代数与数论

李超 周悦 编著

科学出版社

国防科技大学研究生数学公共课程系列教材

代数与数论

李 超 周 悦 编著

科学出版社

北京

内 容 简 介

本书以域的扩张理论为主线，通过介绍域扩张、伽罗瓦扩张、数域扩张和有限域扩张的基本理论与方法，为纠错编码与密码研究提供所必需的代数与数论方面的知识.

本书可作为数学专业和密码学专业高年级本科生和研究生的选修课教材，也可以作为从事编码密码理论及应用研究的科技人员的参考书.

图书在版编目(CIP)数据

代数与数论/李超，周悦编著. —北京：科学出版社，2018.6
国防科技大学研究生数学公共课程系列教材
ISBN 978-7-03-057474-9

Ⅰ.①代… Ⅱ.①李… ②周… Ⅲ.①代数数论-研究生-教材 Ⅳ.①O156.2

中国版本图书馆 CIP 数据核字 (2018) 第 103623 号

责任编辑：李静科 / 责任校对：彭珍珍
责任印制：张 伟 / 封面设计：耕者工作室

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

北京教图印刷有限公司印刷
科学出版社发行 各地新华书店经销
*
2018 年 6 月第 一 版 开本：720×1000 B5
2018 年 6 月第一次印刷 印张：13 3/4
字数：267.000

定价：79.00 元

(如有印装质量问题，我社负责调换)

前　言

纠错编码和密码是信息处理中两个重要的研究方向. 纠错编码通过增加消息冗余度的方法, 排除在噪声信道下传输消息时所带来的干扰, 主要解决信息处理中的纠错问题, 为信息的可靠性提供理论与技术支撑. 密码通过在传输的消息中人为地加入噪声, 使其变成窃听者难以解读的信息, 主要解决信息处理中的保密问题, 为信息的安全性提供理论与技术支撑. 纠错编码和密码虽然解决的问题不同, 但这两门应用性学科所用到的数学工具大体一致, 二者都以代数、数论、组合和图论等离散数学为主要研究工具. 特别地, 代数与数论在纠错编码和密码的理论与应用研究中起到了至关重要的作用.

本书以域的扩张理论为主线, 通过介绍域扩张、伽罗瓦扩张、数域扩张和有限域扩张的基本理论与方法, 为纠错编码与密码研究提供所必需的代数与数论方面的知识. 在域扩张中, 主要介绍一般域扩张的基本概念, 包括单扩张、有限扩张、代数扩张、可分扩张、正规扩张和分裂域等; 在伽罗瓦扩张中, 主要介绍伽罗瓦扩张和伽罗瓦群的基本概念, 特别是伽罗瓦扩张的中间域与伽罗瓦群的子群之间的反序一一对应关系, 强调群论在域论研究中所起的重要作用; 在数域扩张中, 主要介绍数域扩张及其代数整数环的特点, 强调数域扩张中代数整数环的理想分解特性和类数有限性定理; 在有限域扩张中, 主要介绍有限域以及有限域扩张的特点, 强调有限域的代数结构特性、有限域上的不可约多项式、有限域上的指数和以及有限域上的方程等基本理论. 本书最后一章给出了纠错编码、密码与组合设计中的五个应用实例, 这些实例所用到的数学工具正是本书所介绍的代数与数论方面的知识.

本书在写作过程中力求做到: 叙述深入浅出, 文字生动活泼, 推导自然流畅, 例题充实新颖. 特别关注各章节之间的逻辑关系和前后呼应关系, 较为系统地介绍了域的扩张理论. 但是由于水平有限, 时间仓促, 书中难免存在不妥之处, 恳请读者批评指正.

本书得以出版, 衷心感谢导师冯克勤教授的鼓励与支持! 也感谢国防科技大学编码密码理论及其应用团队长期以来的和谐合作! 希望本书的出版能够为纠错编码与密码方面的人才培养起到积极的作用.

作　者

2017 年 12 月 25 日

目　录

前言
第 1 章　域扩张……1
1.1　域的特征……1
1.2　单扩张……6
1.3　有限扩张与代数扩张……9
1.4　可分扩张与正规扩张……13
第 2 章　伽罗瓦扩张……18
2.1　伽罗瓦群……18
2.2　伽罗瓦扩张的定义……22
2.3　伽罗瓦基本理论……27
第 3 章　数域扩张……35
3.1　数域的嵌入……35
3.2　判别式与单位根……41
3.3　代数整数环……51
3.4　代数整数环的加法特性……57
3.5　代数整数环的乘法特性……63
第 4 章　代数整数环的分解特性……69
4.1　Dedekind 整环……69
4.2　素理想分解……73
4.3　分解特征……76
4.4　分解算法……85
4.5　伽罗瓦情形下的分解……94
第 5 章　理想类群与类数……103
5.1　格与 Minkowski 定理……103
5.2　理想类群……110
5.3　类数有限性定理……114
5.4　不定方程……121
第 6 章　有限域扩张……129
6.1　有限域的结构特点……129
6.2　有限域上的不可约多项式……134

6.3　有限域上的迹函数、范数与基 ····· 141
6.4　有限域上的指数和 ····· 151
6.5　有限域上的方程 ····· 163
第 7 章　应用实例 ····· 174
7.1　PN 函数的原像分布特征 ····· 174
7.2　基于 PN 函数的线性码的权分布 ····· 182
7.3　广义 Bent 函数的存在性 ····· 192
7.4　乘子定理及其证明 ····· 201
7.5　差集的存在性问题 ····· 207
参考文献 ····· 212

