

域 論

戴 执 中

高等教育出版社

域 论

戴 执 中

高等教育出版社

域论是代数学的一个重要分支,它有许多应用。本书为对域论感兴趣的读者提供一本读物。本书共分八章,前五章介绍域的基本理论,后三章介绍域的非代数结构。

本书叙述清楚,论证严格,文字简炼,并配有一定数量的习题。

本书可用作数学专业高年级学生的选修课教材或研究生教材,也可供代数工作者参考。

域 论

戴 执 中

*

高等教育出版社出版

新华书店北京发行所发行

国防工业出版社印刷厂印装

*

开本 850×1168 1/32 印张 10.75 字数 257,000

1990年7月第1版 1990年7月第1次印刷

印数 0001—1900

ISBN 7-04-002069-6/O·738

定价 2.90元

前 言

作为代数学的一个分支,域论的重要性,无论从它本身的发展,或是与其他数学分支的关系而言,都是无可置疑的。但与群论,或者环论相比,域论方面的书籍却感到缺少,在国内尤其如此。本书的目的,是为对域论有兴趣的读者提供一本读物。它的内容,绝大部分是基本的。因此,只需具有一般抽象代数的知识,就可阅读。全书分八章,第一章是全书的基础。如果用于大学高年级的选修课程,那么前五章,甚至第一、二、五等三章也就够了。后面三章属于域的非代数结构,其中六、七两章稍长,第八章是在上述两章的基础上来讨论域的拓扑结构。至于拓扑域的一般理论,则不在本书的范围之内。书末列举了各章的参考文献,它们仅仅是直接引用到的;或者是该章的一些可资参考的读物;或者是某一方面的最早的论文。中国科技大学冯克勤教授曾对本书提出很宝贵的意见,谨在此对他表示衷心感谢。限于作者的水平,本书虽在试用过程中几经修改,错误与不妥之处必然还有,希望读者批评指正。

作 者

目 录

第一章 代数扩张	1
§ 1.1 一些基本事实	1
§ 1.2 代数元与代数扩张	3
§ 1.3 代数闭域·域的代数闭包	8
§ 1.4 可分代数扩张	2
§ 1.5 正规扩张	18
§ 1.6 同态映射的线性无关性	23
§ 1.7 Galois 扩张	25
§ 1.8 有限 Galois 扩张的基本定理	30
§ 1.9 本原元定理	34
§ 1.10 范与迹	36
§ 1.11 判别式	42
§ 1.12 循环扩张: 次数为特征的幂	45
§ 1.13 循环扩张: 次数与特征互素	52
§ 1.14 分圆域	55
§ 1.15 有限域	62
§ 1.16 正规基	60
习题	64
第二章 方程的 Galois 理论	67
§ 2.1 多项式的 Galois 群	67
§ 2.2 根式扩张·Galois 定理	73
§ 2.3 n 次一般方程	80
§ 2.4 Hilbert 不可约性定理	83
§ 2.5 Galois 群为 S_n 的多项式	90
习题	93

第三章 无限 Galois 理论	94
§ 3.1 无限 Galois 扩张	94
§ 3.2 Galois 群的 Krull 拓扑	96
§ 3.3 反向极限	101
习题	105
第四章 Kummer 扩张与 Abel p-扩张	107
§ 4.1 Galois 上同调	107
§ 4.2 Abel 群的对偶群	109
§ 4.3 Kummer 扩张	112
§ 4.4 Witt 向量	117
§ 4.5 Abel p -扩张	122
习题	127
第五章 超越扩张	128
§ 5.1 代数相关性	128
§ 5.2 单超越扩张·Lüroth 定理	132
§ 5.3 线性分离性	138
§ 5.4 可分扩张	141
§ 5.5 求导	146
§ 5.6 正则扩张	153
§ 5.7 域的张量积与域的合成	159
§ 5.8 曾维数与条件 C_1	169
习题	180
第六章 赋值	182
§ 6.1 绝对值	182
§ 6.2 完全域·阿基米德绝对值	189
§ 6.3 赋值和赋值环	197
§ 6.4 位·同态的拓展定理及应用	204
§ 6.5 赋值在代数扩张上的拓展	211
§ 6.6 基本不等式	216
§ 6.7 Hensel 赋值	222
§ 6.8 非分歧扩张与弱分歧扩张	230

