高等学校教学用书

邦钢新 编著

域论基础

北京师范大学出版社

高等学校教学用书

域论基础

郝钢新　编著

北京师范大学出版社

高等学校教学用书

域论基础

郝炳新 编著

北京师范大学出版社出版
新华书店北京发行所发行
北京师范大学印刷厂印刷

开本：850×1168 1/32 印张：7.5 字数：183千
1988年2月第1版 1988年2月第1次印刷
印数：1—3 000

ISBN7-303-00244-8/O·56
定价：1.60元

内 容 简 介

本书是作者在几所大学授课时所使用讲义的基础上，经多次修改和补充而成。全书共分五章：第一章域的扩张，第二章代数扩张，第三章 Galois理论，第四章超越扩张，第五章整扩张。作者在题材的选择和安排上，着眼于域的基本理论和基本方法以及对于其他学科应用较多的内容，给只具有高等代数及抽象代数初步知识的读者提供了一本系统地学习域论基础的书。

本书可做大学数学系学生的教材或教参。

序

域是代数学中最基本的概念之一，历史悠久。早在十九世纪初叶，在 Galois 研究方程的著作中就有了域的概念的萌芽，虽然那时还没有域的抽象定义．1910年，Ernst Steinitz的论文《体的代数理论》，(Algebraische Theorie der Körper, J.reine und angew. Math. 137 (1910))问世．在这篇论文里，第一次对于域的理论作了全面、系统的阐述，奠定了域论的基础．时至今日，域论不仅本身是代数学中一个内容丰富的重要分支，而且也是学习其它一些分支，如代数数论，代数几何，环论，代数群等所不可缺少的基础知识，此外，有限域在近代的编码和计算机理论中都有着应用．

这本书最初是作者于1982年春应云南大学数学系之邀，在该系讲授域论时所编写的讲义，以后又经过多次修改和补充．共包括五章．第一章介绍域扩张及有关的一些最基本的概念，这是研究域的基本思想；第二章介绍代数扩张，其中对于可分性的问题作了较细致的讨论；第三章介绍 Galois 理论；第四章介绍超越扩张，包括超越基及超越次数，可分性，导子等；第五章介绍整扩张，包括环的整扩张，局部化及Hilbert零点定理等，这是交换代数的最基本的内容，有着广泛的应用．作者的意图是向只具有高等代数及抽象代数初步知识的读者提供一本系统地介绍域论基础的书．在题材的选择和安排上，着眼于域的基本理论和基本方法以及对于其它学科应用较多的内容，并不追求全面和完备，因此，对于有些本来应该属于域论的题材，如有序域，赋值等，就没有包括进去．

首先要感谢云南大学数学系的一些同事，正是由于他们的盛情邀请，才使作者想到要编写一本有关域方面的书。在编写过程中，我的许多同事曾给予不少帮助。特别是蒋滋梅同志，她不仅仔细地阅读了原稿，而且还用原稿作为讲义，在本校及外校讲授了数次，提出了很多宝贵的意见。谨在这里表示感谢。

希望读者批评指正。

郝钢新

1985年12月于

北京师范大学数学系

目　录

第一章　域的扩张

1.1　子域和扩域　添加

读者都已熟悉域的定义。一个域是一个至少有两个元素的集 F，在其中定义了两个代数运算，分别叫做加法和乘法；F 对于加法来说作成一个 Abel 群，F 的全体非零元素对于乘法来说作成一个 Abel 群，并且加法与乘法被分配律联系着。

设 F 是域 K 的一个子集。如果对于 K 的加法和乘法来说，F 本身也作成一个域，就称 F 是 K 的一个**子域**，而 K 是 F 的一个**扩域**，以后我们常常用符号 K/F 表示 K 是 F 的扩域，并且称为一个**域扩张**。