第1章 域 扩 张

1.1 域的特征

设 R 是一个整环, 即 R 是一个无零因子的交换环. 记 $R^* = R\backslash\{0\}$ 为 R 中全体非零元的集合, 在集合 $R \times R^* = \{(a,b) \mid a \in R, b \in R^*\}$ 中定义如下二元关系:

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc.$$

易知上述二元关系 "$\sim$" 具有自反性、对称性和传递性, 即 "$\sim$" 为集合 $R \times R^*$ 上的一个等价关系. 用 $R \times R^*/\sim$ 表示集合 $R \times R^*$ 中全体等价类的集合, 用 $\frac{a}{b}$ 表示元素 (a,b) 所在的等价类, 则

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc.$$

在集合 $R \times R^*/\sim$ 中定义如下加法和乘法:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd},$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

则 $R \times R^*/\sim$ 关于上面定义的加法和乘法构成一个域.

首先, 上面定义的加法和乘法与等价类的代表元选取无关. 事实上, 如果 $\frac{a}{b} = \frac{a'}{b'}, \frac{c}{d} = \frac{c'}{d'}$, 则 $ab' = ba', cd' = dc'$, 故

$$ab'dd' = ba'dd', \quad cd'bb' = dc'bb',$$

于是

$$ab'dd' + cd'bb' = ba'dd' + dc'bb'.$$

又由于 R 为交换环, 所以

$$adb'd' + bcb'd' = a'd'bd + b'c'bd,$$

从而

$$\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}, \quad \text{即} \quad \frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}.$$

这表明加法的定义与等价类的代表元选取无关. 类似可证乘法的定义也与等价类的代表元选取无关.

其次, $(R\times R^*/\sim,+)$ 为一个交换群. 这是因为加法具有如下性质:

(1) 封闭律: 对任意 $\frac{a}{b},\frac{c}{d}\in R\times R^*/\sim$,

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}\in R\times R^*/\sim .$$

(2) 结合律: 对任意 $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in R\times R^*/\sim$,

$$\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{ad+bc}{bd}+\frac{e}{f}=\frac{adf+bcf+bde}{bdf},$$

$$\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}+\frac{cf+de}{df}=\frac{adf+bcf+bde}{bdf},$$

故

$$\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right).$$

(3) 有零元 $\frac{0}{u}$(这里 u 为 R^* 中任意元): 对任意 $\frac{a}{b}\in R\times R^*/\sim$,

$$\frac{a}{b}+\frac{0}{u}=\frac{au}{bu}=\frac{a}{b},$$
$$\frac{0}{u}+\frac{a}{b}=\frac{ua}{ub}=\frac{a}{b}.$$

(4) 有负元: 对任意 $\frac{a}{b}\in R\times R^*/\sim$, 取 $\frac{-a}{b}\in R\times R^*/\sim$, 则

$$\frac{a}{b}+\frac{-a}{b}=\frac{ab-ab}{b^2}=\frac{0}{b^2}=\frac{0}{u},$$

其中 $u=b^2\in R^*$.

(5) 交换律: 对任意 $\frac{a}{b},\frac{c}{d}\in R\times R^*/\sim$,

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}=\frac{da+cb}{db}=\frac{c}{d}+\frac{a}{b}.$$

从而 $(R\times R^*/\sim,+)$ 确实构成一个交换群. 类似可以验证, $\left((R\times R^*/\sim)^*,\cdot\right)$ 同样构成一个交换群, 这里 $(R\times R^*/\sim)^*=\{R\times R^*/\sim \text{中全体非零元}\}$, 并且该乘法群中的单位元为 $\frac{u}{u}$ $(u\in R^*)$, 对每个非零元 $\frac{b}{a}$, 其乘法逆元为 $\frac{a}{b}$.

最后, 乘法对加法的分配律成立: 即对任意 $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in R \times R^* / \sim$,

$$\frac{a}{b} \cdot \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f},$$

$$\left(\frac{a}{b} + \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{a}{b} \cdot \frac{e}{f} + \frac{c}{d} \cdot \frac{e}{f}.$$

我们称 $(R \times R^* / \sim, +, \cdot)$ 为整环 R 的**分式域**.

例 1.1 整数环 $\mathbb{Z}$ 的分式域是有理数域 $\mathbb{Q}$, 域 F 上多项式环 $F[x]$ 的分式域为

$$F(x) = \left\{ \frac{f(x)}{g(x)} \middle| f(x), g(x) \in F[x], g(x) \neq 0 \right\},$$

以后称 $F(x)$ 为有理函数域.

例 1.2 高斯整数环 $\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} | a, b \in \mathbb{Z}\}$ 的分式域为高斯数域 $\mathbb{Q}(\mathrm{i}) = \{a + b\mathrm{i} | a, b \in \mathbb{Q}\}$, 其中 $\mathrm{i} = \sqrt{-1}$ 为虚数单位.

定理 1.1 任意整环 R 均存在分式域 F, 并且在同构意义下, 分式域 F 是包含 R 的最小域.

