普通高等教育“十三五”规划教材
大学本科数学类专业基础课程系列丛书

抽象代数基础（下册）

——域扩张与Galois理论导引

郭聿琦　高　兴　冯爱芳　编著

科学出版社

普通高等教育“十三五”规划教材

大学本科数学类专业基础课程系列丛书

抽象代数基础

(下 册)

——域扩张与 Galois 理论导引

郭聿琦　高　兴　冯爱芳　编著

科 学 出 版 社

北 京

内 容 简 介

本教材分上、下两册，上册由前六章构成，依次为集合论的基本概念、抽象代数的基本概念、Green 关系与正则半群、群(特别地，有限群)、环与理想,模与线性空间；下册由后两章构成，依次为域与域的扩张，Galois 理论导引. 本书为下册. 本教材的内容涵盖数学类专业本科生 (特别地，各类数学人才班)的两门代数课程，上册的前五章或前六章 (特别是未加*的部分)可用作数学类各专业必修基础课程抽象代数的教材或参考资料；下册的后两章可用于后续选修课程域论与 Galois 理论的教材或参考资料.

本书可供高等院校数学类各专业师生以及有关数学工作者使用.

图书在版编目(CIP)数据

抽象代数基础：全 2 册/郭聿琦等编著. —北京：科学出版社, 2019.3
(大学本科数学类专业基础课程系列丛书)
普通高等教育“十三五”规划教材
ISBN 978-7-03-060752-2

Ⅰ. ①抽… Ⅱ. ①郭… Ⅲ. ①抽象代数-高等学校-教材 Ⅳ. ①O153

中国版本图书馆 CIP 数据核字(2019) 第 043100 号

责任编辑：胡海霞 / 责任校对：杨聪敏
责任印制：张 伟 / 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

北京建宏印刷有限公司 印刷
科学出版社发行 各地新华书店经销
*
2019 年 3 月第 一 版 开本：787 × 1092 1/16
2019 年 3 月第一次印刷 印张：17 3/4
字数：346 000

定价：59.00 元(全 2 册)
(如有印装质量问题，我社负责调换)

前　言

“抽象代数”(也称为“近世代数”) 是数学类专业本科生的必修基础课程之一, 通常, 相对于所谓“老三高” (“高等代数”、“数学分析”和“解析几何”), 它与“实变函数”和“微分几何”也合称为“新三高”.

本教材涵盖两门课程的内容, 上册 (特别是未加 $*$ 的章节) 构成本科必修基础课程“抽象代数” (72 学时) 的基本内容; 下册构成后续选修课程“域论与 Galois 理论” (54 学时) 的基本内容.

鉴于数学的高度抽象性和严格逻辑性在“抽象代数”课程上体现得尤为明显, 这门课程的教与学, 需要学生具有一定的数学能力 (这种能力只能通过若干大学数学课程的学习, 在知识的积累过程中形成). 因此, 这门课程置于本科生入学后一年半左右开设较为合适, 尽管原则上它可以开设得更早.

本教材有以下五个处理特色.

(1) 在第 2 章 (抽象代数的基本概念) 里, 关于抽象概念的引进, 我们除了考虑到学生经过前一年半的知识积累过程中已形成的数学能力之外, 也在遵循由已知到未知 (当然还有, 由具体到抽象, 由特殊到一般等) 的认知规律, 还充分使用着学生在这一知识积累过程中获得的若干新的已知. 具体地说, 关于抽象概念的引进, 我们是对“高等代数”内容的“温故知新”入手的, 即在“高等代数”中, 将要介绍的所有抽象代数系统的有关概念 (包括其上的同态、同余和各类子系统, 以及某系统到另一系统 (集合) 上的作用等) 的特殊情形都已出现过.

(2) 我们的这一教材的“教材处理”, 还秉承着“与时俱进”, 即“现代化”, 或曰“更新”的原则, 这一“更新”中也包括某些适当的、必要的和可能的“增新”. 除了术语和符号的与现代数学文献接轨的使用, 本教材还有如下“增新”.

在第 2 章之后的关于各类代数系统的分章讨论中, 相对于国内外本科“抽象代数”的现状, 我们增加了一个新的内容, 即“Green 关系与正则半群” (第 3 章), 用于讨论半群代数理论的某些基本概念, 某些研究课题, 以及某些典型的研究方法. 这一“增新”的理由有二:

其一, “半群代数理论”形成为代数学的一个独立的分支学科已达半个多世纪之久. 从 Green 关系出发形成的半群研究上的 Green 方法, 以及半群作为一类典型的泛代数的同余理论, 使得半群与群的关系很像环与域的关系, 半群理论与群论已经无交了. “半群代数理论”在面向理论计算机科学、信息科学和财经金融领域的“抽象代数”教材里占有很大的篇幅; 但在数学类专业的“抽象代数”教材里, 却始终未见实质性的涉及.

其二, 半群的基本概念和基本方法的介绍, 也有助于在其他各章对群、环等 (它们是最经典的代数系统) 概念的内涵和外延进行较深入的挖掘和把握, 从而让学生认识到对概念、事实 (它们是概念的内涵) 和方法 (它们提供揭示概念内涵和外延的有效步骤) 的较深入的挖掘和把握并非易事, 而且学会这种挖掘和把握, 是健全创新性思维的重要途径.

(3) 整部书稿, 从理论开发路线的设置、概念的整合、事实的陈述到证明的方法和案例

的构造, 都实现了诸多更新. 这里既有我们收集到的, 也有我们自己的学术性教学研究成果.

(4) 关于各种类型的代数系统的讨论, 都通过围绕基本概念, 选择适当课题, 使用行之有效的方法, 开发出一小套理论, 以便让学生体会到理论建立的过程, 也体会到方法的重要性.

(5) 鉴于该教材中, 仅其上册供必修课“抽象代数”课程使用, 我们在其若干部位, 也都设置了许多小的具体问题, 尽管依靠概念就可以读懂它们, 但只有懂得某一套理论才能去解决某个问题, 从而让学生体会到抽象和严格的理论的必要和威力.

“教材撰著”和“课堂讲授”的基本问题都是“教材处理”, 这应该是共识了. 但是, “教材处理”应遵循的原则和具体的处理实践, 就仁者见仁, 智者见智了. 读者从教材中, 可见我们的观点和实践之一斑. 除却前面提到的, 我们还认为, 教材的语言固然严禁艰涩, 也切忌所谓“通俗易懂, 便于自学” (这不利于学生学会读“书”). 欢迎批评指正.

使用本教材的三点说明:

郭聿琦教授部分讲课视频 (下册)

(1) 未加星号章节的内容, 原则上不依赖于加星号章节的任何内容.

(2) 4.1 节的三个定理的证明用到了未加星号的 3.1 节和未加星号的 3.2 节的前半节; 但是, 我们也在作为附录的 4.4 节中, 给出了这三个定理的不依赖于整个第 3 章的初等证明.

(3) 本书附有郭聿琦教授关于抽象代数的部分讲课视频, 观看请扫描左边二维码.

感谢 “教育部基础学科拔尖学生培养试验计划” 的研究课题“拔尖学生知识积累过程中的能力培养” (编号: 20180706) 基金的资助.