设 K/F 是一个域扩张。如果 E 是 K 的一个子域，同时又是 F 的一个扩域，就称 E 是域扩张 K/F 的一个中间域。

设 F 是域 K 的一个子域。T 是 K 的一个子集。令 $\{E_\alpha\}_{\alpha\in I}$（$I$ 是一个指标集）是域扩张 K/F 中包含 T 的中间域的全体。显然，$K\in\{E_\alpha\}_{\alpha\in I}$，所以 $\{E_\alpha\}_{\alpha\in I}\neq\varnothing$。令 $E=\bigcap_{\alpha\in I}E_\alpha$。那么 E 是 K/F 的一个中间域。它是 K 中包含 F 和 T 的最小子域，记作 $F(T)$。称为添加 T 于 F 所得的扩域，或称为 T 在 F 上所生成的域。

当 $T=\{t_1,\cdots,t_n\}$ 是 K 的一个有限子集时，我们把 $F(T)$ 记作 $F(t_1,\cdots,t_n)$。这时就说 $F(t_1,\cdots,t_n)$ 是在 F 上**有限生成的**。特别，添加单独一个元素 t 于 F 所得的扩域 $F(t)$ 叫做 F 的一个**单扩域**。

定理 1.1.1　设 F 是域 K 的一个子域，T，T_1，T_2 都是 K

的子集。

(i) $F(T_1 \cup T_2) = F(T_1)(T_2)$

(ii) 令$\{S_\alpha\}_{\alpha \in I}$是$T$的一切有限子集所成的子集族。那么

$$F(T) = \bigcup_{\alpha \in I} F(S_\alpha)$$

(iii) 设$T = \{t_1, \cdots, t_n\}$是有限集。那么

$$F(T) = \left\{ \frac{f(t_1, \cdots, t_n)}{g(t_1, \cdots, t_n)} \;\middle|\; f, g \in F[X_1, \cdots, X_n], \right.$$
$$\left. g(t_1, \cdots, t_n) \neq 0 \right\}.$$

这里$F[X_1, \cdots, X_n]$是F上不相关不定元$X_1, \cdots, X_n$的多项式环。

证 (i) $F \subseteq F(T_1)(T_2)$，$T_1 \cup T_2 \subseteq F(T_1)(T_2)$，而$F(T_1 \cup T_2)$是$K$的既包含$F$又包含$T_1 \cup T_2$的最小子域，所以

$$F(T_1 \cup T_2) \subseteq F(T_1)(T_2).$$

反过来，$F(T_1)$是$F(T_1 \cup T_2)$的子域，又$T_2 \subseteq F(T_1 \cup T_2)$。因为$F(T_1)(T_2)$是$K$的既包含$F(T_1)$又包含$T_2$的最小子域，所以

$$F(T_1)(T_2) \subseteq F(T_1 \cup T_2).$$

(ii) 由定义，对于每一个$\alpha \in I$，$F(S_\alpha) \subseteq F(T)$，从而$\bigcup_{\alpha \in I} F(S_\alpha) \subseteq F(T)$。

令$L = \bigcup_{\alpha \in I} F(S_\alpha)$。$L$是$K$的一个子域。事实上，设$u, v \in L$，那么存在$T$的有限子集$S_1$和$S_2$，使得$u \in F(S_1)$，$v \in F(S_2)$。令$S = S_1 \cup S_2$，则$S$也是$T$的有限子集，并且$u, v \in F(S)$。由于$F(S)$是子域，所以$u+v$，$u-v$，$uv$，$uv^{-1}$（若$v \neq 0$）都属于$F(S) \subseteq L$。这就证明了$L$是$K$的子域。

现在设$t \in T$，那么$t \in F(t) \subseteq L$。因此$T \subseteq L$又$F \subseteq L$。所以$F(T) \subseteq L$。这样，

$$L = \bigcup_{\alpha \in I} F(S_\alpha) = F(T).$$

(iii) F的元素与 $t_1, \cdots, t_n$ 经过加、减、乘、除运算的结果都可以表示成以下形状

$$\frac{f(t_1, \cdots, t_n)}{g(t_1, \cdots, t_n)}, \quad g(t_1, \cdots, t_n) \neq 0, \tag{1}$$