证明 定理的前半部分已证明, 下面我们证明后半部分, 构造映射:

$$\begin{aligned} f : R &\to F \\ a &\mapsto \frac{au}{u} \text{ (这里 } u \text{ 为 } R^* \text{ 中任意元)}, \end{aligned}$$

则 f 是从 R 到 F 的单射, 并满足

$$f(a+b) = \frac{(a+b)u}{u} = \frac{au + bu}{u} = \frac{au^2 + bu^2}{u^2} = \frac{au}{u} + \frac{bu}{u} = f(a) + f(b),$$

$$f(ab) = \frac{abu}{u} = \frac{abu^2}{u^2} = \frac{au}{u} \cdot \frac{bu}{u} = f(a) f(b).$$

于是 f 是从 R 到 F 的单同态, 从而 F 中包含子环 $f(R)$ 与 R 同构, 即在同构意义下 F 包含 R.

另一方面, 如果某个域 E 包含 R, 则在同构意义下 E 包含 F 的子环 $f(R)$, 即 E 包含形如 $\frac{au}{u}$ $(a \in R)$ 的元素, 又由于 E 为域, 故 E 包含 $\frac{au}{u}$ 的逆元 $\frac{u}{au}$(当 $a \in R^*$ 时), 即 E 包含所有 $\frac{v}{bv}$ $(b \in R^*)$, 从而 E 包含所有 $\frac{au}{u} \cdot \frac{v}{bv} = \frac{a}{b}$, 即 E 包含 F, 因此 F 是包含 R 的最小域. □

推论 1.1 设 R_1 和 R_2 是两个整环, F_1 和 F_2 分别是 R_1 和 R_2 的分式域, 如果 $R_1 \cong R_2$, 则 $F_1 \cong F_2$.

设 E 是一个域, F 是 E 的子集合, 如果 F 对于 E 中的加法与乘法也构成一个域, 则称 F 为 E 的**子域**, E 为 F 的**扩域**. 域 F 的所有子域的交集仍是 F 的子域, 称这个子域为域 F 的**素域**, 易知素域是域 F 的最小子域.

定理 1.2　设 F 是任意域, 则 F 的素域或者同构于有理数域 $\mathbb{Q}$, 或者同构于整数环 $\mathbb{Z}$ 模某个素数 p 的剩余类域 $\mathbb{Z}_p$.

证明　用 e 表示域 F 中的乘法单位元, 则 F 包含如下子环:

$$R_0 = \{\cdots, -2e, -e, 0, e, 2e, \cdots\}.$$

构造 $\mathbb{Z}$ 到 R_0 的映射 $\varphi: n \mapsto ne, \forall n \in \mathbb{Z}$, 则 φ 具有如下性质:

(1) φ 是从 $\mathbb{Z}$ 到 R_0 的满射;

(2) φ 保加法, 即对于任意 $m, n \in \mathbb{Z}$, 均有 $\varphi(m+n) = \varphi(m) + \varphi(n)$;

(3) φ 保乘法, 即对于任意 $m, n \in \mathbb{Z}$, 均有 $\varphi(mn) = \varphi(m)\varphi(n)$.

即 φ 是从整数环 $\mathbb{Z}$ 到 F 的子环 R_0 的满同态.

根据环的同态基本定理, 我们得到

$$\mathbb{Z}/\ker\varphi \cong R_0,$$

其中, $\ker\varphi = \{n | n \in \mathbb{Z}, ne = 0\}$.

由于 $\ker\varphi$ 是整数环 $\mathbb{Z}$ 中的一个理想, 而 $\mathbb{Z}$ 为主理想整环, 从而 $\ker\varphi$ 为 $\mathbb{Z}$ 中的一个主理想, 即存在正整数 m, 使得 $\ker\varphi = (m)$.

下证 $m = 0$ 或 m 为素数.

如果 $m \neq 0$ 并且 m 也不为素数, 则存在两个正整数 $m_1, m_2, 0 < m_1, m_2 < m$, 使得 $m = m_1 m_2$, 由于 $\varphi(m) = me = 0$, 故

$$(m_1 e) \cdot (m_2 e) = (m_1 m_2) e = me = 0,$$

注意到 F 为域, 于是 R_0 中无零因子, 从而

$$m_1 e = 0 \quad 或 \quad m_2 e = 0.$$

即 $m_1 \in (m)$ 或 $m_2 \in (m)$, 这是不可能的! 假设不成立, 从而 $m = 0$ 或 m 为素数.

如果 $m = 0$, 则 $\ker\varphi = \{0\}$, 从而 $\mathbb{Z}/\ker\varphi = \mathbb{Z} \cong R_0$, 注意到 $\mathbb{Z}$ 的分式域为 $\mathbb{Q}$, R_0 的分式域为 F 的素域, 由推论 1.1 可知, F 的素域同构于有理数域 $\mathbb{Q}$.

如果 $m = p$ 为素数, 则 $\ker\varphi = (p)$, 这时 $\mathbb{Z}/\ker\varphi = \mathbb{Z}_p$ 为模 p 的剩余类域, 而 $\mathbb{Z}_p \cong R_0$, 故 R_0 本身已具有域结构, 即 R_0 本身为域 F 的素域, 它同构于整数环 $\mathbb{Z}$ 模 p 的剩余类域 $\mathbb{Z}_p$. □

定义 1.1　设 F 是一个域, 如果域 F 的素域同构于有理数域 $\mathbb{Q}$, 则称域 F 的特征为 0, 记为 $\mathrm{Char}F = 0$. 如果域 F 的素域同构于整数环 $\mathbb{Z}$ 模 p 的剩余类域 $\mathbb{Z}_p$, 则称域 F 的特征为 p, 记为 $\mathrm{Char}F = p$.