§ 6.9 局部域	236
习题	245
第七章 实域	247
§ 7.1 可序域与实域	247
§ 7.2 实闭域	254
§ 7.3 Artin-Schreier 定理	262
§ 7.4 Sturm 性质与 Sturm 定理	264
§ 7.5 序扩张·实闭包	270
§ 7.6 Pythagoras 域	279
§ 7.7 阿基米德序域	283
§ 7.8 实函数域	289
§ 7.9 具有 Hilbert 性质的序域	295
§ 7.10 序域的相容赋值·实位的拓展	303
习题	310
第八章 赋值或序所确定的拓扑结构	313
§ 8.1 拓扑域	313
§ 8.2 赋值与 V -拓扑	315
§ 8.3 局部紧致域	322
§ 8.4 序域的拓扑	327
索引	330
参考文献	334

第一章 代数扩张

§ 1.1 一些基本事实

设 K 是一个域; F 是它的子集, 至少包含两个元素. 若对于 K 的加法与乘法运算, F 也成一个域, 而且与 K 有公共的乘法单位元素 1, 则称 F 是 K 的一个子域, K 是 F 的扩张(或扩域). 这种关系常简记成 $F \subseteq K$. 由 K 中所有子域所成的交, 仍然是 K 的子域, 而且是按包含关系的最小子域. 这个唯一确定的子域, 称为 K 的素子域. 在 $F \subseteq K$ 的情形下, F 的素子域也就是 K 的素子域. 一个域, 如果它的素子域就是它自身, 则称为素域. 素域可分为两类, 一类同构于有理数域 $\mathbf{Q}$, 我们称它的特征为 0. 另一类同构于整数环 $\mathbf{Z}$ 关于某个素主理想 (p) 的剩余类域 $\mathbf{Z}/(p)$, 我们称它的特征为 $p (\neq 0)$. 后者只含 p 个元素, 有时记作 $\mathbf{F}_p$. 域的特征是指它的素子域的特征.

设 K 是域 F 的扩张. 它可以作为 F 上的向量空间, 所以也写作 K/F . 我们称它的维数 $\dim K/F$ (或 $\dim_F K$) 为 K 关于 F 的扩张次数(也可径称 K/F 的扩张次数), 记作 $[K:F]$. 当 $[K:F]$ 是个有限数时(简记作 $[K:F] < \infty$), 称 K 是 F 的有限扩张.

设 S 是域 K 的一个子集. K 中所有包含 S , 以及子域 F 的子域, 它们所成的交仍然是 K 的一个子域, 而且是具有此一性质的最小子域(按包含关系而言). 我们称这个确定的子域是添加 S 于 F 所得的扩张, 或者, S 在 F 上生成的域, 记作 $F(S)$. 此时存在如下的关系

$$F \subseteq F(S) \subseteq K.$$

今考虑 $F(S)$ 的元素. 作单项式

$$au_1^{r_1} \cdots u_m^{r_m}, \quad (1.1.1)$$

其中 $a \in F$, $u_j \in S$, $r_j \geq 0$ 是整数. 按 K 中的加法与乘法, 所有具形式 (1.1.1) 的单项式, 生成一个子环, 记作 $F[S]$. 从而 $F(S)$ 的元素都可以表如

$$f(S)/g(S),$$

其中 $f(S), g(S) \in F[S]$. 这就是说, $F(S)$ 的元素可表如 $F[S]$ 中两个元素的商. 因此, 称 $F(S)$ 为子环 $F[S]$ 的商域.