这里$f, g \in F[X_1, \cdots, X_n]$。这样的元素都属于 $F(t_1, \cdots, t_n)$。另一方面，K中一切形如(1)的元素已经作成一个既包含 F 又包含$t_1, \cdots, t_n$的子域。这就证明了(iii)成立。 ∎

域F的扩域K可以看成 F 上一个向量空间。如果K在F上的维数是有限的，那么就称K是F的一个有限次扩域或者称K/F是一个有限次扩域。如果K是F上无限维的向量空间，就称K是F的一个无限次扩域，相应地，称K/F是一个无限次扩张。作为向量空间，K在F上的维数叫做K在F上的**次数**，记作$[K : F]$，向量空间K在F上的基也称为域K在F上的**基**。

定理 1.1.2 设E是域扩张K/F的一个中间域。$\{u_\alpha\}_{\alpha \in I}$是$E$在$F$上的一个基而$\{v_\beta\}_{\beta \in J}$是$K$在$E$上的一个基。那么$\{u_\alpha v_\beta\}_{\alpha \in I, \beta \in J}$是$K$在$F$上的一个基。

证 首先$\{u_\alpha v_\beta\}_{\alpha \in I, \beta \in J}$里任意有限个元素$\{u_i v_j\}_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n}$在$F$上线性无关。事实上，如果有$a_{ij} \in F$，$1 \leqslant i \leqslant m$，$1 \leqslant j \leqslant n$．使得

$$\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} u_i v_j = 0,$$

则

$$\sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_{ij} u_i \right) v_j = 0.$$

$\sum_{i=1}^{m} a_{ij} u_i \in E$，$1 \leqslant j \leqslant n$，而$v_1, \cdots, v_n$在$E$上线性无关，所以

$$\sum_{i=1}^{m} a_{ij}u_i = 0, \quad 1 \leqslant j \leqslant n.$$

又因为$u_1, \cdots, u_m$在F上线性无关，所以$a_{ij} = 0$，$1 \leqslant i \leqslant m$，$1 \leqslant j \leqslant n$。

其次，设$u \in K$，那么u可以由$\{u_\beta\}_{\beta \in J}$中有限个元素$v_1, \cdots, v_n$线性表示，系数属于$E$：

$$u = \sum_{j=1}^{n} b_j v_j, b_j \in E \ (1 \leqslant j \leqslant n).$$

每一个b_j又可以表成$\{u_\alpha\}_{\alpha \in I}$中有限元素的$F$-线性组合。因此存在$u_1, \cdots, u_m \in \{u_\alpha\}_{\alpha \in I}$，使得

$$b_j = \sum_{i=1}^{m} a_{ij}u_i, a_{ij} \in F (1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n).$$

于是

$$u = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij}u_i v_j.$$

所以u可以表成$\{u_\alpha v_\beta\}_{\alpha \in I, \beta \in J}$中有限个元素的$F$-线性组合。这就证明了$\{u_\alpha v_\beta\}_{\alpha \in I, \beta \in J}$是$K$在$F$上的一个基。 ∎

由这个定理，我们立即得到以下

推论 1.1.3 设K/F是一个有限次域扩张，而

$$E_1 \subseteq E_2 \subseteq \cdots \subseteq E_s$$

都是K/F的中间域。那么

$$[K : F] = [K : E_s][E_s : E_{s-1}] \cdots [E_1 : F]. \quad ∎$$

1.2 素域

如果一个域没有真子域，就称为一个**素域**。

有理数域$\mathbf{Q}$显然是一个素域。设$\mathbf{Z}$是整数环，p是一个素数。令

$$(p) = \{pn \mid n \in Z\}$$

是 p 所生成的 $\mathbf{Z}$ 的理想. 我们知道，以 p 为模的剩余类环 $\mathbf{Z}/(p)$ 是一个域并且也是素域.