该教材的撰著得到兰州大学教务处、兰州大学萃英学院 (国家“基础学科拔尖学生培养试验计划”的兰州大学执行单位) 和兰州大学数学与统计学院的大力支持, 特别地, 得到了教务处“兰州大学教材建设基金”的资助和萃英学院“出版基金”的资助, 我们在此表示由衷的感谢.

本书是“大学本科数学类专业基础课程系列丛书”中的一本, 在这套丛书中, 我们承担撰写的涵盖四门代数学课程内容的三部教材 (另两部此前已出版) 的责任编辑都是科学出版社的胡海霞编辑, 我们在此也对她认真负责的辛勤工作表示衷心的感谢.

中国科学院李宝研究员、西安建筑科技大学任学明教授、西北大学赵宪钟教授、曲阜师范大学郑恒武教授和西南大学王正攀教授阅读了本教材第五稿的全部或部分章节, 提出了若干中肯的修改建议; 博士生刘祖华、冷静、刘海艳、梁星亮、冯辛阳也承担了某些课程的助教工作和部分书稿的打印, 硕士生皇甫振国、高梦、童俊、王楠和徐子棋也各参加了一届抽象代数或域论与 Galois 理论课程的助教工作, 他们关于本书的前几稿的修订做了不少具体工作. 在此也一并向他们表达我们诚挚的感谢.

郭聿琦

(兰州大学, 西南大学)

2018 年 9 月

此为试读, 需要完整PDF请访问: www.ertongbook.com

目　录

第 7 章　域与域的扩张

7.1　基 本 概 念

7.1.1　域及其特征, 素域

从已知的某些概念和事实的回顾开始.

定义 7.1.1　域是满足下面两个性质的环 $\mathbb{F} \overset{\mathrm{d}}{=} (\mathbb{F}; +, \cdot)$:

(1) $|\mathbb{F}| \geqslant 2$;

(2) $(\mathbb{F} \setminus \{0\}, \cdot)$ 为一 Abel 群.

注 7.1.1　(1) 令 $\mathbb{F}$ 为一域, $a, b \in \mathbb{F}$. 则 $a+b=c$ 时, 称 c 为 a 与 b 的和; $a-b \overset{\mathrm{d}}{=} a+(-b)=c$ 时, 称 c 为 a 与 b 的差; $a \cdot b=c$ 时, 称 c 为 a 与 b 的积; $b \neq 0$, $a/b \overset{\mathrm{d}}{=} a \cdot b^{-1}=c$ 时, 称 c 为 a 与 b 的商.

(2) 在域的定义中的条件 (2) 下, (1) 中的 $|\mathbb{F}| \geqslant 2$ 等价于 $\mathbb{F}$ 为一幺环.

(3) 关于域, 除了读者熟悉的数域, 我们在上册第 5 章 (环与理想) 里已经看到, 从某些类型的环可以构造出某些类型的域, 诸如, ① 令 R 为一交换的幺环 (特别地, 整环), $I \trianglelefteq R$. 则 R/I 为一域当且仅当 I 为 R 的一个极大理想; 而且由 R 构造出的这样的域一定存在. ② 令 R 为一交换的无零因子环 (特别地, 整环). 则类似于由整数环构造出有理数域, 可由 R 构造出一个域 $\mathbb{F}$, 使得 $R \leqslant \mathbb{F}$, 且

$$\mathbb{F} = \{ab^{-1} | a, b \in R, b \neq 0\}.$$

$\mathbb{F}$ 显然是包含 R 的最小的域, 称其为 $\mathbb{F}$ 的分式域.

(4) 令 $\mathbb{F}$ 为一域, $f(x) \in \mathbb{F}[x]$, $\partial(f(x)) = n \in \mathbb{Z}^+$. 则 $f(x)$ 在 $\mathbb{F}$ 中至多有 n 个根 (重数计算在内). 下面我们会看到, 关于 $f(x)$, 存在一个域 $\mathbb{G}_{f(x)}$, 使得 $\mathbb{F} \leqslant \mathbb{G}_{f(x)}$, 且 $f(x)$ 在 $\mathbb{G}_{f(x)}$ 中恰有 n(次数) 个根.

定义 7.1.2　令 $\mathbb{F} \overset{\mathrm{d}}{=} (\mathbb{F}; +, \cdot)$ 为一域. 则 $\mathbb{F} \setminus \{0\}$ 中元在 $(\mathbb{F}, +)$ 中有相同的阶; 当此阶有限时, 必为素数, 记其为 p, 称域的特征为 p; 否则, 称域的特征为零.

例 7.1.1　数域和其上多项式环的分式域的特征皆为零; 关于素数 p, $\mathbb{F}_{p^k}, \mathbb{F}_{p^k}(x)$, 特别地, $\mathbb{F}_p$ $(\cong \mathbb{Z}/\langle p \rangle), \mathbb{F}_p(x)$ 都是特征为 p 的域 (详见 7.5 节).

推论 7.1.1　令 $\mathbb{F} \overset{\mathrm{d}}{=} (\mathbb{F}; +, \cdot)$ 为一特征为 p 的域, $k \in \mathbb{Z}^+$. 则在 $\mathbb{F}$ 中, 有

$$(a+b)^{p^k} \equiv a^{p^k} + b^{p^k} \quad (\text{因此}, (a-b)^{p^k} \equiv a^{p^k} - b^{p^k}).$$

这等价于 $(a+b)^p \equiv a^p + b^p$ (因此, $(a-b)^p \equiv a^p - b^p$). 事实上, p 为素数时, $p | \mathrm{C}_p^i$, $i = 1, 2, \cdots, p-1$.

定义 7.1.3　令 $\mathbb{F}$ 为一域. 称 $\mathbb{F}$ 为一素域, 如果 $\mathbb{F}$ 没有真子域.

例 7.1.2　有理数域 $\mathbb{Q}$ 和关于素数 p 的剩余类环 $\mathbb{Z}/\langle p \rangle$ 都是素域.

定理 7.1.1　任意域 $\mathbb{F}$ 都含且只含一个素域; $\mathrm{char}(\mathbb{F})=0$ 时, $\mathbb{F}$ 的素域同构于 $\mathbb{Q}$, $\mathrm{char}(\mathbb{F})=p$ 时, $\mathbb{F}$ 的素域同构于 $\mathbb{Z}/\langle p\rangle$; 两个域的特征相同当且仅当它们的素域是同构的.

证明　令

$$\{\mathbb{F}_i|\mathbb{F}_i\leqslant\mathbb{F},\ i\in I\}$$

为 $\mathbb{F}$ 的子域的全体构成的集合. 则

$$\mathbb{P}=\bigcap_{i\in I}\mathbb{F}_i$$

非空, 且为 $\mathbb{F}$ 的一个子域, 显然 $\mathbb{P}$ 为一素域, 其唯一性是显然的.

定理中的第三个结论显然是第二个结论的推论, 因此, 只需证明第二个结论.

作整数环 $\mathbb{Z}$ 到 $\mathbb{F}$ 的映射

$$\begin{aligned}\varphi:\mathbb{Z}&\longrightarrow\mathbb{F},\\ m&\longmapsto me,\end{aligned}$$

其中, e 为 $\mathbb{F}$ 的幺元. 关于任意 $m,n\in\mathbb{Z}$,

$$\varphi(m+n)=(m+n)e=me+ne=\varphi(m)+\varphi(n),$$

$$\varphi(mn)=(mn)e=mene=\varphi(m)\varphi(n),$$

因此, φ 为一同态映射.