有理数域 $\mathbb{Q}$ 和整数环模素数 p 的剩余类域 $\mathbb{Z}_p$ 是两类最基本的域, 一切域都可以作为这两类域的扩张. 以有理数域为素域的域的特征为 0, 比如高斯数域 $\mathbb{Q}(\mathrm{i})$、实数域 $\mathbb{R}$、复数域 $\mathbb{C}$ 等; 以 $\mathbb{Z}_p$ 为素域的域的特征为 p, 比如有限域 F_{p^n}、有理函数域 $F_p(x)$ 等等.

例 1.3 设 F 为一个域, 并且 $\mathrm{Char}F=p$, 则对任意 $a\in F$, 均有 $pa=0$, 从而在 F 中下列两式成立:

$$(a+b)^p=a^p+b^p,\quad (a-b)^p=a^p-b^p,$$

这里 $a,b\in F$.

证明 由于 $\mathrm{Char}F=p$, 故对 F 中乘法单位元 e, 有 $pe=0$, 于是对每一个 $a\in F$,

$$pa=\overbrace{a+a+\cdots+a}^{p}=\overbrace{ea+ea+\cdots+ea}^{p}=(pe)a=0a=0.$$

另外, 由于 F 中乘法是可交换的, 故

$$(a+b)^p=\sum_{k=0}^{p}C_p^k a^k b^{p-k},$$

其中, $C_p^k=\dfrac{p!}{k!\,(p-k)!}$.

当 $1\leqslant k\leqslant p-1$ 时, $(p,k!)=(p,(p-k)!)=1$, 故 $(p,k!\,(p-k)!)=1$, 而 $p!$ 中含有因子 p, 故 p 整除 C_p^k, 于是 $C_p^k a^{p-k}b^k=0$, 从而 $(a+b)^p=a^p+b^p$, 同理 $(a-b)^p=a^p-b^p$. □

习 题 1.1

1. 证明高斯整数环 $\mathbb{Z}[\mathrm{i}]=\{a+b\mathrm{i}|a,b\in\mathbb{Z}\}$ 的分式域为高斯数域 $\mathbb{Q}(\mathrm{i})=\{a+b\mathrm{i}|a,b\in\mathbb{Q}\}$.

2. 令 $R=\left\{a+b\sqrt{2}\,|a,b\in\mathbb{Z}\right\}$, 证明 R 是一个整环, 并且 R 的分式域为

$$\mathbb{Q}(\sqrt{2})=\left\{a+b\sqrt{2}\,|a,b\in\mathbb{Q}\right\}.$$

3. 对于任意正整数 n, 当 n 满足什么条件时, 整数环 $\mathbb{Z}$ 模 n 的剩余类环 $\mathbb{Z}_n$ 是整环? 当 $\mathbb{Z}_n$ 为整环时, 给出其分式域.

4. 设 p 是一个素数, V 是剩余类域 $\mathbb{Z}_p$ 上的 n 维线性空间, 证明 V 上可逆线性变换的个数为

$$(p^n-1)(p^n-p)\cdots(p^n-p^{n-1}).$$

5. 设 F 是一个域, 证明多元多项式环 $F[x_1,x_2,\cdots,x_n]$ 是一个整环, 并且其分式域为

$$F(x_1,x_2,\cdots,x_n)=\{f(x_1,x_2,\cdots,x_n)/g(x_1,x_2,\cdots,x_n)\,|f,g\in F[x_1,x_2,\cdots,x_n],g\neq 0\}.$$

6. 设 F 是特征为 p 的有限域, $a\in F$, 证明 x^p-x-a 在 F 中不可约当且仅当 x^p-x-a 在 F 中无根.

1.2　单　扩　张

设 E 是域 F 的扩域, S 是 E 的一个非空子集合, E 中包含 F 和 S 的最小子域称为**由 F 添加 S 生成的域**, 记为 $F(S)$. 易知

$$F(S)=\bigcap\{L|L \text{ 是 } E \text{ 的子域, 并且 } F\bigcup S\subseteq L\}.$$

特别地, 如果 S 是一个单元集, 即 $S=\{\alpha\}$, 则称 $F(\alpha)$ 为 F 的**单扩张**. 如果 S 是一个有限集, 即 $S=\{\alpha_1,\alpha_2,\cdots,\alpha_t\}$, 则称 $F(S)=F(\alpha_1,\alpha_2,\cdots,\alpha_t)$ 为 F 的**有限生成扩张**.

容易证明:

$$\begin{aligned}F(\alpha_1,\alpha_2,\cdots,\alpha_t)&=F(\alpha_1,\alpha_2,\cdots,\alpha_{t-1})(\alpha_t)\\&=F(\alpha_1,\alpha_2,\cdots,\alpha_{t-2})(\alpha_{t-1})(\alpha_t)\\&\cdots\cdots\\&=F(\alpha_1)(\alpha_2)\cdots(\alpha_t),\end{aligned}$$

也就是说域的有限生成扩张可以通过有限次单扩张来实现.

定理 1.3　域 F 的单扩张或者同构于有理函数域 $F(x)$, 或者同构于多项式环 $F[x]$ 模某个不可约多项式 $p(x)$ 的剩余类域 $F[x]/(p(x))$.

证明　设 E 为域 F 的扩域, $\alpha\in E$, 令

$$F[\alpha]=\{f(\alpha)\,|f(x)\in F[x]\}\subseteq E,$$

则 $F[\alpha]$ 构成域 E 的一个无零因子的子环.