对于 K 中两个元素集 S_1, S_2 , 由上面的定义, 可知 $S_1 \cup S_2$ 在 F 上生成的域 $F(S_1 \cup S_2)$, 与 S_2 在 $F(S_1)$ 上生成的 $F(S_1)(S_2)$ 是相同的. 因此, 不妨记作 $F(S_1, S_2)$. 据此, 当 S 是有限集 $\{u_1, \dots, u_n\}$ 时, $F(S)$ 可以径写如 $F(u_1, \dots, u_n)$. 我们称后者在 F 上是有限生成的; 特别当 $S = \{u\}$ 只含一个元素时, 称 $F(u)$ 为 F 的单扩张. 从而 F 上有限生成的域 $F(u_1, \dots, u_n)$ 可以经有限个单扩张而得到:

$$F \subseteq F(u_1) \subseteq F(u_1, u_2) \subseteq \cdots \subseteq F(u_1, \dots, u_n).$$

命题 1 若 K 是 F 的一个有限扩张, 则 K 在 F 上是有限生成的.

证明 设 $[K:F] = n$; $\{w_1, \dots, w_n\}$ 是 K/F 作为向量空间的一个基. 于是 K 的元素都可以表如

$$\alpha = \sum_{j=1}^n a_j w_j, \quad a_j \in F.$$

因此有 $F(w_1, \dots, w_n) \subseteq K \subseteq F(w_1, \dots, w_n)$, 从而 $K = F(w_1, \dots, w_n)$. ■

这个命题的逆理一般是不成立的, 以后将可见到.

定理 1.1 若域 F, E, K 满足 $F \subseteq E \subseteq K$, 则有等式

$$[K:F] = [K:E][E:F]. \quad (1.1.2)$$

证明 设 $\{\alpha_1, \dots, \alpha_r\}$ 是 K/E 的一组线性无关元; $\{\beta_1, \dots, \beta_t\}$ 是 E/F 的一组线性无关元. 于是,

$$\{\alpha_i \beta_j \mid i=1, \dots, r; j=1, \dots, t\}$$

是 K/F 的 rt 个线性无关元(证明略). 这示明了, 从 $[K:E] \geq r$ 以及 $[E:F] \geq t$, 可以导至 $[K:F] \geq rt$. 从而有 $[K:F] \geq [K:E][E:F]$. 若(1.1.2)的右边有一个是无限数, 定理即告成立. 今设 $[K:E] = n < \infty$, $[E:F] = m < \infty$. 任取 K/E 的一个基 $\{\alpha_1, \dots, \alpha_n\}$, 与 E/F 的一个基 $\{\beta_1, \dots, \beta_m\}$. 于是 K 的每个元素都可由

$$\{\alpha_i \beta_j \mid i=1, \dots, n; j=1, \dots, m\}$$

在 F 上的线性组合表出, 故又有 $[K:F] \leq [K:E][E:F]$. ■

推论 1 对于由有限多个域所成的列

$$F = E_0 \subseteq E_1 \subseteq \dots \subseteq E_{n-1} \subseteq E_n = K,$$

有 $[K:F] = [K:E_{n-1}][E_{n-1}:E_{n-2}] \dots [E_1:F]$. ■

推论 2 在定理的所设下, 若 K/F 是有限扩张, 则 E/F 也是有限扩张. ■

定理中的域 E , 以及推论 1 中的 E_i , 都称作 K/F 的中间域.

§ 1.2 代数元与代数扩张

定义 1.1 设 K 是 F 的扩张, $\alpha \in K$. 若 α 满足 F 上的方程 $f(X) = a_0 X^n + a_1 X^{n-1} + \dots + a_n = 0$, $a_i \in F$, $a_0 \neq 0$ (1.2.1) 就称 α 是 F 上的代数元, 或者, α 关于 F 是代数的. 否则, 如果 α 不满足 F 上任何一个方程, 就称 α 是 F 上的超越元, 或者, 关于 F 是超越的. 如果 K 的每个元素都是 F 上的代数元, 就称 K 是 F 的一个代数扩张. 否则, 称 K 是 F 的超越扩张.

设 $u \in K$ 是 F 上的一个代数元. 在所有满足 $f(u) = 0$ 的多项式 $f(X) \in F[X]$ 中, 令 $m(X)$ 是次数最低、且首系数是 1 的一

个. 易知, 这个 $m(X)$ 是唯一确定的; 而且满足: (1) 它在 F 上是不可约的, (2) 若 $f(X) \in F[X]$ 使得有 $f(u) = 0$, 则必有 $m(X) \mid f(X)$. 我们称这个 $m(X)$ 是 u 在 F 上的极小多项式. F 上的代数元 u_1, u_2 , 如果在 F 上有相同的极小多项式, 就称 u_1 与 u_2 是 F 上的共轭元. 或者说, 它们是 F -共轭的.

