伽罗瓦理论简明教程

Huichi Huang

Mathematical Department, College of mathematics and statistics, Chongqing University, Chongqing, China, 401331电子邮箱地址: huanghuichi@cqu.edu.cn

arXiv:2601.01876v1 [math.HO] 5 Jan 2026

代数是魔鬼向数学家提出的交易。魔鬼说：“我会给你这台强大的机器，它能回答你提出的任何问题。你只需要把灵魂交给我：放弃几何，你就能得到这台奇妙的机器。”

Michael Atiyah

目录

前言 1

记号 3

第1章 基础群论 5 1.1 定义和例子 5 1.2 对称群 S_n 7 1.3 群的构造 8 1.4 同构定理 9 1.5 群作用 10 1.6 A_n 的单性 12 1.7 可解群 13 习题 15

第2章 基础环论 17 2.1 定义和例子 17 2.2 整环的分式域 20 2.3 素理想与极大理想 21 2.4 多项式环 23 2.5 主理想整环 24 2.6 艾森斯坦判别法和高斯引理 26 习题 27

第3章 基础域论 29 3.1 有限域 29 3.2 向量空间 29 3.3 域扩张 29 3.4 分裂域 31 3.5 可分扩张 34 习题 39

第4章 伽罗瓦理论及其应用 43 4.1. 伽罗瓦扩张的刻画 43 4.2. 伽罗瓦理论基本定理 46 4.3. 伽罗瓦群的计算 49 4.4. 伽罗瓦大定理与根式可解多项式 51 4.5. 尺规作图问题 53 习题 56

参考文献 59

前言

代数的本质是一种关于对称性与结构的语言。从古人探索如何解多项式方程，到现代对抽象代数系统的研究，代数的发展历程充满了深刻的洞见与优雅的理论。其中，伽罗瓦理论堪称一项卓越成就，它将群论、域论与方程几何融为一体，构建起统一的框架。本书旨在引领读者领略这一优美的领域。

本书源于作者多年在重庆大学教授本科生和研究生代数课程的经验，旨在以尽可能少的先修知识为基础，向读者介绍伽罗瓦理论。本书试图将现代代数的抽象工具——群、环和域——与启发伽罗瓦理论诞生的历史问题重新联系起来：如何确定一个多项式能否用根式求解。通过以具体动机为抽象概念奠定基础，我们希望阐明代数结构的“如何”与“为何”。

本书分为四章，每章都循序渐进地构建内容，逐步迈向 e
伽罗瓦理论的核心：

1. 基础群论：从 Lagrange 的开创性工作到西洛定理，我们奠定群论基础，重点讲解对称群、可解性以及交错群的简单性。

2. 基础环论与域论：介绍多项式环、理想和域扩张，并着重阐述它们在分裂域与可分性中的作用。

3. 伽罗瓦理论：严格证明基本定理及其推论，揭示域扩张与群作用之间的联系，并为应用奠定基础。

4. 应用：从用根式求解多项式到经典的尺规作图问题，我们展示伽罗瓦理论如何借助现代工具解决由来已久的问题。

本书具有以下特点：

极简基础：仅介绍群、环和域论中的基本概念，在保持严谨性的同时避免不必要的抽象。

历史动机：叙述经常回到用根式求解的问题，将抽象思想置于其历史背景之中。

计算洞见：对伽罗瓦群和分裂域的具体计算架起了理论与实践之间的桥梁。

习题与例子：150 多道习题涵盖从基础证明到探索性问题的不同层次，并配有详尽的例子，鼓励主动学习。

本书专为数学专业高年级本科生和研究生新生编写。读者需熟悉线性代数和基本集合论，但无需具备抽象代数的先修知识。教师可以

将其用于一学期课程，并可灵活地侧重理论深度或计算技术。

Huichi Huang 重庆
大学 2025年春季

符号说明

全书中，我们使用以下记号。$\mathbb{Z}$：整数集；$\mathbb{N}$：非负整数集；$\mathbb{Z}^+$：正整数集；$\mathbb{Q}$：有理数集；$\mathbb{Q}^+$：正有理数集；$\mathbb{R}$：实数集；$\mathbb{C}$：复数集；$|A|$：有限集 A 的基数；$\emptyset$：空集。$\mathbb{F}$：域。