下面的定理对素域作了完全的描述.

定理 1.2.1 令 F 是一个素域. 那么 F 或者与有理数域 $\mathbf{Q}$ 同构，或者与以某一个素数 p 为模的剩余类环同构.

证 令 1 是素域 F 的单位元，映射

$$\varphi: \mathbf{Z} \to F, \quad n \to n \cdot 1$$

是一个环同态. 令 $\mathfrak{p} = \ker\varphi$ 是 φ 的核. 则 $\mathfrak{p}$ 是 $\mathbf{Z}$ 的一个理想，且

$$\mathbf{Z}/\mathfrak{p} \cong \varphi(\mathbf{Z}) \subseteq F.$$

因为 $\varphi(1) \neq 0$，所以 $\mathfrak{p} \neq \mathbf{Z}$. 由于 $\varphi(\mathbf{Z})$ 是整环，而 $\mathbf{Z}$ 是主理想环，因此，或者 $\mathfrak{p} = (0)$，或者 $\mathfrak{p} = (p)$，这里 (p) 是由某一个素数 p 所生成的 Z 的理想.

如果 $\mathfrak{p} = (0)$，那么 φ 是单射，并且可以开拓为 $\mathbf{Z}$ 的商域 $\mathbf{Q}$ 到 F 的单射，$\varphi(\mathbf{Q})$ 是 F 的子域. 因为 F 是素域，所以 $\varphi(\mathbf{Q}) = F$. 这样，$\mathbf{Q} \cong F$.

如果 $\mathfrak{p} = (p)$，那么 $\mathbf{Z}/\mathfrak{p} = \mathbf{Z}/(p)$ 是域，从而 $\varphi(\mathbf{Z})$ 是 F 的子域. 因为 F 是素域，所以 $\varphi(\mathbf{Z}) = F$，这样就得到 $\mathbf{Z}/(p) \cong F$. ∎

设 F 是任意一个域. F 的一切子域的交 F_0 仍是 F 的一个子域. F_0 显然是 F 的最小子域，所以 F_0 是一个素域，称为域 F 的素域. 由 1.2.1 知，或者 $F_0 \cong \mathbf{Q}$，或者 $F_0 \cong \mathbf{Z}/(p)$，p 是一个素数. 在前一情形，就说 F **具有特征零**；在后一情形，就说 F **具有特征** p. 我们把域 F 的特征记作 $\mathrm{char}\ F$. 下面两个定理是比较显易的，我们把它们的证明留给读者去作.

定理 1.2.2 设 F 是一个域.

(i) 如果 $\mathrm{char}\ F = 0$，那么对于 $n \in \mathbf{Z}$，$x \in F$，

$$nx = 0 \Longleftrightarrow x = 0 \text{ 或 } n = 0.$$

(ii) 如果 $\mathrm{char}\ F = p > 0$，那么对于 $n \in \mathbf{Z}$，$x \in F$，

$$nx = 0 \Longleftrightarrow x = 0 \text{ 或 } n \equiv 0 \pmod{p}.$$ ∎

定理 1.2.3 设F是一个域，$\mathrm{char}F=p>0$．那么对于任意$x,y\in F$和任意非负整数n，

(i) $(x\pm y)^{p^n}=x^{p^n}+y^{p^n}$；

(ii) 映射$\varphi: x\longmapsto x^{p^n}$是$F$到自身内的同态单射． ∎

1.3 单扩域

设F是一个域，添加一个元素α于F所得的扩域$F(\alpha)$叫做F的一个**单扩域**。

单扩域的结构和所添加的元素α的性质有着密切的关系，先引入以下的概念。

设R是一个有单位元1的交换环，F是R的一个子域且F含有R的单位元。R的一个元素α称为**关于F是代数的**或者说α是F上一个**代数元**，如果存在F上一个非零多项式$f(X)$，使得$f(\alpha)=0$，如果α不是F上的代数元，就称α**关于F是超越的**或者说α是F上一个**超越元**。