命题 1 F 上的有限扩张都是代数扩张.

证明 设 $[K:F] = n < \infty$. 任取 $0 \neq u \in K$, 并且考虑 K 中的元素组

$$\{1, u, u^2, \dots, u^n\}. \quad (1.2.2)$$

如果其中出现相等的, 例如 $u^r = u^t$ ($r < t$), 则 u 显然是 F 上的代数元. 设 (1.2.2) 中的元素全不相等. 由于它所含的元素数是 $n+1$, 按所设, 在 F 上应是线性相关的, 故

$$a_0 u^n + a_1 u^{n-1} + \dots + a_n = 0, \quad a_j \in F.$$

因此 u 是 F 上的代数元. 从 u 的任意性, 知 K 是 F 上的代数扩张. ■

从这个命题可以知道, F 上有限生成的扩张不必是有限扩张. 因若 $\alpha \in K$ 是 F 上的超越元, $F(\alpha)$ 就不能是 F 上的有限扩张. 例如在实数域 $\mathbb{R}$ 中, 由超越数 π 在 $\mathbb{Q}$ 上生成的子域 $\mathbb{Q}(\pi)$, 就是一个例子.

当 u 是 F 上的代数元时, $F(u)$ 称作 F 上的单代数扩张. 今有以下的

定理 1.2 设 u 是 F 上的一个代数元, 它的极小多项式为 $m(X)$. 于是有 $[F(u):F] = \deg m(X)$, 以及 $F(u) = F[u]$.

证明 设 $m(X) = X^n + a_1 X^{n-1} + \dots + a_n$. 于是有

$$u^n = -a_1 u^{n-1} - \dots - a_n. \quad (1.2.3)$$

从而在子环 $F[u]$ 中, 每个元素都可以表作 $1, u, \dots, u^{n-1}$ 在 F 上的线性组合. 另一方面, $\{1, u, \dots, u^{n-1}\}$ 是 F 上的一个线性无关

组. 因此, 作为 F 上的向量空间 $F[u]$, $\{1, u, \dots, u^{n-1}\}$ 是它的一个基.

前面提到, $F(u)$ 中每个元素都可表如 $f(u)/g(u)$, 其中 $f(u), g(u) \in F[u]$, 且 $f(u), g(u)$ 的次数都 $\leq n-1$. 由于 $m(X)$ 在 F 上不可约, 故 $m(X)$ 与 $g(X)$ 在 F 上是互素的. 因此有

$$a(X), b(X) \in F[X],$$

使得 $a(X)g(X) + b(X)m(X) = 1$,

并且 $a(X), b(X)$ 的次数都 $\leq n-1$. 以 $X=u$ 代入上式, 得

$$a(u)g(u) = 1, \text{ 或者 } 1/g(u) = a(u).$$

这说明了

$$f(u)/g(u) = a(u)f(u) \in F[u],$$

从而

$$F(u) = F[u].$$

至于

$$[F(u):F] = n = \deg m(X),$$

从证明的过程中已经得知. ■

结合定理 1.1, 可得

推论 设 $u_1, \dots, u_n$ 是 F 上有限个代数元. 于是, $F(u_1, \dots, u_n)$ 是 F 上的有限扩张. ■

代数扩张具有可传性, 具体如下:

命题 2 若 K 是 F 上的代数扩张, L 是 K 上的代数扩张, 则 L 也是 F 上的代数扩张.