若 $\mathrm{char}(\mathbb{F})=0$, 则 $\mathrm{Ker}\ \varphi=\{0\}$. 记

$$R_e\overset{\mathrm{d}}{=}\mathrm{Im}\ \varphi=\{me|m\in\mathbb{Z}\}.$$

由同态基本定理, $R_e\cong\mathbb{Z}$, R_e 为一整环. 又, 同构的整环有同构的分式域, 从而

$$\mathbb{F}_e\cong\mathbb{Q},$$

其中,

$$\mathbb{F}_e=\left\{me/ne|m,n\in\mathbb{Z},n\neq0\right\}$$

为 R_e 的分式域. 显然, $\mathbb{F}_e\leqslant\mathbb{F}$, 且 $\mathbb{F}$ 的任一子域都包含 $\mathbb{F}_e$. 于是, $\mathbb{F}_e$ 为 $\mathbb{F}$ 的同构于 $\mathbb{Q}$ 的素域.

若 $\mathrm{char}(\mathbb{F})=p$, 则 $\mathrm{Ker}\ \varphi=\langle p\rangle$. 记

$$\mathbb{R}_e\overset{\mathrm{d}}{=}\mathrm{Im}\ \varphi=\{e,2e,\cdots,(p-1)e,0\}\subseteq\mathbb{F}.$$

由同态基本定理, $\mathbb{R}_e\cong\mathbb{Z}/\langle p\rangle$, 后者显然为一 (素) 域, 于是, $\mathbb{R}_e$ 为 $\mathbb{F}$ 的同构于 $\mathbb{Z}/\langle p\rangle$ 的素域.

□

推论 7.1.2　素域的自同构只有一个, 即恒等自同构.

7.1.2 域的扩张 (域) 及其分类

定义 7.1.4 令 $\mathbb{F}$, $\mathbb{K}$ 为两个域. 称 $\mathbb{K}$ 为 $\mathbb{F}$ 的一个扩张 (域), 如果 $\mathbb{F} \leqslant \mathbb{K}$ ($\mathbb{F}$ 为 $\mathbb{K}$ 的子域). 此时, 也称 $\mathbb{F}$ 为其扩域 $\mathbb{K}$ 的基域.

域的扩张的第一种分类——代数扩张和超越扩张

定义 7.1.5 令 $\mathbb{K}$ 为 $\mathbb{F}$ 的一个扩域. 称 $\mathbb{K}$ 为 $\mathbb{F}$ 的代数扩域, 如果 $\mathbb{K}$ 的每一个元素都是 $\mathbb{F}$ 上的代数元 (见定义 5.4.2), 即

$$(\forall\, a \in \mathbb{K})\ (\exists\, f(x) \in \mathbb{F}[x] \setminus \mathbb{F})\ f(a) = 0.$$

否则, 即至少有一非代数元 (非代数元称为超越元) 时, 称 $\mathbb{K}$ 为 $\mathbb{F}$ 的超越扩域. 又, 当 $\mathbb{K} \setminus \mathbb{F}$ 的元素都是 $\mathbb{F}$ 上的超越元时, 称 $\mathbb{K}$ 为 $\mathbb{F}$ 的纯超越扩域.

例 7.1.3 (1) $\mathbb{C}$ 为 $\mathbb{R}$ 的代数扩域;

(2) $\mathcal{A}_{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha$ 为 $\mathbb{Q}$ 上的代数元$\}$ 为 $\mathbb{Q}$ 的代数扩域 (详见 7.3 节);

(3) $\mathbb{F}_{p^k}$ 为 $\mathbb{F}_p$ ($\cong \mathbb{Z}/\langle p\rangle$) 的代数扩域 (详见 7.5 节);

(4) $\bigcup_{i=1}^{\infty} \mathbb{F}_{p^{k_i}}$ 为 $\mathbb{F}_p$ 的代数扩域, 其中, $i < j$ 时, $k_i | k_j$ (详见 7.5 节).

例 7.1.4 (1) $\mathbb{R}$ 为 $\mathbb{Q}$ 的一般超越扩域;

(2) $\mathbb{C}$ 为 $\mathbb{Q}$ 的一般超越扩域;

(3) $\mathbb{F}(x)$ 为 $\mathbb{F}$ 的纯超越扩域, 其中, $\mathbb{F}(x)$ 为 $\mathbb{F}[x]$ 的分式域 (详见 7.3 节);

(4) $\mathbb{C}$ 为 $\mathcal{A}_{\mathbb{Q}}$ 的纯超越扩域 (详见 7.3 节).

域的扩张的第二种分类——有限次扩张和无限次扩张

定义 7.1.6 令 $\mathbb{K}$ 为 $\mathbb{F}$ 的一个扩域. 则当视 $\mathbb{K}$ 为 $\mathbb{F}$ 上的线性空间 (将 $\mathbb{K}$ 的域加法作为加法, 域乘法作为 $\mathbb{F}$-乘所构成的那一线性空间) 时, 称 $\mathbb{F}$-线性空间 $\mathbb{K}$ 的维数为 $\mathbb{K}$ 在 $\mathbb{F}$ 上的扩张次数, 记为 $\partial(\mathbb{K}, \mathbb{F})$. 于是, $\mathbb{K}$ 作为 $\mathbb{F}$ 的扩域, 又可分为有限次和无限次两类.

例 7.1.5 (1) $\mathbb{C}$ 为 $\mathbb{R}$ 的有限 2 次扩域;

(2) $\mathbb{F}_{p^k}$ 为 $\mathbb{F}_p$ ($\cong \mathbb{Z}/\langle p\rangle$) 的有限 k 次扩域 (详见 7.5 节);

(3) $\mathcal{A}_{\mathbb{Q}}$ 为 $\mathbb{Q}$ 的无限次扩域 (详见 7.3 节);

(4) $\bigcup_{i=1}^{\infty} \mathbb{F}_{p^{k_i}}$ 为 $\mathbb{F}_p$ 的无限次扩域, 其中, $i < j$ 时, $k_i | k_j$ (详见 7.5 节);

(5) 超越扩域都是无限次的.

推论 7.1.3 由例 7.1.5 的 (5) 知, 有限次域扩张都是代数的.

鉴于推论 7.1.3, 上面关于域的扩张的第二种分类只对于代数扩张是有意义的. 于是, 关于代数扩张, 我们有

代数扩张的一种分类——有限次 (代数) 扩张和无限次代数扩张

例子见例 7.1.5.

我们还有

代数扩张的另一种分类——正规扩张和非正规扩张

定义 7.1.7 令 $\mathbb{K}$ 为域 $\mathbb{F}$ 的一个代数扩域. 关于任意 $f(x) \in \mathbb{F}[x] \setminus \mathbb{F}$, $\partial(f(x)) = n$, 记

$$S_{f(x)} = \{f(x) \text{ 的 } n \text{ 个根}\} \quad (\text{详见 7.4 节}).$$

称 $\mathbb{K}$ 为 $\mathbb{F}$ 的一个正规扩域, 如果关于任意不可约多项式 $p(x) \in \mathbb{F}[x]$,

$$S_{p(x)} \subseteq \mathbb{K},$$

或

$$S_{p(x)} \cap \mathbb{K} = \varnothing.$$

否则, 称 $\mathbb{K}$ 为 $\mathbb{F}$ 的一个非正规扩域.

