一卷. 这里所给出的域论及伽罗瓦[1] (Galois) 理论是在本书第 1 卷中所出现的一般代数学概念与结果以及涉及线性代数的第 2 卷的较初等部分的基础上阐述的，本卷内容的深度大致与第 2 卷的相同.

在准备本书时我们曾作过多方面的考虑: 首要的是编入基础域论，这是理解现代代数数论、环论及代数几何学所必需的. 本卷涉及这个问题的部分是第一、四、五章，它们分别讨论有限维域扩张及伽罗瓦理论、域的一般结构理论和赋值论；还有第三章关于阿贝尔(Abel) 扩张的结果，虽然看来专门了一些，但却是与数论密切相关的. 我们的第二个目标是要指出域的现代理论与引导它发展的古典问题之间的联系，这一想法在第一章和第六章中得以实现，前者给出方程的根式可解性的伽罗瓦理论，后者给出阿廷 (Artin) 把实闭域理论用于正定有理函数上的希尔伯特 (Hilbert) 问题的解答. 最后，我们还介绍域论对分析学具有重要意义的那些部分，这里特别值得注意的是我们在第六章所论述的实闭域里的多项式方程与不等式的塔尔斯基-赛登堡 (Tarski-Seidenberg) 判定法.

同前两卷书一样，习题也构成本卷的重要部分，其中有少部分是十分困难的.

在这里，我要向我的朋友们致谢: P. 柯恩 (P. Cohn) 与 G. 西利曼 (G. Seligman) 教授细心审阅了初稿，本卷采纳了他们的很多建议；我还感谢柯恩和 J. 莱特 (J. Reid) 教授以及我的妻

1) 在第一卷和第二卷中，“Galois” 一词均译为 “加罗华”，本卷按目前习惯，译为“伽罗瓦”——译者注.

子帮助校对本书．最后，对于美国空军科学发展局给予的长达一个夏季和半个学年的大力支持表示感谢，这一支持使本书能较原计划提前完成。

贾柯勃逊（N. Jacobson）

New Haven, Conn.

1964年1月20日

目　　录

导　言

本书假定读者已熟悉卷1中所出现的代数学的一般概念和域的结果以及卷2的较初等部分.特别地,我们假定读者已具有域的特征、素域、交换整区的分式域的构造法以及域的单代数扩张与单超越扩张的构造法等知识，这些概念在卷1的第二、三章介绍过.我们还需要第四章的因式分解的初等理论.在卷2中，我们需要域上的向量空间、维数、线性变换、线性函数、线性变换的合成、双线性型等基本概念.但线性变换及双线性型的标准形等较高深结果却不是必要的.

在这个导言中我们将复习前面已经讲过的一些内容，这有双重意义：首先，强调以前的一些结果对今后的使用是有利的；其次,为了方便查阅,所以将今后经常用到的一些结果列举出来.这里要讨论的主题有：同态的扩张(参看卷1,第三章)、代数(卷2,第七章)以及向量空间和代数的张量积[1](卷2，第七章).同态的扩张这一概念在域论中是一个重要的工具；代数的概念是在研究一个域以一个选定的子域为其基域时自然产生的；本来张量积的概念在域论中不怎么重要,我们完全可以避开它,然而，这个概念近年来在整个代数学及代数拓朴学中却显得非常重要，所以对于学生来说，熟练掌握张量积是十分必要的.在适当场合我们将要自由地运用它.

1. 同态的扩张　我们约定：本书中所考虑的环都有单位元$1\neq 0$,从而子环一词将仍如卷1那样表示包含1的子环,而环$\mathfrak{A}$到环$\mathfrak{B}$内的同态我们将理解为在旧意义下的将$\mathfrak{A}$的1映到$\mathfrak{B}$的

1) 在卷2中此概念原称为克罗内克（Kronecker）积，但近来常爱用张量积一词，所以我们在本卷中将采用这个名词,而且将使用近代标准符号⊗来代替卷2中的×. ——著者注.

1 的同态.