第1章

基础群论

1.1. 定义与例子

群的形式化定义由 Cayley 于19世纪20年代提出，不过具体例子早在一个世纪前就已出现在 Lagrange 的著作中。 [Kle86] 如今，群在数学和物理学中无处不在。

DEFINITION 1.1.1. **群**是一个非空集合 G，配备一种二元运算“$\cdot$”，并满足

(1) 对任意 $a,b \in G$，$a \cdot b \in G$；(2) 对所有 a、b、$c \in G$，$(a \cdot b) \cdot c = a \cdot (b \cdot c)$；(3) 存在一个元素 $e \in G$，使得对每个 $a \in G$，都有 $e \cdot a = a \cdot e = a$；(4) 对每个 $a \in G$，存在 $b \in G$，使得 $a \cdot b = b \cdot a = e$。

为简便起见，当二元运算明确时，我们只将 $a \cdot b$ 写作 ab。如果对于所有 a，b 中的 G，都有 $ab = ba$，则称 G 为一个**阿贝尔群**。

EXAMPLES 1.1.1.

(1) 整数集 $\mathbb{Z}$ 在加法下构成一个阿贝尔群；(2) 非零实数集 $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ 在乘法下构成一个阿贝尔群；(3) 可逆 $n \times n$ 实矩阵在矩阵乘法下构成一个群，记为 $\mathrm{GL}_n(\mathbb{R})$；(4) 设 X 是一个非空集合。其上的双射在映射的复合下构成一个群。将该群记为 S_X，称其为 X 的对称群。(5) 对于 $n \geq 1$，令 $\mathbb{Z}/n\mathbb{Z}$ 为集合 $\{\bar{0}, \bar{1}, \cdots, n-1\}$，并定义 $\bar{i}$与 $\bar{}$ $\bar{}$在 $\mathbb{Z}/n\mathbb{Z}$ 中的加法为 k，其中 k 在 $[0, n)$ 中是 $i + j$ 除以n所得的余式。于是，$\mathbb{Z}/n\mathbb{Z}$ 在上述定义的加法（仍记为 $+$）下构成一个群。$\mathbb{Z}/n\mathbb{Z}$ 的另一~~种常~~见记法是 $\mathbb{Z}_n$。(6) 对于 $n \geq 1$，令 $(\mathbb{Z}/n\mathbb{Z})^\times$ 为不超过 n 且与 n互素的正整数集合。定义 $(\mathbb{Z}/n\mathbb{Z})^\times$ 中 i 与 j 的乘积为 $i \times j$ 除以 n所得的余式。于是，$(\mathbb{Z}/n\mathbb{Z})^\times$ 在上述定义的乘法下构成一个阿贝尔群。REMARKS 1.1.1. (1) 群 G 不仅由集合决定，也由二元运算决定。同一个集合在一种二元运算下可能构成群，但在另一种运算下却不构成群。例如，$\mathbb{Z}$在加法下构成一个群，但在乘法下不构成群。(2) 群中存在唯一单位元。

(3) 给定群 G中的一个元素 a，存在唯一的 b 属于 G，使得 $ab = ba = e$； b 称为 a 的**逆元**，记为 a^{-1}。

如果群 G 中存在 a，使得 G 中的每个 b 都可以表示为某个 n（$\mathbb{Z}$）的 $b = a^n$，则称群 G 为**循环**群，而 a 称为 G 的生成元。在这种情况下，将 G 写作 $\langle a\rangle$。例如 $\mathbb{Z} = \langle 1\rangle$ 和 $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1}\rangle$。

群 G 的子集 A 称为 G 的**生成集**，如果 G 的每个元素 a 都可以表示为

$$a = a_1^{n_1} a_2^{n_2} \cdots a_m^{n_m}$$

其中 A 中的 a_i，以及 $\mathbb{Z}$ 中的 n_i。我们也说，G 由 A 生成。循环群是由单个元素生成的群。包含某些元素的 G 的最小子群称为由这些元素生成的子群。