证明 只需证明, L 的任意元素 x , 都是 F 上的代数元. 按所设, 存在 $u_1, \dots, u_m \in K$, 使得等式

$$x^m + u_1 x^{m-1} + \dots + u_m = 0 \quad (1.2.4)$$

成立. 因此, x 是 $F(u_1, \dots, u_m)$ 上的代数元. 由定理 1.2,

$$[F(x; u_1, \dots, u_m):F(u_1, \dots, u_m)] \leq m.$$

由于 $F(u_1, \dots, u_m)$ 是 F 上的有限扩张, 故 $F(x; u_1, \dots, u_m)$ 也是 F 上的有限扩张. 再按定理 1.1 的推论 2, 以及本节的命题 1, 知

$F(x)$ 是 F 上的代数扩张, 换言之, x 是 F 上的代数元. ■

从这个命题, 我们还可以认识一个事实: 在 F 的任一扩域 K 中, 所有关于 F 的代数元所成的集, 形成 K 的一个子域, 而且是 F 在 K 中最大(按包含关系)的代数子扩张. 我们称这个子域为 F 在 K 中的代数闭包.

以上关于代数元和代数扩张的讨论, 是在假定 F 为某个 K 的子域的情形下来进行的. 如果没有事先给出的 K , 如何从 F 作出关于它的代数元, 以及 F 上的代数扩张? 现在我们来讨论这个问题. 按定理 1.2, 只要作出 F 上的代数元, 也就同时得到 F 的一个代数扩张. 根据我们对代数元所下的定义, 不妨把问题改作如下形式: 设 $f(X) \in F[X]$, $\deg f(X) > 1$. 问如何作出一个元素 u (在 F 的某个扩域 K 中), 使得方程 $f(X) = 0$ 以 u 为它的根?

如果 $f(X)$ 在 $F[X]$ 中能分解出一个一次因式, 此时解答至为明显. 因为 F 中的某个元素已能满足要求. 因此, 不妨设 $f(X)$ 在 F 上无一次因式. 令

$$p(X) = c_0 X^r + \cdots + c_r, \quad c_i \in F, \quad c_0 \neq 0 \quad (1.2.5)$$

是 $f(X)$ 在 F 上的一个不可约因式, $r > 1$. 今以 $(p(X))$ 表 $p(X)$ 在 $F[X]$ 中生成的主理想. 由 $p(X)$ 在 F 上的不可约性, $(p(X))$ 是 $F[X]$ 中的极大理想. 因此, 剩余类环 $F[X]/(p(X))$ 成一个域, 记作 K_0 . 今考虑从 $F[X]$ 到 K_0 的自然同态

$$\tau_1: F[X] \rightarrow K_0.$$

τ_1 在 F 上的限制记作 τ , 即

$$\tau: F \rightarrow K_0. \quad (1.2.6)$$

这是由映射

$$a \mapsto a + (p(X)), \quad a \in F$$

所确定的嵌入(单一同态). 因若不然, 则有 $0 \neq a \in F$, 使得

$$\tau(a) = 0 + (p(X)),$$

即 $a \in \ker \tau$. 由此又有 $\ker \tau_1$ 包含 $(a, p(X)) = F[X]$, 矛盾. 现在以 F^τ 记 F 在 K_0 内的象; 又以 $p^\tau(X)$ 记

$$\tau(c_0)X^r + \tau(c_1)X^{r-1} + \cdots + \tau(c_r).$$

这是 F^τ 上的多项式. 若令

$$\tau_1(X) = \alpha \in K_0,$$

则有 $p^\tau(\alpha) = p^\tau(\tau_1(X)) = \tau_1(p(X)) = 0$,

即 α 是 $p^\tau(X) = 0$ 的一个根.

取 S 是一个与 $K_0 \setminus F^\tau$ 有相同的基数, 且与 F 无公有元素的任意元素集; 又令 $K = F \cup S$. 由于 K 与 K_0 有相同的基数, 故可扩大(1.2.6), 使它成为由 K 到 K_0 的一个叠合映射(一一对应), 仍记作 τ . 对于集 K 的元素 x, y , 现在来规定其间的加法与乘法运算如下:

$$\begin{aligned} x + y &= \tau^{-1}(\tau(x) + \tau(y)), \\ xy &= \tau^{-1}(\tau(x)\tau(y)), \end{aligned} \quad (1.2.7)$$