例 7.1.6　(1) $\mathbb{C}$ 为 $\mathbb{R}$ 的 (二次) 正规扩域.

(2) $\mathcal{A}_{\mathbb{Q}}$ 为 $\mathbb{Q}$ 的 (无限次) 正规扩域.

(3) $\mathbb{R} \cap \mathcal{A}_{\mathbb{Q}}$ 为 $\mathbb{Q}$ 的 (无限次, 为什么?) 非正规扩域. 事实上, 显然, $\mathbb{R} \cap \mathcal{A}_{\mathbb{Q}}$ 为 $\mathbb{Q}$ 的代数扩域. 令

$$p(x) = x^4 - p \in \mathbb{Q}[x],$$

其中, p 为一正素数. 则由 Eisenstein 判别法知, $p(x)$ 在 $\mathbb{Q}$ 上不可约. 在 $\mathbb{C}$ 上,

$$\begin{aligned} p(x) = x^4 - p &= (x^2 - \sqrt{p})(x^2 + \sqrt{p}) \\ &= (x - \sqrt[4]{p})(x + \sqrt[4]{p})(x^2 + \sqrt{p}) \\ &= (x - \sqrt[4]{p})(x + \sqrt[4]{p})(x - \mathrm{i}\sqrt[4]{p})(x + \mathrm{i}\sqrt[4]{p}). \end{aligned}$$

从而 $p(x)$ 在 $\mathbb{C}$ 中的四个根分别为 $\sqrt[4]{p}$, $-\sqrt[4]{p}$, $\mathrm{i}\sqrt[4]{p}$, $-\mathrm{i}\sqrt[4]{p}$. 显然, $\sqrt[4]{p}$, $-\sqrt[4]{p} \in \mathbb{R} \cap \mathcal{A}_{\mathbb{Q}}$, 而 $\mathrm{i}\sqrt[4]{p}$, $-\mathrm{i}\sqrt[4]{p} \notin \mathbb{R} \cap \mathcal{A}_{\mathbb{Q}}$. 因此, $\mathbb{R} \cap \mathcal{A}_{\mathbb{Q}}$ 为 $\mathbb{Q}$ 的一个非正规扩域.

(4) $\mathbb{Q}(\sqrt[4]{p})$ 为 $\mathbb{Q}$ 的 (四次) 非正规 (单) 扩域 (单扩域的概念见下段)(因此, 有限次扩域未必是正规扩域, 正如上面的例子指出的, 正规扩域未必是有限次的).

7.1.3　域的扩张到域的单扩张的归结

定义 7.1.8　令 $\mathbb{K}$ 为 $\mathbb{F}$ 的一个扩域, $S \subseteq \mathbb{K}$. 则

$$\mathbb{L} \overset{\mathrm{d}}{=} \langle \mathbb{F} \cup S \rangle \overset{\mathrm{d}}{=} \mathbb{K} \text{ 的既含 } \mathbb{F} \text{ 又含 } S \text{ 的子域的交}$$

显然是 $\mathbb{K}$ 的包含 $\mathbb{F}$ 和 S 的最小域. 称其为添加子集 S 到基域 $\mathbb{F}$ 上所得到的 $\mathbb{K}$ 与 $\mathbb{F}$ 之间的中间域, 记为 $\mathbb{F}(S)$. 适当地选择 S (例如, 取 $S = \mathbb{K} \setminus \mathbb{F}$) 可使得 $\mathbb{F}(S) = \mathbb{K}$. 当 $S = \{a\}$ (即, S 为一单元集) 时, 称 $\mathbb{F}(a)$ 为 $\mathbb{F}$ 的一个单扩域.

定理 7.1.2　令 $\mathbb{K}$ 为 $\mathbb{F}$ 的一个扩域, $S_1, S_2 \subseteq \mathbb{K}$. 则

$$\mathbb{F}(S_1 \cup S_2) = [\mathbb{F}(S_1)](S_2) = [\mathbb{F}(S_2)](S_1).$$

证明　只需证明 $\mathbb{F}(S_1 \cup S_2) = [\mathbb{F}(S_1)](S_2)$.

显然, $[\mathbb{F}(S_1)](S_2)$ 是 $\mathbb{K}$ 的一个包含 $\mathbb{F}, S_1$ 和 S_2, 因而包含 $\mathbb{F}$ 和 $S_1 \cup S_2$ 的子域, 而 $\mathbb{F}(S_1 \cup S_2)$ 是 $\mathbb{K}$ 的一个包含 $\mathbb{F}$ 和 $S_1 \cup S_2$ 的最小子域. 因此

$$\mathbb{F}(S_1 \cup S_2) \subseteq [\mathbb{F}(S_1)](S_2).$$

另一方面, $\mathbb{F}(S_1 \cup S_2)$ 是 $\mathbb{K}$ 的一个包含 $\mathbb{F}, S_1$ 和 S_2, 因而包含 $\mathbb{F}(S_1)$ 和 S_2 的子域, 而 $[\mathbb{F}(S_1)](S_2)$ 是 $\mathbb{K}$ 的一个包含 $\mathbb{F}(S_1)$ 和 S_2 的最小子域, 因此

$$\mathbb{F}(S_1 \cup S_2) \supseteq [\mathbb{F}(S_1)](S_2).$$

于是

$$\mathbb{F}(S_1 \cup S_2) = [\mathbb{F}(S_1)](S_2). \qquad \square$$

令 $\mathbb{K}$ 为 $\mathbb{F}$ 的一个扩域, $S \subseteq \mathbb{K}$, $\mathbb{K} = \mathbb{F}(S)$. 根据良序公理, 可令 $S \overset{\mathrm{d}}{=} (S, \leqslant)$ 为一良序集, a_0 为 S 的最小元. 又根据定理 7.1.2,

$$\mathbb{F}(S) = [\mathbb{F}(a_0)](S \setminus \{a_0\}).$$

关于任意 $a \in S, a > a_0$, 假设 a 的前段

$$T_a = \{x \in S | x < a\}$$

的元素都可以逐次作单扩域先添加进来, 即

$$\mathbb{F}(S) = \{\{\{\{[\mathbb{F}(a_0)] \cdots\}(a_i)\}(a_j)\} \cdots\}(S \setminus T_a).$$

那么, 由

$$S \setminus T_a = \{a\} \cup [S \setminus (T_a \cup \{a\})],$$

根据定理 7.1.2, 有

$$\begin{aligned}\mathbb{F}(S) &= \{\{\{\{[\mathbb{F}(a_0)] \cdots\}(a_i)\}(a_j)\} \cdots\}(S \setminus T_a) \\ &= \{\{\{\{\{[\mathbb{F}(a_0)] \cdots\}(a_i)\}(a_j)\} \cdots\}(a)\}(S \setminus (T_a \cup \{a\})).\end{aligned}$$

即 $T_a \cup \{a\}$ 的元素也可以逐次作单扩域先添加进来. 于是, 根据超限归纳法, S 的元素都可以逐次作单扩域添加进来.

因此, 我们有下面的推论.

推论 7.1.4 域 $\mathbb{F}$ 上的任一扩域都可以通过 $\mathbb{F}$ 上的一系列单扩张获得.