现设 $\mathfrak{o}$ 为域 P 的子环而 Φ 为 P 的由 $\mathfrak{o}$ 生成的子域. 我们知道, Φ 的元能表成简单分式 $\alpha\beta^{-1}$, 这里的元 $\alpha, \beta \in \mathfrak{o}(\beta \neq 0)$. 因此 Φ 是 P 的一个子环, 它是由 $\mathfrak{o}$ 及 $\mathfrak{o}$ 的非零元的逆元生成的, 我们将 $\mathfrak{o}$ 的非零元集用 $\mathfrak{o}^*$ 表示, 则集 $\mathfrak{o}^*$ 包含 1 且关于 $\mathfrak{o}$ 的乘法封闭. 有时将此情况作如下的推广是有益的: 设已给定 P 的一个子环 $\mathfrak{o}$ 及 $\mathfrak{o}^*$ 的一个子集 M, 它包含 1 且关于乘法封闭, 我们把这样的一个子集称为域的乘法群的子半群. 我们感兴趣的是由 $\mathfrak{o}$ 及 M 的元的逆元生成的子环 $\mathfrak{o}_M$. 例如, 我们可取 P 为有理数域 R_0 而 $M = \{2^k | k = 0, 1, 2, \cdots\}$, 则 $\mathfrak{o}_M$ 是分母为 2 的方幂的有理数子环. 一般情况是

$$\mathfrak{o}_M = \{\alpha\beta^{-1} | \alpha \in \mathfrak{o}, \beta \in M\};$$

因为, 如果将这个等式的右端的集合表为 $\mathfrak{o}'$, 则显然 $\mathfrak{o}' \subseteq \mathfrak{o}_M$, 而 $\mathfrak{o}'$ 包含 $\mathfrak{o} = \{\alpha = \alpha 1^{-1}\}$. 对于 $\beta \in M$, $\mathfrak{o}'$ 也包含每个 $\beta^{-1} = 1\beta^{-1}$. 可以直接验证 $\mathfrak{o}'$ 是 P 的一个子环, 故得 $\mathfrak{o}' = \mathfrak{o}_M$.

设 P′ 是第二个域且有 $\mathfrak{o}$ 到 P′ 内的一个同态 s; 它对于每个 $\beta \in M$ 总有 $\beta^s \neq 0$. 我们的第一个同态扩张定理就是关于这种情况的, 其结果是:

I 设 $\mathfrak{o}$ 是域 P 的(含有 1)一个子环, M 是 $\mathfrak{o}$ 的一个非零元的子集, 它包含 1 且关于乘法封闭, $\mathfrak{o}_M$ 是 $\mathfrak{o}$ 及 M 的元的逆元所生成的 P 的子环, 设 s 是 $\mathfrak{o}$ 到域 P′ 内的一个同态, 它对每个 $\beta \in M$ 都有 $\beta^s \neq 0$, 则 s 能唯一地扩张成 $\mathfrak{o}_M$ 到 P′ 内的同态 S. 此外, S 是一个同构, 当且仅当 s 是一个同构.

证 设 $\alpha_1\beta_1^{-1} = \alpha_2\beta_2^{-1}$, $\alpha_i \in \mathfrak{o}$, $\beta_i \in M$, 则 $\alpha_1\beta_2 = \alpha_2\beta_1$, 从而 $\alpha_1^s\beta_2^s = \alpha_2^s\beta_1^s$. 这个关系在 P′ 中给出 $\alpha_1^s(\beta_1^s)^{-1} = \alpha_2^s(\beta_2^s)^{-1}$. 因此定义在整个 $\mathfrak{o}_M = \{\alpha\beta^{-1}\}$ 上的映射

$$S: \alpha\beta^{-1} \to \alpha^s(\beta^s)^{-1}, \quad \alpha \in \mathfrak{o}, \ \beta \in M$$

是单值的. 可以验证 S 是一个同态 (卷 1 中译本 p.86). 今取 $\alpha \in \mathfrak{o}$, 则 $\alpha^S = (\alpha 1^{-1})^S = \alpha^s 1^s = \alpha^s$, 因此 S 在 $\mathfrak{o}$ 上是与 s 相同的. 故 S 是 $\mathfrak{o}_M$ 的一个同态, 它是由 $\mathfrak{o}$ 的已知同态扩张而成的. 现

设 S' 是任一这样的扩张，则对于 $\beta \in M$，关系 $\beta\beta^{-1}=1$ 将给出 $\beta^{S'}(\beta^{-1})^{S'}=1$，因此 $(\beta^{-1})^{S'}=(\beta^{S'})^{-1}$. 若 $\alpha \in \mathfrak{o}$，则有 $(\alpha\beta^{-1})^{S'}=\alpha^{S'}(\beta^{S'})^{-1}=\alpha^{s}(\beta^{s})^{-1}=(\alpha\beta^{-1})^{S}$，因此 $S'=S$，故 S 是唯一的. 显然，若 S 是一个同构，则它在 $\mathfrak{o}$ 上的限制 s 也是一个同构. 现设 s 是一个同构，且设 $\alpha\beta^{-1}$ 属于同态 S 的核：

$$0=(\alpha\beta^{-1})^{S}=\alpha^{s}(\beta^{s})^{-1},$$

则 $\alpha^{s}=0$，$\alpha=0$ 及 $\alpha\beta^{-1}=0$. 这表示 S 的核是 0；因此 S 是一个同构.