其中右边出现的和与积, 是从 K_0 中运算而得. 由于 τ 是经拓展(1.2.6)而得到, 所以在 $x, y \in F$ 时, (1.2.7)的规定与 F 中原有的运算相一致. 在这样的规定下, K 成一个域, 它是 F 的扩域, 而且 τ 就是 K 与 K_0 间的一个同构. 若令 $u = \tau^{-1}(\alpha)$, 则有 $p(u) = 0$, 换言之, $p(X) = 0$ 在域 K 中有解. 这就证明了

定理 1.3 (Kronecker) 设 F 是一个域; $f(X)$ 是 F 上一个次数 > 1 的多项式. 于是存在 F 的一个扩张 K , 使得方程 $f(X) = 0$ 在 K 中有解. ■

推论 1 设 F 是一个域; $f_1(X), \dots, f_m(X)$ 是 F 上 m 个次数 > 1 的多项式. 于是存在 F 的一个扩张 K , 使得每个

$$f_j(X) = 0 \quad (j = 1, \dots, m)$$

在 K 中都有解. ■

推论 2 若 u_1, u_2 是 F 上两个共轭元, 则 $F(u_1)$ 与 $F(u_2)$ 是 F -同构的.

证明 设 $m(X)$ 是 u_1 与 u_2 在 F 上的极小多项式. 从定理的证明, 可知 $F(u_1)$ 与 $F(u_2)$ 都与 $F[X]/(m(X))$ 成 F -同构, 从而 $F(u_1)$ 与 $F(u_2)$ 成 F -同构. ■

§ 1.3 代数闭域·域的代数闭包

我们称域 Ω 为一代数闭域, 如果对于 Ω 上任何一个多项式 $f(X)$, 方程 $f(X)=0$ 在 Ω 中都有一个解(从而有全部的解). 这个定义又等价于: Ω 除了它本身外, 无其他的代数扩张. 当代数闭域 Ω 是 F 的扩域时, 可称 Ω 为 F 的一个代数闭扩张. 在本节中, 我们所要讨论的课题是: 对于任意的域 F , 是否存在代数的代数闭扩张, 而且具有某种意义下的唯一性. 首先有

定理 1.4 每个域 F , 都至少有一个代数闭扩张.

证明(Artin) 若 F 本身是代数闭域, 结论自然成立. 今设 F 不是代数闭域. 先来作 F 的一个扩张 K_1 , 使得 $F[X]$ 中每个方程 $f(X)=0$ 在 K_1 中都有一个解. 不失一般性, 只需考虑次数 >1 的 $f(X)$. 对于每个这样的 $f(X)$, 令符号 X_f 与它相对应; 又以 S 记由所有这些 X_f 所组成的集. 于是

$$f(X) \mapsto X_f,$$

就是从 $F[X]$ 的全部次数 >1 的多项式所成的集, 到集 S 的一个叠合映射. 作多项式环 $F[S]$, 并且考虑其中由所有多项式 $f(X_f)$ 所生成的理想 I . 首先有 I 不是单位理想. 因若不然, 则存在等式

$$g_1 f_1(X_{f_1}) + g_2 f_2(X_{f_2}) + \cdots + g_r f_r(X_{f_r}) = 1, \quad (1.3.1)$$

其中 $g_i \in F[S]$. 今以 X_i 简记 X_{f_i} ; 又设在多项式 $g_1, \dots, g_r$ 中出现的有限多个符号为 $X_1, \dots, X_d$. 于是(1.3.1)又可写如

$$\sum_{j=1}^n g_j(X_1, \dots, X_n) f_j(X_j) = 1. \quad (1.3.2)$$

按定理 1.3 的推论 1, 在 F 的某个扩域 K 中, 每个 $f_j(X_j) = 0$ 都有解. 若以 K 中这些元素代入 X_j , 由 (1.3.2) 就给出等式 $0 = 1$, 矛盾.

由于 $F[S]$ 是有单位元素的交换环, 因此存在包含 I 的极大理想, 令 M 是其中之一. 此时 $F[S]/M$ 成一个域. 使用在定理 1.3 的证明中所用的论证, 就得到 F 的一个扩张 K_1 , 使得 $F[X]$ 中每个方程 $f(X) = 0$, 在 K_1 内都有解.