构作 $F[x]$ 到 $F[\alpha]$ 的映射 $\varphi: f(x)\mapsto f(\alpha)$, 对任意 $f(x)\in F[x]$. 则 φ 是多项式环 $F[x]$ 到域 E 的子环 $F[\alpha]$ 的满同态, 由环的同态基本定理, $F[x]/\ker\varphi\cong F[\alpha]$. 由于 $F[x]$ 为主理想整环, 而 $\ker\varphi$ 为 $F[x]$ 中一个理想, 故存在 $p(x)\in F[x]$ 使得 $\ker\varphi=(p(x))$.

下证 $p(x)=0$ 或者 $p(x)$ 为不可约多项式.

事实上, 如果 $p(x)\neq 0$ 并且 $p(x)$ 不是 $F[x]$ 中不可约多项式, 则存在两个多项式 $p_1(x)$ 和 $p_2(x)$, $\deg p_i(x)<\deg p(x)\,(i=1,2)$, 使得 $p(x)=p_1(x)p_2(x)$, 从而 $p_1(\alpha)p_2(\alpha)=p(\alpha)=0$. 注意到 $F[\alpha]$ 中无零因子, 故 $p_1(\alpha)=0$ 或 $p_2(\alpha)=0$, 即 $p_1(x)\in(p(x))$ 或 $p_2(x)\in(p(x))$, 这是不可能的, 故 $p(x)=0$ 或 $p(x)$ 为不可约多项式.

如果 $p(x)=0$, 则 $\ker\varphi=\{0\}$, 从而 $F[x]/\ker\varphi=F[x]\cong F[\alpha]$. 由推论 1.1 可知, $F[x]$ 的分式域 $F(x)$ 同构于 $F[\alpha]$ 的分式域 $F(\alpha)$.

如果 $p(x)$ 不可约, 则 $\ker\varphi=(p(x))$ 为 $F[x]$ 中的极大理想, 从而 $F[x]/(p(x))$ 为域结构, 故 $F[\alpha]\cong F[x]/(p(x))$ 也为域结构, 从而 $F(\alpha)=F[\alpha]\cong F[x]/(p(x))$. □

定义 1.2 设 E 是 F 的扩域, $\alpha\in E$, 如果存在 $F[x]$ 中的非零多项式 $f(x)$, 使得 $f(\alpha)=0$, 则称 α 为 F 上的**代数元**. 否则, 称 α 为 F 上的**超越元**. 如果 α 为 F 上的代数元, 则使得 $f(\alpha)=0$ 的首项系数为 1 并且次数最低的多项式是唯一的, 称该多项式为元素 α 的**极小多项式**.

域 F 中每个元素为 F 的代数元, 这是因为对每个 $\alpha\in F, x-\alpha$ 为 α 在 F 上的极小多项式. 如果 α 为 F 上的代数元, 则 α 在 F 上的极小多项式一定是不可约多项式. 事实上, 如果 α 的极小多项式 $f(x)$ 是可约的, 则可以分解为 $f(x)=f_1(x)f_2(x)$, 这里 $f_i(x)\in F[x], \deg f_i(x)<\deg f(x)\,(i=1,2)$, 于是由 $f_1(\alpha)f_2(\alpha)=f(\alpha)=0$ 可得 $f_1(\alpha)=0$ 或 $f_2(\alpha)=0$, 这与极小多项式的次数最低矛盾! 故 $f(x)$ 不可约. 如果 α 的极小多项式为 n 次多项式, 则称 α 为 $\boldsymbol{n}$ **次代数元**.

例 1.4 $\mathrm{i}, \sqrt[3]{2}, e^{\frac{2\pi\mathrm{i}}{n}}$ 均为有理数域 $\mathbb{Q}$ 上的代数元, 它们分别为 $\mathbb{Q}[x]$ 中多项式 x^2+1, x^3-2, x^n-1 的根. 特别地, x^2+1 和 x^3-2 分别为 i 和 $\sqrt[3]{2}$ 的极小多项式, 但 x^n-1 不一定为 $e^{\frac{2\pi\mathrm{i}}{n}}$ 的极小多项式.

例 1.5 π 和 e 均为有理数域 $\mathbb{Q}$ 上的超越元.

超越元的证明不是一件容易的事情, 例 1.5 的证明超出了本书的范围.

注意到有理数集是可数集, 从而有理数域上单变元多项式集合 $\mathbb{Q}[x]$ 也为可数集, 于是 $\mathbb{Q}$ 上代数元的集合是可数集. 考虑到复数集 $\mathbb{C}$ 是不可数集, 从而复数集中 $\mathbb{Q}$ 上的代数元相对于超越元而言, 数目非常少.

例 1.6 求 $\sqrt{2}+\mathrm{i}$ 在有理数域 $\mathbb{Q}$ 上的极小多项式.