7.2 域的单扩张 (域)

定义 7.2.1 令 $\mathbb{K}$ 为 $\mathbb{F}$ 的一个扩域, $\alpha \in \mathbb{K}$. 若 α 为 $\mathbb{F}$ 上的代数元 (超越元), 则称 $\mathbb{F}(\alpha)$ 为 $\mathbb{F}$ 的添加代数元 (超越元) α 的单扩域. 添加一超越元的单扩域称为单超越扩域 (实为一纯超越扩域 (详见推论 7.3.7)). 添加一代数元的单扩域称为单代数扩域 (理由详见定理 7.2.2).

定理 7.2.1 令 $\mathbb{K}$ 为 $\mathbb{F}$ 的一个扩域, $\alpha \in \mathbb{K}$ 为 $\mathbb{F}$ 上的超越元. 则添加超越元 α 的单超越扩域 $\mathbb{F}(\alpha)$ 同构于 $\mathbb{F}[x]$ 的分式域 $\mathbb{F}(x)$.

证明 因为 α 为 $\mathbb{F}$ 上的超越元, 所以

$$\mathbb{F}[x] \cong \mathbb{F}[\alpha].$$

又, 同构的整环有同构的分式域, 从而, 关于单超越扩域 $\mathbb{F}(\alpha)$, 有

$$\mathbb{F}(x) \cong \mathbb{F}(\alpha). \qquad \square$$

此为试读, 需要完整PDF请访问: www.ertongbook.com

定义 7.2.2　令 $\mathbb{K}$ 为 $\mathbb{F}$ 的一个扩域, $\alpha\in\mathbb{K}$ 为 $\mathbb{F}$ 上的代数元. 称 α 的首 1 的次数最低的 $\mathbb{F}$ 上的零化多项式为 α 在 $\mathbb{F}$ 上的最小多项式. 它显然是存在且唯一的. 称 α 在 $\mathbb{F}$ 上的最小多项式的次数为 α 在 $\mathbb{F}$ 上的次数, 记为 $\partial(\alpha,\mathbb{F})$.

定理 7.2.2　令 $\mathbb{K}$ 为 $\mathbb{F}$ 的一个扩域, $\alpha\in\mathbb{K}$ 为 $\mathbb{F}$ 上的代数元, 且 $p(x)$ 为 α 在 $\mathbb{F}$ 上的最小多项式. 则 $p(x)$ 在 $\mathbb{F}$ 上不可约, 而且单代数扩域

$$\mathbb{F}(\alpha)\cong\mathbb{F}[x]/\langle p(x)\rangle,$$

又, $\mathbb{F}(\alpha)$ 为 $\mathbb{F}$ 上的 $n\overset{\mathrm{d}}{=}\partial(\alpha,\mathbb{F})\overset{\mathrm{d}}{=}\partial(p(x))$ 次有限扩张. 因此, $\mathbb{F}(\alpha)$ 为 $\mathbb{F}$ 上的代数扩张 (这是称添加一代数元的单扩域为单代数扩域的缘由).

证明　若 $p(x)$ 在 $\mathbb{F}$ 上可约, 则

$$(\exists\, f(x),g(x)\in\mathbb{F}[x])\ p(x)=f(x)g(x),\quad 0<\partial(f(x)),\quad \partial(g(x))<\partial(p(x)).$$

由 $f(\alpha)g(\alpha)=p(\alpha)=0$ 和 $\mathbb{F}(\alpha)$ 无零因子知, $f(\alpha)=0$, 或 $g(\alpha)=0$, 这与 $p(x)$ 为 α 在 $\mathbb{F}$ 上的最小多项式矛盾. 因此, $p(x)$ 在 $\mathbb{F}$ 上不可约.

作映射

$$\begin{aligned}\varphi:\quad &\mathbb{F}[x]\longrightarrow\mathbb{F}[\alpha],\\ &f(x)\longmapsto f(\alpha).\end{aligned}$$

则容易验证 φ 为一满射, 且保持运算, 从而 φ 为一满同态映射. 显然, $\operatorname{Ker}\varphi=\langle p(x)\rangle$, 因此, 根据同态基本定理

$$\mathbb{F}[x]/\langle p(x)\rangle\cong\mathbb{F}[\alpha].$$

又, $\mathbb{F}[x]$ 为一主理想整环, $p(x)$ 在 $\mathbb{F}$ 上不可约, 从而, 根据定理 5.5.5, $\langle p(x)\rangle$ 为 $\mathbb{F}[x]$ 的一个极大理想, 因此, $\mathbb{F}(x)/\langle p(x)\rangle$ 为一域. 于是, $\mathbb{F}[\alpha]$ 已经为一域了, 即 $\mathbb{F}[\alpha]=\mathbb{F}(\alpha)$.

令

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

关于任意 $f(x)\in\mathbb{F}[x]$,

$$(\exists\, q(x),r(x)\in\mathbb{F}[x])\ f(x)=q(x)p(x)+r(x),$$

其中, $r(x)=0$, 或 $\partial(r(x))<n$. 从而, 关于任意 $f(\alpha)\in\mathbb{F}(\alpha)=\mathbb{F}[\alpha]$,

$$f(\alpha)=q(\alpha)p(\alpha)+r(\alpha)=r(\alpha).$$

因此

$$\mathbb{F}(\alpha)=G_{\mathbb{F}}[1,\alpha,\alpha^2,\cdots,\alpha^{n-1}],$$

这里, 等式右边表示 $\mathbb{K}$ 的由 $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$ 生成的 ($\mathbb{F}$ 上的) 子线性空间. 又, 显然 $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$ 线性无关, 因此, $(1,\alpha,\alpha^2,\cdots,\alpha^{n-1})$ 为 $\mathbb{F}$ 上线性空间 $\mathbb{F}(\alpha)$ 的一个基底. 从而, $\mathbb{F}(\alpha)$ 为 $\mathbb{F}$ 上的 n 次有限扩张. 于是, 根据推论 7.1.3, $\mathbb{F}(\alpha)$ 为 $\mathbb{F}$ 上的代数扩张. □

注 7.2.1 定理 7.2.2 的证明指出, $\partial(\alpha,\mathbb{F})$ 恰为使得 $1,\alpha,\alpha^2,\cdots,\alpha^n$ 在含 α 的 $\mathbb{F}$ 的代数扩域中线性相关的最小正整数 n.

根据定理 7.2.2, 易知下面的推论成立. 罗列如下, 以备后用.

推论 7.2.1 令 $\mathbb{K}$ 为 $\mathbb{F}$ 的一个扩域, $\alpha\in\mathbb{K}$. 则下列三条等价:

(1) α 为 $\mathbb{F}$ 上的代数元;

(2) $\mathbb{F}(\alpha)$ 为 $\mathbb{F}$ 上的有限次扩域;

(3) $\mathbb{F}(\alpha)$ 为 $\mathbb{F}$ 上的代数扩域.

上面讨论了两种单扩域的结构. 下面将讨论关于任意给定的域 $\mathbb{F}$, $\mathbb{F}$ 的单超越扩域和单代数扩域的存在性和唯一性.

定义 7.2.3 令 $\mathbb{K}$, $\mathbb{K}'$ 为 $\mathbb{F}$ 的两个扩域. 称同构 $\eta:\mathbb{K}\longrightarrow\mathbb{K}'$ 为一 $\mathbb{F}$-同构, 如果

$$(\forall\ a\in\mathbb{F})\ \eta(a)=a.$$

例 7.2.1 定理 7.2.1 和定理 7.2.2 证明中的同构都是使得 $x\mapsto\alpha$ 的 $\mathbb{F}$-同构.