其次考虑任一交换环 $\mathfrak{A}$ 及多项式环 $\mathfrak{A}[x]$，x 是关于 $\mathfrak{A}$ 的超越元(卷1，中译本 p.87). $\mathfrak{A}[x]$ 的元形如

$$a_0+a_1x+a_2x^2+\cdots+a_nx^n,$$

其中 $a_i \in \mathfrak{A}$，而且仅当所有的 $a_i=0$ 时 $a_0+a_1x+\cdots+a_nx^n=0$. 于是我们有如下的同态定理：

II 令 $\mathfrak{A}$ 是一个交换环，$\mathfrak{A}[x]$ 是 $\mathfrak{A}$ 上的超越元 x 的多项式环，且 s 是 $\mathfrak{A}$ 到交换环 $\mathfrak{B}$ 内的同态，若 u 是 $\mathfrak{B}$ 的任一元，则必存在唯一的 $\mathfrak{A}[x]$ 到 $\mathfrak{B}$ 内的同态 S 使

$$a^{S}=a^{s},\quad a \in \mathfrak{A},\quad x^{S}=u.$$

对于这个证明读者可参看卷1(中译本 p.89). 此结果可直接扩广到多项式环 $\mathfrak{A}[x_1, x_2, \cdots, x_r]$，这里的 x_i 是代数无关元，而 x_i 的代数无关性指的是：若 $(m_1, m_2, \cdots, m_r)$ 是非负整数 m^i 的 r 数组，则关系 $\sum_{m_i} a_{m_1\cdots m_r}x_1^{m_1}\cdots x_r^{m_r}=0$ $(a_{m_1\cdots m_r} \in \mathfrak{A})$ 仅当每个 $a_{m_1\cdots m_r}=0$ 时成立. 今后我们把属于交换环而关于子环 $\mathfrak{A}$ 为代数无关的元 x_i 称为(关于 $\mathfrak{A}$ 的)未定元. 我们有

III 设 $\mathfrak{A}[x_1, \cdots, x_r]$ 是(关于 $\mathfrak{A}$ 的)未定元 x_i 的交换多项式环，s 是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的一个同态，若 $u_1, u_2, \cdots, u_r$ 是 $\mathfrak{B}$ 的任意元，则存在唯一的 $\mathfrak{A}[x_i]$ 到 $\mathfrak{B}$ 内的同态 S 使 1) $a^{S}=a^{s}$，$a \in \mathfrak{A}$；2) $x_i^{S}=u_i$，$i=1, 2, \cdots, r$.

现在我们假定有一个交换环 $\mathfrak{C}$，$\mathfrak{A}$ 是它的一个子环，s 是 $\mathfrak{A}$ 到另一交换环 $\mathfrak{B}$ 内的同态. 设 $t_1, t_2, \cdots, t_r$ 是 $\mathfrak{C}$ 的元而 $\mathfrak{A}[t_1, t_2, \cdots,$

$t_r]$ 是由 $\mathfrak{A}$ 及 t_i 生成的 $\mathfrak{C}$ 的子环. 我们问: 在什么条件下能使 s 扩张成一个 $\mathfrak{A}[t_i]=\mathfrak{A}[t_1, t_2, \cdots, t_r]$ 到 $\mathfrak{B}$ 内的同态 S 使 $t_i^S=u_i$, $1\leqslant i\leqslant r$, 其中 u_i 是 $\mathfrak{B}$ 的预先指定的元? 这个基本问题的回答是:

IV 令 $\mathfrak{B}$ 及 $\mathfrak{C}$ 都是交换环, $\mathfrak{A}$ 是 $\mathfrak{C}$ 的一个子环, s 是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的一个同态, $t_1, t_2, \cdots, t_r$ 是 $\mathfrak{C}$ 的元, $u_1, u_2, \cdots, u_r$ 是 $\mathfrak{B}$ 的元, 则存在一个 $\mathfrak{A}[t_1, \cdots, t_r]$ 到 $\mathfrak{B}$ 内的同态 S 使 $a^S=a^s$ ($a\in\mathfrak{A}$) 及 $t_i^S=u_i (i=1, 2, \cdots, r)$, 当且仅当对于每个多项式 $f(x_1, \cdots, x_r)\in\mathfrak{A}[x_i]$ (x_i 是未定元) 都有: 若 $f(t_1, \cdots, t_r)=0$, 则 $f^s(u_1, \cdots, u_r)=0$, 这里 $f^s(x_1, \cdots, x_r)$ 是将 s 作用在 $f(x_1, \cdots, x_r)$ 的系数上而得到的. 若 S 存在, 则它是唯一的.