解 设 $f(x)$ 是 $\sqrt{2}+\mathrm{i}$ 在 $\mathbb{Q}$ 上的极小多项式, 由于实系数多项式的虚数根是共轭成对出现的, 因此 $\sqrt{2}-\mathrm{i}$ 也是 $f(x)$ 的一个根, 于是在 $\mathbb{R}[x]$ 中 $(x-\sqrt{2}-\mathrm{i})(x-\sqrt{2}+\mathrm{i})$ 一定为 $f(x)$ 的因式, 也就是说在 $\mathbb{R}[x]$ 中, $x^2-2\sqrt{2}x+3|f(x)$, 但 $x^2-2\sqrt{2}x+3$ 不是有理系数多项式, 从而它不是 $\sqrt{2}+\mathrm{i}$ 在 $\mathbb{Q}$ 上的极小多项式. 注意到 $\left[(x^2+3)-2\sqrt{2}x\right]\left[(x^2+3)+2\sqrt{2}x\right]=x^4-2x^2+9$ 是一个有理系数不可约多项式, 并且 x^4-2x^2+9 以 $\sqrt{2}+\mathrm{i}$ 为根, 故 $f(x)=x^4-2x^2+9$.

例 1.7 已知 n 为正整数, p 为素数, $\zeta_{p^n}=e^{\frac{2\pi\mathrm{i}}{p^n}}$ 是 p^n 次本原单位根, 计算 ζ_{p^n} 在有理数域 $\mathbb{Q}$ 上的极小多项式.

解 根据本原单位根的定义, ζ_{p^n} 是多项式 $x^{p^n}-1$ 的根, 但不是 $x^{p^{n-1}}-1$ 的根, 从而 ζ_{p^n} 是如下多项式 $f(x)$ 的根:

$$f(x)=\frac{x^{p^n}-1}{x^{p^{n-1}}-1}=x^{p^n-p^{n-1}}+x^{p^n-2p^{n-1}}+\cdots+x^{p^n-(p-1)p^{n-1}}+1.$$

下面证明 $f(x)$ 是 $\mathbb{Z}[x]$ 中的不可约多项式.

令 $g(x)=f(x+1)$, 则

$$g(x)=\frac{(x+1)^{p^n}-1}{(x+1)^{p^{n-1}}-1}\equiv\frac{x^{p^n}+1-1}{x^{p^{n-1}}+1-1}\equiv x^{p^n-p^{n-1}}(\mathrm{mod}\,p).$$

上式表明 $g(x)\in\mathbb{Z}[x]$ 的系数除最高项系数之外, 其余均是素数 p 的倍数, 而 $g(x)$ 的常数项 $g(0)=f(1)$ 是 p 的倍数, 但不是 p^2 的倍数, 根据艾森斯坦判别法, $g(x)$ 是 $\mathbb{Z}[x]$ 中的不可约多项式, 从而 $f(x)$ 也是 $\mathbb{Z}[x]$ 中的不可约多项式, 于是 $f(x)$ 为 ζ_{p^n} 在 $\mathbb{Q}$ 上的极小多项式. □

例 1.8　设 E 为域 F 的扩张, $\alpha\in E$, 如果 α 为 F 上的超越元, 则 $F(\alpha)\cong F(x)$. 如果 α 为 F 的 n 次代数元, 则

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

证明　定理 1.3 的证明过程表明: 当 α 为 F 上的超越元时, $F(\alpha)\cong F(x)$. 当 α 为 F 上的代数元时,

$$F(\alpha)=F[\alpha]=\{g(\alpha)\,|g(x)\in F[x]\}.$$

如果 α 为 F 上的 n 次代数元, 不妨设 $f(x)$ 为 α 的极小多项式, 这时 $\deg f(x)=n$, 则对每一个多项式 $g(x)\in F[x]$, 根据带余除法, 存在唯一的 $q(x),r(x)\in F[x]$, 使得

$$g(x)=f(x)q(x)+r(x),$$

其中 $r(x)=0$ 或 $\deg r(x)<\deg f(x)=n$. 从而

$$g(\alpha)=f(\alpha)q(\alpha)+r(\alpha)=r(\alpha),$$

故

$$\begin{aligned}F(\alpha)=F[\alpha]&=\{r(\alpha)\,|r(x)\in F[x],r(x)=0\text{ 或 }\deg r(x)<n\}\\&=\{a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}|a_i\in F,0\leqslant i\leqslant n-1\}.\end{aligned}$$ □

例 1.9　证明 $f(x)=x^3-3x+1$ 为 $\mathbb{Q}[x]$ 中的不可约多项式. 假设 α 为 $f(x)$ 在复数域中的一个根, 计算 $\beta=\alpha^2+\alpha+1$ 的乘法逆元.

证明　由于 $f(x)$ 是 $\mathbb{Q}[x]$ 中的 3 次多项式, 假设 $f(x)$ 为 $\mathbb{Q}[x]$ 中可约多项式, 则 $f(x)$ 在 $\mathbb{Q}[x]$ 中必有一次因式, 从而 $f(x)$ 在 $\mathbb{Q}$ 中一定有根. 由于 $f(x)$ 的有理根只能为 ±1, 但 $f(1)=-1$, $f(-1)=3$, 故 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约.

令 $g(x)=x^2+x+1$, 则 $(f(x),g(x))=1$, 利用多项式的辗转相除法可得

$$f(x)\left(\frac{3}{19}x+\frac{5}{19}\right)+g(x)\left(-\frac{3}{19}x^2-\frac{2}{19}x+\frac{14}{19}\right)=1,$$

于是由 $f(\alpha)=0$ 可以得到

$$g(\alpha)\left(-\frac{3}{19}\alpha^2-\frac{2}{19}\alpha+\frac{14}{19}\right)=1,$$

故

$$\beta^{-1}=g^{-1}(\alpha)=-\frac{3}{19}\alpha^2-\frac{2}{19}\alpha+\frac{14}{19}.$$ □

以上我们在讨论域的单扩张时, 总是假设存在一个比 F 更大的域 E, 然后在 E 中讨论包含 F 和 E 中元素 α 的最小域 $F(\alpha)$. 事实上, 我们可以不必事先知道 E, 即有如下事实.