设K是R的一个子域，且$F\subseteq K$．如果$\alpha\in R$关于F是代数的，那么显然α关于K也是代数的．一个等价的提法是，如果α关于K是超越的，那么α关于F也是超越的。

单扩域的结构由下面的定理完全决定。

定理 1.3.1 设$K=F(\alpha)$是域F的一个单扩域。

(i) 如果α关于F是超越的，那么K与F上不定元X的有理分式域$F(X)$同构。

(ii) 如果α关于F是代数的，那么存在F上一个最高次项系数是1的不可约多项式$p(X)$．而K与剩余类环$F[X]/(p(X))$同构，这里$(p(X))$表示由多项式$p(X)$所生的$F[X]$的理想；这个多项式$p(X)$由α唯一确定。

证 对于每一个$f(X)\in F[X]$，令$f(\alpha)\in K$与它对应，这

样就定义了一个环同态φ：$F[X]\to K$，并且φ保持F的元素不动。$\varphi(F[X])=F[\alpha]$是K的一个子整环。令

$$\mathfrak{p}=\mathrm{Ker}\varphi=\{f(X)\mid f(X)\in F[X],\ f(\alpha)=0\}.$$

$\mathfrak{p}$是环$F[X]$的一个理想。

（i） 如果α关于F是超越的，那么不存在非零多项式$f(X)\in F[X]$使$f(\alpha)=0$，从而$\mathfrak{p}=(0)$。所以φ是$F[X]$到$F[\alpha]$的同构映射，这个映射可以开拓为有理分式域$F(X)$到整环$F[\alpha]$的商域$F(\alpha)$的同构映射，仍以φ表示：

$$\varphi:\frac{f(X)}{g(X)}\longmapsto\frac{f(\alpha)}{g(\alpha)}.$$

这样，φ是$F(X)$到K同构映射，且$\varphi(X)=\alpha$。

(ii) 设α关于F是代数的，那么存在$F[X]$的非零多项式$f(X)$，使得$f(\alpha)=0$，所以$\mathfrak{p}\neq(0)$。由于$F[X]$是欧氏环，所以$\mathfrak{p}$由一个多项式$p(X)\neq 0$生成：$\mathfrak{p}=(p(X))$，$p(X)$是使$p(\alpha)=0$的非零多项式中次数最低的一个。不妨设$p(X)$的最高次项系数等于1，于是$p(X)$由α唯一确定，并且容易看出，$p(X)$是不可约的。于是$\mathfrak{p}=(p(X))$是$F[X]$的一个极大理想，从而剩余类环$F[X]/\mathfrak{p}$是一个域，于是就有

$$F[X]/\mathfrak{p}\cong\varphi(F[X])=F[\alpha]\subseteq K.$$

因此$F[\alpha]$也是域，然而$K=F(\alpha)$是含有F及α的最小域，所以

$$F(\alpha)=F[\alpha],\ \text{即}$$

$$F[X]/\mathfrak{p}\cong K.$$ ∎

定理 1.3.1 完全给出了一个域F的单扩域$F(\alpha)$的结构，当α是F上的代数元时，我们还可以说得更具体一些。首先，由1.3.1，当α是F上代数元时，存在唯一的最高次项系数是1的不可约多项式$p(X)\in F[X]$，使得$p(\alpha)=0$。我们把这个由α所唯一确定的多项式$p(X)$叫做α在F上的**最小多项式**。我们有

定理 1.3.2 设α是域F上一个代数元，$p(X)\in F[X]$是α在F上的最小多项式，设$\deg\ p(X)=n$。

（i） 元素$1,\alpha,\cdots,\alpha^{n-1}$构成$F(\alpha)$在$F$上的一个基，从而$F(\alpha)$的每一元素$\xi$可以唯一地表示成

$$\xi=a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1},\ a_i\in F(0\leqslant i\leqslant n-1),$$