证. 使 $f(t_1, \cdots, t_r)=0$ 的多项式 $f(x_1, \cdots, x_r)$ 的集 $\mathfrak{K}$ 是 $\mathfrak{A}[x_i]$ 到 $\mathfrak{A}[t_i]$ 内的同态 $h(x_1, \cdots, x_r)\to h(t_1, \cdots, t_r)$ 的核, 因此我们有 $\mathfrak{A}[t_i]$ 到差环 $\mathfrak{A}[x_i]/\mathfrak{K}$ 上的同构 $\tau: h(t_1, \cdots, t_r)\to h(x_1, \cdots, x_r)+\mathfrak{K}$. 然后考虑 $\mathfrak{A}[x_i]$ 到 $\mathfrak{B}$ 内的同态 $h(x_1, \cdots, x_r)\to h^s(u_1, \cdots, u_r)$ (参考 III). 假定对于每个 $f\in\mathfrak{K}$ 都有 $f^s(u_1, \cdots, u_r)=0$, 则每个 $f\in\mathfrak{K}$ 都被同态 $h(x_1, \cdots, x_r)\to h^s(u_1, \cdots, u_r)$ 映入到0, 因此 $\mathfrak{K}$ 含于此同态的核中, 从而(参看卷 1 中译本 p.67)我们有 $\mathfrak{A}[x_i]/\mathfrak{K}$ 到 $\mathfrak{B}$ 内的同态 $h(x_1, \cdots, x_r)+\mathfrak{K}\to h^s(u_1, \cdots, u_r)$. 把它与同构 τ 结合就得到 $\mathfrak{A}[t_i]$ 到 $\mathfrak{B}$ 内的同态

$$S: h(t_1, \cdots, t_r)\to h^s(u_1, \cdots, u_r), \tag{1}$$

这就是所要求的 s 的扩张. 若 S' 是 s 的由 $\mathfrak{A}[t_i]$ 到 $\mathfrak{B}$ 内的同态的任一扩张, 它使 $a^{S'}=a^s$ 及 $t_i^{S'}=u_i$, 则 $h(t_1, \cdots, t_r)^{S'}=h^s(u_1, \cdots, u_r)$; 因此 $S'=S$. 故 S 是唯一的. 显然还有: 若 S 是 $\mathfrak{A}[t_1, \cdots, t_r]$ 的一个满足条件的同态, 那么由 $f(t_1, \cdots, t_r)=0$ 必有 $0=f(t_1, \cdots t_r)^S=f^s(u_1, \cdots, u_r)$. 显然可见定理中的条件是存在扩张 S 所必须的.

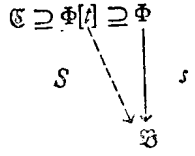
我们在定理的证明中曾经指出, 使 $f(t_1, \cdots, t_r)=0$ 的多项式 $f(x_1, \cdots, x_r)$ 的集 $\mathfrak{K}$ 是同态的核, 因此它是多项式环 $\mathfrak{A}[x_1, x_2, \cdots, x_r]$ 中的一个理想. 令 $X=\{g\}$ 为 $\mathfrak{K}$ 的一个生成元集:

$X\subseteq\mathfrak{R}$，则每个元 $f\in\mathfrak{R}$ 可表成 $\sum a_i(x_1,\cdots x_r)g_i(x_1,\cdots,x_r)$，这里 $a_i(x_1,\cdots,x_r)\in\mathfrak{A}[x_1,x_2,\cdots,x_r]$，而 $g_i(x_1,\cdots,x_r)\in X$. 显然可见：如果 $g^s(u_1,\cdots,u_r)=0$ 对每个 $g\in X$ 成立，则 $f^s(u_1,\cdots,u_r)=0$ 也对每个 $f\in\mathfrak{R}$ 成立，因而我们可以从 IV 得到一个较 IV 更便于应用的下述结果：

IV 令 $\mathfrak{B}$ 及 $\mathfrak{C}$ 为交换环，$\mathfrak{A}$ 为 $\mathfrak{C}$ 的一个子环，s 是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的一个同态，X 是 $\mathfrak{A}[x_1,x_2,\cdots,x_r]$ 中适合条件 $f(t_1,t_2,\cdots,t_r)=0$ 的多项式 f 构成的理想 $\mathfrak{R}$ 的生成元集，其中 x_i 为未定元，则当且仅当对于每个 $g\in X$ 都有 $g^s(u_1,\cdots,u_r)=0$ 时，存在一个 $\mathfrak{A}[t_1,t_2,\cdots,t_r]$ 到 $\mathfrak{B}$ 内的同态 S 使 $a^S=a^s(a\in\mathfrak{A})$，$t_i^S=u_i$ $(1\leqslant i\leqslant r)$. 若 S 存在，则它是唯一的.