定理 7.2.3 令 $\mathbb{F}$ 为一域. 则 $\mathbb{F}$ 的单超越扩域和单代数扩域都是存在的, 且在 $\mathbb{F}$-同构下是唯一的 (关于单代数扩张的唯一性, 指的是关于 $\mathbb{F}$ 上的同一个不可约多项式的任两个根 α 和 β, $\mathbb{F}(\alpha)$ 与 $\mathbb{F}(\beta)$ 是 $\mathbb{F}$-同构的).

证明 (1) 域 $\mathbb{F}$ 上一元多项式环 $\mathbb{F}[x]$ 的分式域 $\mathbb{F}(x)$ 就是 $\mathbb{F}$ 上添加超越元 x 的单超越扩域. 若 $\mathbb{F}(y)$ 也是 $\mathbb{F}$ 上的一个单超越扩域, 则 $\mathbb{F}(y)$ 也是 $\mathbb{F}[y]$ 的分式域. 作映射

$$\begin{aligned}\varphi:\quad &\mathbb{F}(x)\longrightarrow\mathbb{F}(y),\\ &\frac{f(x)}{g(x)}\longmapsto\frac{f(y)}{g(y)}.\end{aligned}$$

则容易验证 φ 为一 $\mathbb{F}$-同构. 因此, $\mathbb{F}(x)$ 和 $\mathbb{F}(y)$ 是 $\mathbb{F}$-同构的, 即 $\mathbb{F}$ 上的单超越扩域在 $\mathbb{F}$-同构意义上是唯一的.

(2) 关于单代数扩域的情形, 鉴于定理 7.2.2, 我们只需作下面的讨论. 令 $p(x)$ 为 $\mathbb{F}$ 上一首 1 的 n 次不可约多项式. 则

$$\mathbb{F}[x]/\langle p(x)\rangle=\{f(x)+\langle p(x)\rangle|f(x)\in\mathbb{F}_n[x]\}$$

为一域, 其中, $\mathbb{F}_n[x]$ 为 $\mathbb{F}$ 上全体次数小于 n 的多项式连同零多项式构成的集合. 显然

$$\mathbb{F}'=\{a+\langle p(x)\rangle|a\in\mathbb{F}\}$$

为 $\mathbb{F}[x]/\langle p(x)\rangle$ 的一个子域. 作映射

$$\begin{aligned}\varphi:\quad &\mathbb{F}\longrightarrow\mathbb{F}',\\ &a\longmapsto a+\langle p(x)\rangle.\end{aligned}$$

容易验证, φ 为一同构映射, 从而 $\mathbb{F}\cong\mathbb{F}'$. 因此, 可以将 $\mathbb{F}$ 和 $\mathbb{F}'$ 等同, 即可视 $\mathbb{F}[x]/\langle p(x)\rangle$ 为 $\mathbb{F}$ 的一个扩域.

记 $\overline{f(x)}=f(x)+\langle p(x)\rangle$. 则 $\overline{x}=x+\langle p(x)\rangle$ 为 $\mathbb{F}$ 上的代数元, 且 $p(x)$ 为 $\overline{x}$ 在 $\mathbb{F}$ 上的最小多项式. 事实上, 令

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

则

$$\begin{aligned}
p(\overline{x})&=\overline{x}^n+a_{n-1}\overline{x}^{n-1}+\cdots+a_1\overline{x}+a_0\\
&=(x+\langle p(x)\rangle)^n+a_{n-1}(x+\langle p(x)\rangle)^{n-1}+\cdots+a_1(x+\langle p(x)\rangle)+a_0\\
&=(x^n+\langle p(x)\rangle)+a_{n-1}(x^{n-1}+\langle p(x)\rangle)+\cdots+a_1(x+\langle p(x)\rangle)+a_0\\
&=(x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0)+\langle p(x)\rangle\\
&=p(x)+\langle p(x)\rangle\\
&=0+\langle p(x)\rangle\\
&=\overline{0}.
\end{aligned}$$

从而, $p(x)$ 为 $\overline{x}$ 在 $\mathbb{F}$ 上的一个零化多项式, 因此, $\overline{x}$ 为 $\mathbb{F}$ 上的代数元. 又 $p(x)$ 为 $\mathbb{F}$ 上零化 $\overline{x}$ 的次数最低的多项式 (请读者思考为什么?), 从而 $p(x)$ 为 $\overline{x}$ 在 $\mathbb{F}$ 上的最小多项式. 记 $\alpha=\overline{x}$, 基于 $\mathbb{F}$ 与 $\mathbb{F}'$ 等同, 我们有

$$\mathbb{F}(\alpha)\cong\mathbb{F}[x]/\langle p(x)\rangle,$$

这就是 $\mathbb{F}$ 上添加代数元 α 的单代数扩域.

令 $\mathbb{F}(\beta)$ 也是 $\mathbb{F}$ 上的一个单代数扩域, 且 β 和 α 有相同的最小多项式 $p(x)$. 由定理 7.2.2 的证明过程, 容易验证

$$\mathbb{F}(\alpha)=G_{\mathbb{F}}[1,\alpha,\alpha^2,\cdots,\alpha^{n-1}]$$

与

$$\mathbb{F}(\beta)=G_{\mathbb{F}}[1,\beta,\beta^2,\cdots,\beta^{n-1}]$$

间的映射

$$\begin{aligned}
\varphi:\mathbb{F}(\alpha)&\longrightarrow\mathbb{F}(\beta),\\
\sum_{i=0}^{n-1}a_i\alpha^i&\longmapsto\sum_{i=0}^{n-1}a_i\beta^i
\end{aligned}$$

为一 $\mathbb{F}$-同构 (请读者思考为什么?). 因此, 关于 $\mathbb{F}$ 上任一不可约多项式 $p(x)$, 添加 $p(x)$ 的任意两个根所得到的 $\mathbb{F}$ 的两个单代数扩域都是 $\mathbb{F}$-同构的. 这就是单代数扩域的一种唯一性. □

定义 7.2.4　令 $\mathbb{F}$ 为一域. 称 $\mathbb{F}$ 为一代数闭域, 如果 $\mathbb{F}$ 没有真代数扩域.

注 7.2.2　定理 7.2.3 中域 $\mathbb{F}$ 上单代数扩域的存在性的事实, 还构成代数闭域 (诸如, 复数域 $\mathbb{C}$、"代数数" 域 $\mathcal{A}_{\mathbb{Q}}$) 上任意次数大于等于 1 的多项式在其内至少有一个根的代数学基本定理的一个替代定理 (任意域 $\mathbb{F}$ 上的任意不可约多项式总在 $\mathbb{F}$ 的某个扩域里有根).