设 F 为任意域, α 为任意元素, 如果 α 不是 $F[x]$ 中非零多项式的根, 则 α 为 F 的超越元, 这时 $F(\alpha)$ 取有理函数域 $F(x)$, 只是将其中 x 换成 α 即可. 如果 α 为 $F[x]$ 中某个非零多项式的根, 这时 α 为 F 的代数元, $F(\alpha)$ 取 $F[\alpha]=\{g(\alpha)\,|g(x)\in F[x]\}$, 这里 $F[\alpha]$ 中元素的运算由 F 的某个隐含扩张所决定, 即有如下定理.

定理 1.4 设 F 是一个域, $f(x)\in F[x]$ 为不可约多项式, 则存在 F 的扩域 E, 使得 E 包含 $f(x)$ 的一个根.

证明 由于 $F[x]$ 为主理想整环, $f(x)\in F[x]$ 为不可约多项式, 故 $(f(x))$ 为 $F[x]$ 中一个极大理想, 从而 $F[x]/(f(x))$ 为一个域. 令 $E=F[x]/(f(x))$, 则 E 中含有子域 $\bar{F}=\{\bar{\alpha}|\alpha\in F\}$ 与 F 同构, 故在同构意义下, F 可以看作 E 的一个子域, 这时对 $\bar{x}\in E$, 有 $f(\bar{x})=\overline{f(x)}=\bar{0}=0$. □

推论 1.2 设 F 是一个域, $f(x)$ 是 $F[x]$ 中次数 $\geqslant 1$ 的多项式, 则存在 F 的扩域 E, 使得 $f(x)$ 的全部根都包含在 E 中.

习 题 1.2

1. 计算复数 $\sqrt{2}+\mathrm{i}$ 在数域 $\mathbb{Q}(\sqrt{2})$ 上的极小多项式.

2. 设 E/F 为域的扩张, $\alpha\in E$ 是域 F 上的代数元, 并且代数次数为奇数, 证明 $F(\alpha)=F(\alpha^2)$.

3. 证明 $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

4. 证明 $f(x)=x^3-3x-1$ 是有理数域上的不可约多项式. 假设 α 是 $f(x)$ 的一个复数根, 计算复数 $3\alpha^2+7\alpha+5$ 的乘法逆元.

5. 设 p 是一个素数, α 是多项式 $f(x)=x^{p-1}+x^{p-2}+\cdots+x+1\in\mathbb{Q}[x]$ 的一个复数根, 试证明 $[\mathbb{Q}(\alpha):\mathbb{Q}]=p-1$.

1.3 有限扩张与代数扩张

单扩张是由域 F 添加一个元素 α 得到的扩张, 如果 α 为 F 上的超越元, 我们称 $F(\alpha)$ 是 F 的**单超越扩张**, 如 $\mathbb{Q}(\pi)$ 为 $\mathbb{Q}$ 的单超越扩张. 如果 α 是 F 上的代数元, 我们称 $F(\alpha)$ 为 F 的**单代数扩张**, 如 $\mathbb{Q}(\mathrm{i})$ 为 $\mathbb{Q}$ 的单代数扩张. 单扩张是一

类比较简单的扩张, 下面介绍比单代数扩张更为广泛的两类扩张: 有限扩张与代数扩张.

设 E 是 F 的扩域, 则 E 关于 E 中元素的加法运算以及 F 中元素与 E 中元素的乘法运算构成域 F 上的线性空间. 如果 E 为 F 上的有限维线性空间, 则称 E 是 F 的有**限扩张**, 这时空间的维数称为**域扩张次数**, 记为 $[E:F]$.

例 1.10　复数域 $\mathbb{C}$ 是实数域 $\mathbb{R}$ 的扩域, $\mathbb{C}$ 可以作为 $\mathbb{R}$ 上的线性空间, 这时 1 和 i 构成 $\mathbb{C}$ 在 $\mathbb{R}$ 上的一组基. 因为对每个复数 $\alpha \in \mathbb{C}$, 存在两个实数 $a, b \in \mathbb{R}$, 使得 $\alpha = a \cdot 1 + b \cdot \mathrm{i}$, 并且 1 和 i 在 $\mathbb{R}$ 上线性无关, 于是 $\mathbb{C}$ 是 $\mathbb{R}$ 上的 2 维线性空间, 即 $\mathbb{C}$ 为 $\mathbb{R}$ 的有限扩张, 域扩张次数为 $[\mathbb{C}:\mathbb{R}] = 2$.

例 1.11　设 α 是域 F 上的 n 次代数元, 则 F 是 $F(\alpha)$ 的子域, 从而 $F(\alpha)$ 可以作为 F 上的线性空间. 对任意 $\beta \in F(\alpha)$, 均存在 $a_0, a_1, \cdots, a_{n-1} \in F$, 使得 $\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$, 并且 $1, \alpha, \cdots, \alpha^{n-1}$ 在 F 上线性无关 (否则与 α 为 n 次代数元矛盾), 故 $1, \alpha, \cdots, \alpha^{n-1}$ 构成 $F(\alpha)$ 在 F 上的一组基, 于是 $F(\alpha)$ 是 F 的有限扩张, 并且域扩张次数为 $[F(\alpha):F] = n$, 这表明单代数扩张必为有限扩张.