现考虑 IV′ 的一个重要特殊情况：$\mathfrak{A}=\Phi$ 是一个域且 $r=1$. 我们知道这时的 $\Phi[x]$ 是一个主理想整区(卷 1 的中译本 p.93)，所以此理想 $\mathfrak{R}=(f(x))$，这里 $(f(x))$ 表示多项式 $f(x)\in\mathfrak{R}$ 的多项式倍式构成的理想. 显然 $\mathfrak{R}\neq 1=\Phi[x]$，因若不然，将有 $0=\Phi[x]/\mathfrak{R}\cong\Phi[t]\supseteq\Phi$，而这是与 $1\neq 0$ 矛盾的. 因为如果 α 是 Φ 的非零元时有 $(\alpha)=(1)$，显然 $\mathfrak{R}$ 只能有两种可能，即 $\mathfrak{R}=(0)$ 或者 $\mathfrak{R}=(f(x))$，这里的 $f(x)$ 是 $\Phi[x]$ 中的一个非零的正次数多项式. 在第一种情况，我们有 $\Phi[x]\cong\Phi[t]$，而 t 是超越元. 这时应用 II (或 IV) 就能将 s 扩张成将 t 映入到任一 $u\in\mathfrak{B}$ 的一个同态 S. 现设 $f(x)\neq 0$，在这一情况下，我们称元 $t\in\mathfrak{C}$ 为 Φ 上的代数元，这是因为我们有非零多项式 $f(x)$ 使 $f(t)=0$. 由定义，理想 $\mathfrak{R}$ 是使 $g(t)=0$ 的多项式 $g(x)$ 的集. 多项式 $f(x)$ 是 $\mathfrak{R}$ 中次数最低的一个多项式，而含于 $\mathfrak{R}=(f(x))$ 之中的每个其它多项式的形式为 $g(x)f(x)$. 用 $f(x)$ 的首项系数的逆元乘 $f(x)$，就能将 $f(x)$ 正规化为首项系数为 1 的多项式. 令 $f(x)$ 为这个多项式，则 f 显然可用下列性质来刻划：它是 $\Phi[x]$ 的、首项系数为 1 的、满足 $f(t)=0$ 的最低次数多项式，我们将称 $f(x)$ 为 (Φ 上的) 代数元 $t\in\mathfrak{C}$ 的最小多项式. 对于 IV′ 的这种特殊情况，有如下结论：

V 设 $\mathfrak{B}$ 及 $\mathfrak{C}$ 为交换环，Φ 为 $\mathfrak{C}$ 的子域，$t\in\mathfrak{C}$ 是 Φ 上的代数元，s 是 Φ 到 $\mathfrak{B}$ 内的一个同构：



则 s 可扩张成 $\Phi[t]$ 到 $\mathfrak{B}$ 内的一个同态 S 使 $t^S=u$，当且仅当对于 Φ 上的 t 的最小多项式 $f(x)$ 有 $f^s(u)=0$. 若此扩张存在，则它是唯一的.

附注 保证 S 存在的附加在 u 上的条件也可改用下列方式表述：u 是 Φ 的象 Φ^s 上的代数元，它在 Φ^s 上的最小多项式是 $f^s(x)$ 的一个因式，关于 S 的(1)式现变为

$$S:\ g(t)\to g^s(u). \tag{2}$$

由此易得：S 是一个同构当且仅当 $f^s(x)$ 是 u 的最小多项式.

2. 代数 现在来回顾域 Φ 上的代数 $\mathfrak{A}$ 的定义（卷 2 的中译本 p.32 及 p.201）：$\mathfrak{A}$ 是 Φ 上的向量空间，而且对于 $\mathfrak{A}$ 中的任意元 x，y 定义了一个“乘积” $xy\in\mathfrak{A}$，使得

$$\begin{aligned}&(x_1+x_2)y=x_1y+x_2y,\ x(y_1+y_2)=xy_1+xy_2\\&\alpha(xy)=(\alpha x)y=x(\alpha y)\quad(\alpha\in\Phi).\end{aligned} \tag{3}$$

我们关心的仅是有单位元 1 且可结合的代数，因此本卷中的“代数”仅限于这种.