的形式。$[F(\alpha):F]=\deg\ p(X)$。

(ii) 设 $\xi=\sum_{i=0}^{n-1}a_i\alpha^i$，$\eta=\sum_{i=0}^{n-1}b_i\alpha^i\in F(\alpha)$，那么

$$\xi+\eta=\sum_{i=0}^{n-1}(a_i+b_i)\alpha^i$$

(iii) 令 $f(X)=\sum_{i=0}^{n-1}a_iX^i$，$g(X)=\sum_{i=0}^{n-1}b_iX^i$ 而

$$r(X)=c_0+c_1X+\cdots+c_{n-1}X^{n-1}$$

是以$p(X)$除$f(X)g(X)$所得的余式，则

$$\xi\eta=\sum_{i=1}^{n-1}c_i\alpha^i.$$

证 由1.3.1，对于$K=F(\alpha)=F[\alpha]$的任意元素，存在$f(X)\in F[X]$，使得$\xi=f(\alpha)$。设

$$f(X)=p(X)q(X)+r(X),$$

这里或者$r(X)=0$，或者$\deg r(X)<n$，那么

$$\xi=f(\alpha)=r(\alpha).$$

因此

$$\xi=a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1},\ a_i\in F(0\leqslant i\leqslant n-1).$$

这个表示法是唯一的，因为如果

$$\xi=\sum_{i=0}^{n-1}a_i\alpha^i=\sum_{i=0}^{n-1}a_i'\alpha^i,\ a_i,a_i'\in F,$$

那么令$g(X)=\sum_{i=0}^{n-1}(a_i-a_i')X^i\in F[X]$，则$g(\alpha)=0$，所以$p(X)$整除$g(X)$，从而必须$g(X)=0$，这样就证明了，$1,\alpha,\cdots,\alpha^{n-1}$是

$F(\alpha)$ 在 F 上的一个基，从而$[F(\alpha):F]=n$。至于论断 (ii) 和 (iii)是显然的。 ∎

由以上两个定理立即得到

推论1.3.3 设$K=F(\alpha)$是域F的一个单扩域。K是F上有限次扩域必要且只要α关于F是代数的。 ∎

因为域F上不定元是存在的，所以由 1.3.1 (i)可知，域F上添加一个超越元的单扩域是存在的。下面的定理表明，域F上添加一个代数元的单扩也是存在的。

定理 1.3.4 设$p(X)\in F[X]$是域F上不定元X的一个不可约多项式。那么存在F的一个扩域K，使得 $p(X)$ 在K内有一个根α，并且$K=F(\alpha)$。

证 令 $\mathfrak{p}=(p(X))$是$p(X)$所生成的$F[X]$理想。由于$p(X)$不可约，所以 $\mathfrak{p}$ 是一个极大理想。令$K=F[X]/\mathfrak{p}$，则K是一个域。因为$F\cap\mathfrak{p}=\{0\}$，所以自然同态$\varphi:F[X]\to K$将F单一地映入K，从而可以将$\varphi(F)$与F等同，而将F看成K的一个子域。令$\alpha=\varphi(X)\in K$，对于任意$g(X)\in F[X]$，我们有

$$\varphi(g(X))=g(\varphi(X))=g(\alpha).$$

所以$K=\varphi(F[X])=\{g(\alpha)\mid g(X)\in F[X]\}=F[\alpha]$，然而$K$是域，所以$K=F[\alpha]=F(\alpha)$。 ∎

习　题

1. 设K是域F的一个有限次扩域，证明：

(i) $[K:F]=1\Longleftrightarrow K=F$；

(ii) 如果$[K:F]=p$是一个素数，则在F与K之间没有不等于F或K的中间域；

(iii) 如果$\alpha\in K$是F上一个n次代数元，则$n\mid[K:F]$。

2. 设$K=Q(\sqrt{2},\sqrt{3})$。求出$[K:Q]$，并且给出K在Q上一个基。