定理 1.5　设 E 是 F 的有限扩张, K 是 E 的有限扩张, 则 K 是 F 的有限扩张, 并且

$$[K:F] = [K:E][E:F].$$

证明　设 $[K:E] = m, [E:F] = n$, 并且 K 在 E 上的一组基为 $\alpha_1, \alpha_2, \cdots, \alpha_m$, E 在 F 上的一组基为 $\beta_1, \beta_2, \cdots, \beta_n$, 下证 $\{\alpha_i\beta_j\}\,(1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n)$ 构成 K 在 F 上的一组基.

对任意 $\alpha \in K$, 存在 $e_1, e_2, \cdots, e_m \in E$, 使得 $\alpha = \sum\limits_{i=1}^{m} e_i\alpha_i$. 又对每个 $e_i \in E$, 存在 $f_{i1}, f_{i2}, \cdots, f_{in} \in F$ 使得 $e_i = \sum\limits_{j=1}^{n} f_{ij}\beta_j$, 于是

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

这说明 K 中任意元均可表示为 $\{\alpha_i\beta_j\}\,(1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n)$ 的 F-线性组合形式.

再证 $\{\alpha_i\beta_j\}\,(1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n)$ 在 F 上线性无关. 事实上, 如果存在 $c_{ij} \in F\,(1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n)$, 使得

$$\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}\alpha_i\beta_j = 0,$$

则

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

由 $\alpha_1,\alpha_2,\cdots,\alpha_m$ 的线性无关性可以推出 $\sum\limits_{j=1}^{n}c_{ij}\beta_j=0$, 再由 $\beta_1,\beta_2,\cdots,\beta_n$ 的线性无关性推出 $c_{ij}=0$, 于是 $\{\alpha_i\beta_j\}(1\leqslant i\leqslant m,1\leqslant j\leqslant n)$ 在 F 上线性无关. 因此, K 构成 F 的有限扩张, 并且 $[K:F]=[K:E][E:F]$. □

例 1.11 表明单代数扩张必为有限扩张, 更进一步, 我们有如下结论.

定理 1.6 设 E 是 F 的扩域, $\alpha_i\in E$ 并且 α_i 是 F 上的代数元, $i=1,2,\cdots,n$, 则 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 是 F 的有限扩张.

证明 当 $n=1$ 时, $F(\alpha_1)$ 为 F 的单代数扩张, 从而 $F(\alpha_1)$ 为 F 的有限扩张.

假设命题当 $n-1$ 时成立, 即 $F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})$ 是 F 的有限扩张, 下证 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 必为 F 的有限扩张. 由于 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)=F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})(\alpha_n)$, 并且 α_n 为 F 上的代数元, 从而 α_n 为 $F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})$ 上的代数元, 于是 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 是 $F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})$ 的有限扩张. 由定理 1.5 中有限扩张的传递性, $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 是 F 的有限扩张. □

例 1.12 计算 $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]$, 并求 $\mathbb{Q}(\sqrt{2},\sqrt{3})$ 在 $\mathbb{Q}$ 上的一组基.

解 由于 $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$, 又 $1,\sqrt{2}$ 为 $\mathbb{Q}(\sqrt{2})$ 在 $\mathbb{Q}$ 上的一组基, 而 $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$, 并且 $1,\sqrt{3}$ 为 $\mathbb{Q}(\sqrt{2},\sqrt{3})$ 在 $\mathbb{Q}(\sqrt{2})$ 上的一组基, 故

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2\times2=4,$$

并且 $1,\sqrt{2},\sqrt{3},\sqrt{6}$ 为 $\mathbb{Q}(\sqrt{2},\sqrt{3})$ 在 $\mathbb{Q}$ 上的一组基. □

定义 1.3 设 E 是 F 的扩域, 如果 E 中每个元素都是 F 上的代数元, 则称 E 为 F 的**代数扩张**, 否则称 E 为 F 的**超越扩张**.

例 1.13 复数域 $\mathbb{C}$ 是实数域 $\mathbb{R}$ 的代数扩张, 实数域 $\mathbb{R}$ 是有理数域 $\mathbb{Q}$ 的超越扩张.

解 对每个复数 $\alpha=a+b\mathrm{i}\,(a,b\in\mathbb{R})$, 均存在 $\varphi(x)=x^2-2ax+a^2+b^2\in\mathbb{R}[x]$, 使得 $\varphi(\alpha)=0$, 从而 α 为 $\mathbb{R}$ 上的代数元, 故复数域 $\mathbb{C}$ 是实数域 $\mathbb{R}$ 的代数扩张. 注意到 $\pi\in\mathbb{R}$ 是有理数域 $\mathbb{Q}$ 上的超越元, 故实数域 R 是有理数域 $\mathbb{Q}$ 的超越扩张. □

定理 1.7 设 E 是 F 的有限扩张, 则 E 必为 F 的代数扩张.

证明 由于 E 是 F 的有限扩张, 不妨设 $[E:F]=n$, 则对每个 $\alpha\in E,n+1$ 个元素 $1,\alpha,\alpha^2,\cdots,\alpha^n$ 在 F 上线性相关, 于是存在 F 中不全为零的元素 $a_0,a_1,a_2,\cdots,a_n$, 使得

$$a_0 1+a_1\alpha+\cdots+a_n\alpha^n=0.$$