然后对域 K_1 作同样的考虑, 以得出它的一个扩张 K_2 , 使得 K_1 上的每个方程在其中都有解.

继续以上的论证, 就得到一个由域所组成的递增列

$$F \subseteq K_1 \subseteq K_2 \subseteq \dots, \quad (1.3.3)$$

使得 $K_n[X]$ 中的每个方程在 K_{n+1} 中都有解. 现在令

$$\Omega = \bigcup_{n=1}^{\infty} K_n. \quad (1.3.4)$$

容易验知, Ω 是一个域. $\Omega[X]$ 中每个次数 > 1 的方程 $f(X) = 0$, 其系数必属于某个 K_n . 因此, $f(X) = 0$ 在 K_{n+1} 中有解, 从而也在 Ω 中有解. 这证明了 Ω 是个代数闭域. ■

定理 1.5 每个域 F , 都至少有一个代数的代数闭扩张.

证明 从定理 1.4, 知存在 F 上的代数闭扩张 Ω . 令 $\hat{F}$ 是 F 在 Ω 中的代数闭包. 今证明 $\hat{F}$ 本身也是一个代数闭域. 设 $f(X)$ 是 $\hat{F}$ 上一个次数 > 1 的多项式. 作为 Ω 上的多项式而论, 必有某个 $u \in \Omega$, 使得 $f(u) = 0$. 这个 u 是 $\hat{F}$ 上的代数元, 从而也是 F 上的代数元. 因此 $u \in \hat{F}$, 即 $\hat{F}$ 是个代数闭域. ■

对于任意域, 现在已经获得了至少一个代数的代数闭扩张. 进一步要讨论的, 就是唯一性的问题. 为此, 先有一个一般性的命

题:

命题 1 设 τ 是从域 F 到域 Ω 的一个嵌入; 又设 u 是 F 上的一个代数元, $m(X)$ 是它在 F 上的极小多项式. τ 能拓展成 $F(u)$ 到 Ω 的嵌入, 当且仅当 $m^\tau(X) = 0$ 在 Ω 中有解, 此处 $m^\tau(X) \in \Omega[X]$ 是 $m(X)$ 的象. 此外, τ 在 $F(u)$ 上拓展的个数不超过 $\deg m(X)$.

证明 必要性显然. 今证其充分性. 设

$$\deg m(X) = n > 1,$$

此时

$$\deg m^\tau(X) = n.$$

按定理 1.2, $F(u)$ 中元素都可以表如

$$\alpha = c_0 + c_1 u + \cdots + c_{n-1} u^{n-1}, \quad c_j \in F. \quad (1.3.5)$$

设 γ 是 $m^\tau(X) = 0$ 在 Ω 中的一个解. 我们令

$$\tau_1(\alpha) = \tau(c_0) + \tau(c_1)\gamma + \cdots + \tau(c_{n-1})\gamma^{n-1}. \quad (1.3.6)$$

作为映射而论, τ_1 自然是 τ 的一个拓展, 而且 (1.3.6) 给出 $F(u)$ 到 Ω 内的一个单一映射. 要证明它又是一个嵌入, 只需对加法与乘法进行验证. 今仅就乘法来验证. 设 $g(u)h(u) = r(u)$. 从 $F(u)$ 中的运算法则, 知有

$$g(X)h(X) = q(X)m(X) + r(X).$$

从而得到

$$g^\tau(X)h^\tau(X) = q^\tau(X)m^\tau(X) + r^\tau(X).$$

再以 $\gamma = \tau_1(u)$ 代入, 即得

$$g^{\tau_1}(\gamma)h^{\tau_1}(\gamma) = r^{\tau_1}(\gamma).$$

这证明了 τ 拓展成为嵌入 $\tau_1: F(u) \rightarrow \Omega$. 至于结论的最后部分, 从论证过程即知. ■

结合定理 1.1 的推论 1, 可得

推论 1 设 K/F 是一个有限扩张, $[K:F] = n$. 若 τ 是 F 到某个域 Ω 内的嵌入, 则 τ 至多只能拓展成 n 个 K 到 Ω 的嵌