7.3 域的有限次扩张

7.3.1 有限次扩张和单代数扩张

定理 7.3.1 (次数公式) 令 $\mathbb{F} \leqslant \mathbb{L} \leqslant \mathbb{K}$, 它给出了三个域扩张, 即 $\mathbb{F}$ 的两个域扩张 $\mathbb{L}$ 和 $\mathbb{K}$, $\mathbb{L}$ 的一个域扩张 $\mathbb{K}$. 则

$$\partial(\mathbb{K},\mathbb{F}) < \infty \Longleftrightarrow \partial(\mathbb{K},\mathbb{L}) < \infty, \quad \text{且} \quad \partial(\mathbb{L},\mathbb{F}) < \infty.$$

此时, 有

$$\partial(\mathbb{K},\mathbb{F}) = \partial(\mathbb{K},\mathbb{L}) \cdot \partial(\mathbb{L},\mathbb{F}).$$

证明 (1) $\partial(\mathbb{K},\mathbb{F}) < \infty \Longrightarrow \partial(\mathbb{K},\mathbb{L}) < \infty$, 且 $\partial(\mathbb{L},\mathbb{F}) < \infty$.

令 $\partial(\mathbb{K},\mathbb{F}) = n < \infty$. 则 $\mathbb{K}$ 为 $\mathbb{F}$ 上的有限维线性空间. 因此, $\mathbb{L}$ 作为 $\mathbb{K}$ 的子空间, 当然也是 $\mathbb{F}$ 上的有限维线性空间, 即 $\partial(\mathbb{L},\mathbb{F}) < \infty$. 令 $(\alpha_1, \alpha_2, \cdots, \alpha_n)$ 为 $\mathbb{K}$ 作为 $\mathbb{F}$ 上线性空间的一个基底. 则关于任意 $\alpha \in \mathbb{K}$,

$$\alpha = f_1\alpha_1 + f_2\alpha_2 + \cdots + f_n\alpha_n,$$

其中, $f_i \in \mathbb{F} \leqslant \mathbb{L}$, $i = 1, 2, \cdots, n$. 从而,

$$\mathbb{K} = G_{\mathbb{L}}[\alpha_1, \alpha_2, \cdots, \alpha_n].$$

令 $\alpha_{i_1}, \alpha_{i_2}, \cdots, \alpha_{i_r}$ 为 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 在 $\mathbb{L}$ 上的一个极大线性无关组. 则 $(\alpha_{i_1}, \alpha_{i_2}, \cdots, \alpha_{i_r})$ 为 $\mathbb{K}$ 作为 $\mathbb{L}$ 上线性空间的一个基底. 因此, $\partial(\mathbb{K},\mathbb{L}) = r < \infty$.

(2) $\partial(\mathbb{K},\mathbb{L}) < \infty$, 且 $\partial(\mathbb{L},\mathbb{F}) < \infty \Longrightarrow \partial(\mathbb{K},\mathbb{F}) < \infty$.

令 $(\alpha_1, \alpha_2, \cdots, \alpha_n)$ 为 $\mathbb{K}$ 作为 $\mathbb{L}$ 上线性空间的一个基底, $(\beta_1, \beta_2, \cdots, \beta_m)$ 为 $\mathbb{L}$ 作为 $\mathbb{F}$ 上线性空间的一个基底. 则关于任意 $\alpha \in \mathbb{K}$,

$$\alpha = \sum_{i=1}^{n} l_i\alpha_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} f_{ij}\beta_j \right) \alpha_i = \sum_{i=1}^{n}\sum_{j=1}^{m} f_{ij}(\alpha_i\beta_j),$$

其中, $l_i \in \mathbb{L}$, $f_{ij} \in \mathbb{F}$, $i = 1, 2, \cdots, n$, $j = 1, 2, \cdots, m$. 从而,

$$\mathbb{K} = G_{\mathbb{F}}\big[\{\alpha_i\beta_j | i = 1, 2, \cdots, n,\ j = 1, 2, \cdots, m\}\big].$$

因此, $\partial(\mathbb{K},\mathbb{F}) \leqslant nm < \infty$.

(3) 当 $\partial(\mathbb{K},\mathbb{F}) < \infty$, 即 $\partial(\mathbb{K},\mathbb{L}) < \infty$ 且 $\partial(\mathbb{L},\mathbb{F}) < \infty$ 时,

$$\partial(\mathbb{K},\mathbb{F}) = \partial(\mathbb{K},\mathbb{L}) \cdot \partial(\mathbb{L},\mathbb{F}).$$

由 (2) 的证明过程知, 只需证明 $\{\alpha_i\beta_j \mid i = 1, 2, \cdots, n,\ j = 1, 2, \cdots, m\}$ 线性无关. 若

$$\sum_{i=1}^{n} \left(\sum_{j=1}^{m} f_{ij}\beta_j \right) \alpha_i = \sum_{i=1}^{n}\sum_{j=1}^{m} f_{ij}(\alpha_i\beta_j) = 0,$$

则由 $(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 为 $\mathbb{K}$ 关于 $\mathbb{L}$ 的一个基底知,

$$\sum_{j=1}^{m} f_{ij}\beta_j = 0, \quad i = 1,2,\cdots,n.$$

又, $(\beta_1,\beta_2,\cdots,\beta_n)$ 为 $\mathbb{L}$ 关于 $\mathbb{F}$ 的一个基底,

$$f_{ij} = 0, \quad i = 1,2,\cdots,n, \quad j = 1,2,\cdots,m.$$

因此, $\{\alpha_i\beta_j \mid i = 1,2,\cdots,n,\ j = 1,2,\cdots,m\}$ 线性无关. 于是,

$$\partial(\mathbb{K},\mathbb{F}) = nm = \partial(\mathbb{K},\mathbb{L})\cdot\partial(\mathbb{L},\mathbb{F}).$$ □

推论 7.3.1　令 $\mathbb{F} = \mathbb{F}_0 \leqslant \mathbb{F}_1 \leqslant \mathbb{F}_2 \leqslant \cdots \leqslant \mathbb{F}_l = \mathbb{K}$. 则

$$\partial(\mathbb{K},\mathbb{F}) < \infty \Longleftrightarrow \partial(\mathbb{F}_i,\mathbb{F}_{i-1}) < \infty, \quad i = 1,2,\cdots,l.$$

此时, 有

$$\partial(\mathbb{K},\mathbb{F}) = \partial(\mathbb{F}_l,\mathbb{F}_{l-1})\cdot\partial(\mathbb{F}_{l-1},\mathbb{F}_{l-2})\cdot\cdots\cdot\partial(\mathbb{F}_2,\mathbb{F}_1)\cdot\partial(\mathbb{F}_1,\mathbb{F}_0).$$

推论 7.3.2　关于任意域 $\mathbb{F}$, $\mathbb{F}$ 的有限次扩张具有传递性, 即, $\mathbb{F}$ 的有限次扩张的有限次扩张还是有限次扩张.

推论 7.3.3　令 $\mathbb{L}$ 为域 $\mathbb{F}$ 与 $\mathbb{K}$ 之间的一个中间域, 即 $\mathbb{F} \leqslant \mathbb{L} \leqslant \mathbb{K}$. 则当 $\partial(\mathbb{K},\mathbb{F}) < \infty$ 时, $\partial(\mathbb{L},\mathbb{F})|\partial(\mathbb{K},\mathbb{F})$. 因此, $\partial(\mathbb{K},\mathbb{F})$ 为素数时, $\mathbb{F}$ 与 $\mathbb{K}$ 之间无真中间域 (上两个命题的逆命题是否成立? 读者可以去做一些探索).

注 7.3.1　$\partial(\mathbb{K},\mathbb{F}) = \infty$ 当且仅当 $\partial(\mathbb{K},\mathbb{L})$ 和 $\partial(\mathbb{L},\mathbb{F})$ 至少有一个无限. 因此, 次数公式在 $\partial(\mathbb{K},\mathbb{F}) = \infty$ 时也成立.