Remark 1.1.1. 群的生成集可能并不唯一，有时甚至是无限的。例如，$\mathbb{Z}^2 = \langle (1, 0), (0, 1)\rangle = \langle (1, 2), (2, 3)\rangle$。事实上，$GL_2(\mathbb{Z})$ 中任意元素的行都给出了 $\mathbb{Z}^2$ 的一个生成集。

群 G 的子集 N 称为 G 的一个**子群**，如果 N 在与 G 相同的二元运算下构成一个群。记作 $N \leq G$。将 G 的子群 $\{e\}$ 记作 $\mathbf{1}$。

每个群 G 都有两个平凡子群 $\mathbf{1}$ 和 G。偶整数集合 $2\mathbb{Z}$是 $\mathbb{Z}$的一个子群，而 $\mathbb{Z}$ 是 $\mathbb{R}$的一个子群。

对于群 G 的子群 N，以及 G 中的 x，集合 $xN = \{xy | y \in N\}$ ($Nx = \{yx | y \in N\}$ 称为 G 中 N 的左（右）**陪集**。例如，奇整数集合 $1 + 2\mathbb{Z}$ 既是 $\mathbb{Z}$ 中 $2\mathbb{Z}$ 的左陪集，也是右陪集，因为 $\mathbb{Z}$ 是阿贝尔群。可以验证，任意两个陪集要么相同，要么不相交。

Theorem 1.1.1（拉格朗日定理）。

如果 H 是有限群 G的子群，那么 $|H|$ 整除 $|G|$。

要证明拉格朗日定理，我们需要一个引理。

Lemma 1.1.1. 设 H 是 G的子群。任意两个左陪集 xH 和yH 要么相同，要么不相交。

Proof. 设 $z \in xH \cap yH$。则存在 $h_1, h_2 \in H$ 使得 $z = xh_1 = yh_2$。因此，对于任意 $h \in H$，有 $xh = (xh_1)(h_1^{-1}h) = (yh_2)(h_1^{-1}h) = y(h_2h_1^{-1}h)$，这说明 $xH \subseteqq yH$。类似地，$yH \subseteqq xH$。因此 $xH = yH$。□

Proof. [定理 1.1.1 的证明]
注意，对于 G中的每个 x，都有 $G = \bigcup_{x\in G} xH$ 和 $|xH| = |H|$。根据引理 1.1.1，$|G|$是 $|H|$的倍数。□

记 $[G : H]$ 为 G 中 H 的左陪集数，并称其为 G 中 H 的**指数**。由定理 1.1.1，得

$$[G : H] = \frac{|G|}{|H|}.$$

群 G 中的每个元素 a 都能生成 G 的一个子群 $\langle a\rangle = \{a^n \,|\, n \in \mathbb{Z}\}$。$\langle a\rangle$ 的基数称为 a 的**阶**。记为 Ord_a。a 的阶是满足 $a^n = e$ 的最小正整数 n。如果这样的 n 对 a 不存在，那么我们称 a 的阶为无限阶。

根据拉格朗日定理，有限群中每个元素的阶 G 都是 $|G|$的因子。

1.2. 对称群 S_n

当 $X = \{1, 2, \cdots, n\}$时，群 S_X称为**n 次对称群**，记作 S_n。

在 S_n 中，元素 σ 称为 **m-轮换**，如果 σ 按如下方式置换 $\{i_1, i_2, \cdots, i_m\} \subseteq \{1, 2, \cdots, n\}$：$\sigma(i_k) = i_{k+1}$，其中 $1 \leq k \leq m-1$；以及 $\sigma(i_m) = i_1$ 和 $\sigma(j) = j$，其中 $j \notin \{i_1, i_2, \cdots, i_m\}$。记作 $(i_1\, i_2\, \cdots\, i_m)$。2-循环称为**对换**。

例如，在 S_5 中，3-循环 $\sigma = (1\ 2\ 3)$ 满足：$\sigma(1) = 2$，$\sigma(2) = 3$，$\sigma(3) = 1$，而 $\sigma(4) = 4$，$\sigma(5) = 5$。