我们经常遇到以下述方式出现的代数：给定一个环 $\mathfrak{A}$ 及 $\mathfrak{A}$ 的中心的一个子域 Φ，我们就可以把 $\mathfrak{A}$ 看成是 Φ 上的向量空间，这只要把 $\alpha x(\alpha\in\Phi,\ x\in\mathfrak{A})$ 按照 α 与 x 在 $\mathfrak{A}$ 中的环的乘积规定就行了. 显然这能使 $\mathfrak{A}$ 成为 Φ 上的向量空间. 由于 α 属于环 $\mathfrak{A}$ 的中心，(3)是显然成立的. 因此我们有代数 $\mathfrak{A}/\Phi$（Φ 上的 $\mathfrak{A}$）[1].

---

1) 我们还用记号 $\mathfrak{A}/\mathfrak{B}$ 表示 $\mathfrak{A}$ 关于理想 $\mathfrak{B}$ 的差环，但它们是很容易从前后文区分开来的. ——著者注

这种定义代数的方法将被应用到域 P 关于它的子域 Φ 的研究，这时就得到代数 P/Φ.

另一基本的代数是域 Φ 上的向量空间 $\mathfrak{M}$ 的线性变换代数 $\mathfrak{L}_\Phi(\mathfrak{M})$，这里对于 A, $B\in\mathfrak{L}_\Phi(\mathfrak{M})$ 及 $\alpha\in\Phi$, $A+B$, AB 及 αA 的定义是: $x(A+B)=xA+xB$, $x(AB)=(xA)B$, $x(\alpha A)=\alpha(xA)=(\alpha x)A$. $\mathfrak{L}_\Phi(\mathfrak{M})$ 关于 Φ 的维数 $[\mathfrak{L}_\Phi(\mathfrak{M}):\Phi]$ 有限当且仅当 $[\mathfrak{M}:\Phi]$ 有限. 若 $[\mathfrak{M}:\Phi]=m$, 则 $[\mathfrak{L}_\Phi(\mathfrak{M}):\Phi]=m^2$ (卷 2 的中译本 p.36).

显然一个代数对于向量空间的加法 $a+b$ 及乘法 ab 来说是一个环. Φ 上的代数 $\mathfrak{A}$ 的一个子代数 $\mathfrak{B}$ 是 $\mathfrak{A}$ 的一个子空间而且也是它的一个子环. $\mathfrak{A}/\Phi$ 的一个理想是一个子空间，且在将 $\mathfrak{A}$ 看作环时，它是 $\mathfrak{A}$ 的一个理想. 代数 $\mathfrak{A}/\Phi$ 到代数 $\mathfrak{B}/\Phi$ 内的一个同态 s 是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的一个映射，它是 Φ 线性的而且是环同态的. 同构与自同构可类似地定义. 若 $\mathfrak{R}$ 是 $\mathfrak{A}/\Phi$ 的一个理想，则商空间 $\mathfrak{A}/\mathfrak{R}$ 关于它的向量空间的合成及乘法 $(a+\mathfrak{R})(b+\mathfrak{R})=ab+\mathfrak{R}$ 来说是 Φ 上的代数. 我们有由 $\mathfrak{A}/\Phi$ 到 $\mathfrak{A}/\mathfrak{R}$ 上的关于 Φ 的代数同态 $a\to a+\mathfrak{R}$. 若 s 是 $\mathfrak{A}/\Phi$ 到 $\mathfrak{B}/\Phi$ 内的同态，则象 $\mathfrak{A}^s$ 是 $\mathfrak{B}$ 的一个子代数且 s 的核 $\mathfrak{R}$ 是 $\mathfrak{A}$ 的一个理想. 我们有 $\mathfrak{A}/\mathfrak{R}$ 到 $\mathfrak{A}^s$ 上的同构 $a+\mathfrak{R}\to a^s$. 关于环同态的基本结果可以推广到代数，我们将直接应用它们而不另作声明.