定理 7.3.2　令 $\mathbb{K}$ 为 $\mathbb{F}$ 的一个扩域. 则 $\partial(\mathbb{K},\mathbb{F}) < \infty$ 当且仅当从 $\mathbb{F}$ 到 $\mathbb{K}$ 有一个单代数扩张的有限升链, 即有

$$\mathbb{F} = \mathbb{F}_0 \leqslant \mathbb{F}_1 \leqslant \mathbb{F}_2 \leqslant \cdots \leqslant \mathbb{F}_l = \mathbb{K},$$

其中, $\mathbb{F}_{i+1}$ 为 $\mathbb{F}_i$ 的单代数扩域, $i = 0,1,2,\cdots,l-1$.

证明　充分性. 根据推论 7.3.1,

$$\partial(\mathbb{K},\mathbb{F}) = \partial(\mathbb{F}_l,\mathbb{F}_{l-1})\partial(\mathbb{F}_{l-1},\mathbb{F}_{l-2})\cdots\partial(\mathbb{F}_2,\mathbb{F}_1)\partial(\mathbb{F}_1,\mathbb{F}_0).$$

又, 根据定理 7.2.2, $\partial(\mathbb{F}_{i+1},\mathbb{F}_i) < \infty$, $i = 0,1,2,\cdots,l-1$. 因此, $\partial(\mathbb{K},\mathbb{F}) < \infty$.

必要性. 证法一: 令 $\partial(\mathbb{K},\mathbb{F}) = n < \infty$, $(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 为 $\mathbb{K}$ 作为 $\mathbb{F}$ 上线性空间的一个基底. 则

$$\mathbb{K} = \mathbb{F}(\alpha_1,\alpha_2,\cdots,\alpha_n) = \{\{[\mathbb{F}(\alpha_1)](\alpha_2)\}(\alpha_3)\cdots\}(\alpha_n).$$

因此,

$$\mathbb{F} = \mathbb{F}_0 \leqslant \mathbb{F}_1 \leqslant \mathbb{F}_2 \leqslant \cdots \leqslant \mathbb{F}_n = \mathbb{K}$$

为一单代数扩张的有限升链, 其中, $\mathbb{F}_{i+1}=\mathbb{F}_i(\alpha_{i+1})$, $i=0,1,2,\cdots,n-1$.

证法二: 令 $\partial(\mathbb{K},\mathbb{F})=n<\infty$. 关于 $\partial(\mathbb{K},\mathbb{F})$ 在自然数集 $\mathbb{Z}^+$ 上作第二数学归纳法证明.

当 $\partial(\mathbb{K},\mathbb{F})=1$ 时, $\mathbb{K}=\mathbb{F}$, 结论显然成立.

假设 $\partial(\mathbb{K},\mathbb{F})<n$ 时, 结论都成立. 今考察 $\partial(\mathbb{K},\mathbb{F})=n$ 的情形. 令 $\alpha\in\mathbb{K}\setminus\mathbb{F}$, $\mathbb{F}_1=\mathbb{F}(\alpha)$. 则 $\mathbb{F}_1$ 为 $\mathbb{F}$ 的一个单代数扩张, 且 $\partial(\mathbb{F}_1,\mathbb{F})>1$. 从而由次数公式知, $\partial(\mathbb{K},\mathbb{F}_1)<n$. 由归纳假设, 存在 $\mathbb{F}_1$ 到 $\mathbb{K}$ 的一个单代数扩张升链

$$\mathbb{F}_1\leqslant\mathbb{F}_2\leqslant\cdots\leqslant\mathbb{F}_l=\mathbb{K}.$$

于是,

$$\mathbb{F}\leqslant\mathbb{F}_1\leqslant\mathbb{F}_2\leqslant\cdots\leqslant\mathbb{F}_l=\mathbb{K}$$

就是 $\mathbb{F}$ 到 $\mathbb{K}$ 的一个单代数扩张升链. □

推论 7.3.4 *令 $\mathbb{F}$ 为一域. 则 $\mathbb{F}$ 有不是 $\mathbb{F}$ 的单代数扩张的有限次扩张当且仅当在 $\mathbb{F}$ 上单代数扩张不具传递性.*

注 7.3.2 (1) 定理 7.3.2 证明中的必要性的证法一基于如下的一个易知的事实: 若 $\mathbb{K}$ 为基域 $\mathbb{F}$ 的一个有限 n 次扩域, 即存在 $\mathbb{K}$ 的在 $\mathbb{F}$ 上线性无关的 n 个元素 $\alpha_1,\alpha_2,\cdots,\alpha_n\in\mathbb{K}$, 使得

$$\mathbb{K}=G_{\mathbb{F}}[\alpha_1,\alpha_2,\cdots,\alpha_n],$$

则

$$\mathbb{K}=\mathbb{F}(\alpha_1,\alpha_2,\cdots,\alpha_n).$$

当然, 反之未必, 单代数扩张就是一例.

(2) 有限次 (代数) 扩张是且仅是添加扩域里的有限个元素到基域所得到的扩张.

(3) 域 $\mathbb{F}$ 添加 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 所得到的有限次扩域

$$\mathbb{F}(\alpha_1,\alpha_2,\cdots,\alpha_n)\subseteq\mathbb{F}[\alpha_1,\alpha_2,\cdots,\alpha_n].$$

下面给出利用中间域刻画有限次扩张是单代数扩张的一个定理.

定理 7.3.3 (Artin 本原元定理) *令 $\mathbb{K}$ 为无限域 $\mathbb{F}$ 的一个有限次 (代数) 扩张. 则 $\mathbb{K}$ 为 $\mathbb{F}$ 的一个单代数扩张当且仅当 $\mathbb{F}$ 与 $\mathbb{K}$ 之间只有有限多个不同的中间域.*

证明 充分性. 关于任意 $w\in\mathbb{K}$, $\mathbb{F}(w)$ 为 $\mathbb{F}$ 与 $\mathbb{K}$ 的中间域. 由于 $\mathbb{F}$ 与 $\mathbb{K}$ 之间只有有限多个不同的中间域, 又 $\mathbb{K}$ 为 $\mathbb{F}$ 的一个有限次扩张, 从而可选取适当的 $u\in\mathbb{K}$, 使得 $\partial(\mathbb{F}(u),\mathbb{F})$ 最大. 若 $\mathbb{F}(u)\neq\mathbb{K}$, 即 $\mathbb{F}(u)$ 为 $\mathbb{K}$ 的一个真子域, 则存在 $v\in\mathbb{K}\setminus\mathbb{F}(u)$. 显然, 有且仅有有限多个形如

$$\mathbb{F}(u+av)$$

的中间域, 其中 $a\in\mathbb{F}$. 又 $\mathbb{F}$ 为一无限域, 从而

$$(\exists\, a_1,a_2\in\mathbb{F},\ a_1\neq a_2)\ \mathbb{F}(u+a_1v)=\mathbb{F}(u+a_2v).$$

因此

$$v=\frac{1}{a_1-a_2}[(u+a_1v)-(u+a_2v)]\in\mathbb{F}(u+a_1v),$$

此为试读,需要完整PDF请访问: www.ertongbook.com