我们现在将一些今后常用的有限维代数的基本结果写在下面. 第一个涉及 $\mathfrak{A}/\Phi$ 及 $\mathfrak{A}/E$ 的维数关系，这里 E 是 Φ 的子域. 若 E 是 Φ 的一个子域，则我们可以将乘法 $\alpha x(\alpha\in\Phi,\ x\in\mathfrak{A})$ 中的 α 限制在 E 里面，这就将 $\mathfrak{A}$ 变成 E 上的代数 $\mathfrak{A}$. 还因为 E 是 Φ 的一个子域，我们可以定义代数 Φ/E. 于是有

VI 设 $\mathfrak{A}$ 为 Φ 上的代数，E 为 Φ 的一个子域，若 $[\mathfrak{A}:\Phi]<\infty$ 及 $[\Phi:E]<\infty$, 则

$$[\mathfrak{A}:E]=[\mathfrak{A}:\Phi][\Phi:E] \tag{4}$$

证 设 (u_i) $(1\leqslant i\leqslant n)$ 为 $\mathfrak{A}/\Phi$ 的一个基，$(\gamma_j)(1\leqslant j\leqslant m)$ 为 Φ/E 的一个基，我们若能证明 $(\gamma_j u_i)$ 是 $\mathfrak{A}/E$ 的一个基，

则就证明了(4). 先令 $a \in \mathfrak{A}$, 则 $a = \sum_{1}^{n} \alpha_i u_i (\alpha_i \in \Phi)$, 又因 $\alpha_i = \sum_{j=1}^{m} \varepsilon_{ij}\gamma_j (\varepsilon_{ij} \in E)$, 所以 $a = \sum \varepsilon_{ij}\gamma_j u_i$ 是系数 ε_{ij} 在 E 中的元 $\gamma_j u_i$ 的一个线性组合. 现设 $\sum \varepsilon_{ij}\gamma_j u_i = 0$ $(\varepsilon_{ij} \in E)$, 亦即 $\sum \alpha_i u_i = 0$ $\left(\alpha_i = \sum_{j} \varepsilon_{ij}\gamma_j \in \Phi\right)$. 因为 u_i 是 Φ 无关的, 故 $\alpha_i = 0 (1 \leqslant i \leqslant n)$. 再由公式 $\alpha_i = \sum \varepsilon_{ij}\gamma_j$ 及 γ_j 的 E 无关性得到: 对于一切 i, j, $\varepsilon_{ij} = 0$. 这就证明了元素 $\gamma_j u_i$ 是 E 无关的, 从而它们是 $\mathfrak{A}/E$ 的一个基.

VII 若 $\mathfrak{A}$ 是域 Φ 上的一个有限维代数, 则 $\mathfrak{A}$ 是一个可除环当且仅当 $\mathfrak{A}$ 是一个整区.

证 我们知道除环必为整区 (卷 1 的中译本 p.53). 现设 $\mathfrak{A}$ 是一个整区而 a 是 $\mathfrak{A}$ 的任一非零元, 考虑被 a 决定的右乘映射 a_R: $x \to xa$, 这是 $\mathfrak{A}/\Phi$ 中的一个线性变换, 而且因为在 $\mathfrak{A}$ 中由 $ba = 0$ 可推出 $b = 0$, a_R 的零空间为 0, 因而 a_R 是满射 (即 $\mathfrak{A}$ 到 $\mathfrak{A}$ 上的映射), 因此存在一个元 a' 使 $a'a = a'a_R = 1$, 即 a 有一左逆元; 利用左乘映射作类似的推导可得 a 有一右逆元. 因此 $\mathfrak{A}$ 的每个非零元都是一个单位, 从而 $\mathfrak{A}$ 是一个可除环.

其次我们考虑有单个生成元 t 的代数 $\mathfrak{A} = \Phi[t]$ (参考 §1). 我们有 $\Phi[x]$ (这里 x 是未定元)到 $\mathfrak{A}$ 上的同态 $g(x) \to g(t)$. 若 $\mathfrak{R}$ 是它的核, 则 $\mathfrak{A} \cong \Phi[x]/\mathfrak{R}$. 我们在 §1 中还证明过 $\mathfrak{R} = (f(x))$, 这里 $f(x) = 0$ 或是一个首项系数为 1 的非零多项式. 在第一种情况, t 是超越元而所给的同态是一个同构; 在第二种情况, t 是代数元而 $f(x)$ 是它的最小多项式. 因此我们有:

VIII 令 $\mathfrak{A} = \Phi[t]$ 是 Φ 上的由单个代数元 t 生成的代数, 其最小多项式为 $f(x)$, 则

(5) $$[\mathfrak{A}:\Phi] = \deg f(x),$$

这里, $\deg f(x)$ 表示 $f(x)$ 的次数.

证 令 $n = \deg f(x)$, 我们可断言 $(1, t, \cdots, t^{n-1})$ 是 $\mathfrak{A}/\Phi$

的一个基. 若令 a 为 $\mathfrak{A}=\Phi[t]$ 的任一元,那么它就有多项式形式 $g(t)$, 这里 $g(x)$ 是 $\Phi[x]$ 中的多项式. 由 $\Phi[x]$ 中的除法可得 $g(x)=f(x)q(x)+r(x)$, 这里的 $\deg r(x)<\deg f(x)$. 因此若利用 $\Phi[x]/\Phi$ 到 $\Phi[t]/\Phi$ 上的将 x 变为 t 的同态,我们就可得到 $a=g(t)=0\ q(t)+r(t)$. 由于 $\deg r(x)<n$, 这表示 $a=r(t)$ 是 $1, t, \cdots, t^{n-1}$ 的一个 Φ 线性组合. 其次我们还应注意 $1, t, \cdots, t^{n-1}$ 关于 Φ 是线性无关的(否则我们将有一个次数 $<n$ 的多项式 $g(x)\neq 0$ 使 $g(t)=0$, 这与 $f(x)$ 是最小多项式的假设矛盾). 故 $(1, t, \cdots, t^{n-1})$ 是一个基,因而(5)成立.

我们知道, $\Phi[t]\cong\Phi[x]/(f(x))$ ($f(x)$ 是一个正次数多项式)是一个域当且仅当 $f(x)$ 是不可约的(卷1的中译本 p.96),否则 $\Phi[t]$ 不是一个整区、利用最小多项式 $f(x)$ 对 $\Phi[t]$ 的结构作一个完备的分析是很有用的, 在下面习题中我们将指出这些结果.

习 题 1

1.代数 $\mathfrak{A}$ 是理想 $\mathfrak{A}_i$ 的一个直和, 如果 $\mathfrak{A}$ 是子空间 $\mathfrak{A}_i$ 的向量空间的直和. $\mathfrak{A}=\Phi[t]$, t 是最小多项式为 $f(x)$ 的代数元. 假设 $f(x)=f_1(x)f_2(x)\cdots f_r(x)$, 这里的 $(f_i(x), f_j(x))=1\ (i\neq j)$. 今令 $q_i(x)=f(x)/f_i(x)$, 证明存在多项式 $a_i(x)$ 使得

$$\sum_1^r a_i(x)q_i(x)=1.$$

令 $e_i=a_i(t)q_i(t)$, 证明

$$e_1+e_2+\cdots+e_r=1,\quad e_i^2=e_i,\quad e_ie_j=0,\quad i\neq j.$$

并证明 $\mathfrak{A}=\mathfrak{A}e_1\oplus\mathfrak{A}e_2\oplus\cdots\oplus\mathfrak{A}e_r$, 而且在将理想 $\mathfrak{A}e_i=\{ae_i\mid a\in\mathfrak{A}\}$ 作为有单位元 e_i 的一个代数考虑时有形式 $\Phi[te_i]$, 并与 $\Phi[x]/(f_i(x))$ 同构.

2.设 $\mathfrak{A}=\Phi[t]$, t 是最小多项式为 $f(x)$ 的代数元. 设 $f(x)=p_1(x)^{k_1}p_2(x)^{k_2}\cdots p_r(x)^{k_r}$, $p_i(x)$ 是不可约多项式, $p_i(x)\neq p_j(x)$, $i\neq j$. 证明, 若 $z=p_1(t)p_2(t)\cdots p_r(t)$, 则 $\mathfrak{A}$ 的理想 $\mathfrak{N}=\mathfrak{A}z$ 在下述意义下是幂零的: 存在一个整数 k, $\mathfrak{N}$ 中任意 k 个元的积均为0. 证明: $\mathfrak{A}=\mathfrak{A}/\mathfrak{N}=\Phi[\bar{t}]$, $\bar{t}=t+\mathfrak{N}$, $\bar{t}$ 是最小多项式为 $g(x)=p_1(x)p_2(x)\cdots p_r(x)$的代数元. 证明: $\bar{\mathfrak{A}}=\bar{\mathfrak{A}}_1\oplus\bar{\mathfrak{A}}_2\oplus\cdots\oplus\bar{\mathfrak{A}}_r$, 这里的 $\bar{\mathfrak{A}}_i$ 是一个理想,在看作代数时同构于域 $\Phi[x]/(p_i(x))$.

3.代数 $\mathfrak{A}/\Phi$ 在以下意义下称为代数的,如果 $\mathfrak{A}$ 的每个元都是代数元. 证明: 若