轮换的乘积按照映射的复合从右向左读取。例如，按照这一规则，$(1\ 2)(2\ 3\ 4) = (1\ 2\ 3\ 4)$。

LEMMA 1.2.1. 一个 m-轮换的阶为 m。

PROOF. 考虑 m-轮换 $\sigma = (i_1\, i_2\, \cdots\, i_m)$。可以看出，$\sigma(i_1) = i_2$，$\sigma^2(i_1) = i_3$，$\cdots$，$\sigma^{m-1}(i_1) = i_m$，$\sigma^m(i_1) = i_1$。类似地，对所有 $1 \leq k \leq m$，$\sigma^m(i_k) = i_k$。此外，对于所有不在 $\{i_1, i_2, \cdots, i_m\}$ 中的 j，$\sigma^m(j) = j$。因此 $\sigma^m = e$。而且，对于任意 $k < m$，$\sigma^k \neq e$，因为 $\sigma^k(i_1) = i_{k+1} \neq i_1$。所以 $\mathrm{Ord}_\sigma = m$。□

若两个轮换 $(i_1\, i_2\, \cdots\, i_m)$ 和 $(j_1\, j_2\, \cdots\, j_k)$ 满足 $\{i_1, i_2, \cdots, i_m\}$ 与 $\{j_1, j_2, \cdots, j_k\}$ 是不相交的集合，则称它们不相交。

PROPOSITION 1.2.1. S_n 中的每个元素都是若干不相交轮换的乘积。

PROOF. 设 $\sigma \neq e$。取 $i_1 \in \{1, 2, \cdots, n\}$，使得 $\sigma(i_1) = i_2 \neq i_1$。由于 σ 的阶有限，存在一个整数 $m \geq 2$，使得 $\sigma^m(i_1) = i_1$。设 m 是满足 $\sigma^m(i_1) = i_1$的最小正整数。我们得到一个 m-轮换 $(i_1\, i_2\, \cdots\, i_m)$，其中当 $2 \leq k \leq m$时，$i_k = \sigma^{k-1}(i_1)$。对$\{1, 2, \cdots, n\} \setminus \{i_1, i_2, \cdots, i_m\}$重复这一过程。这样可能会得到另一个轮换。于是，$\sigma$ 是上述过程中得到的所有轮换的乘积，且这些轮换彼此不相交。□

LEMMA 1.2.2. 对于互不相同的 $i_1, i_2, \cdots, i_m, k, j_1, j_2, \cdots, j_l$，

$$(i_1\, i_2\, \cdots\, i_m\, k)(k\, j_1\, j_2\, \cdots\, j_l) = (i_1\, i_2\, \cdots\, i_m\, k\, j_1\, j_2\, \cdots\, j_l).$$

验证这个引理是显而易见的 rd.

THEOREM 1.2.1. S_n 中的每个元素都是若干对换的乘积。

PROOF. 只需证明每个 m-轮换都是若干对换的乘积。由引理 1.2.2，得

$$\begin{aligned}(i_1\, i_2\, \cdots\, i_m) &= (i_1\, i_2)(i_2\, i_3\, \cdots\, i_m) = (i_1\, i_2)(i_2\, i_3)(i_3\, \cdots\, i_m) \\ &= (i_1\, i_2)(i_2\, i_3)\cdots(i_{m-1}\, i_m).\end{aligned}$$

□

将 σ 中 S_n 的一个元素表示为若干对换的乘积，称为将 σ 分解为对换。S_n 中的一个元素可能有不同的对换分解。例如在 S_4中，$(1\ 2\ 3) = (1\ 2)(2\ 3) = (1\ 2\ 3\ 4)(3\ 4) = (4\ 1\ 2\ 3)(3\ 4) = (4\ 1)(1\ 2)(2\ 3)(3\ 4)$。然而，所有分解的奇偶性相同。也就是说，如果一个分解是偶数（奇数）个对换的乘积，那么任何其他分解也都是偶数（奇数）个对换的乘积。

我们将在本节剩余部分证明这一点。

设 G 和 H 是群。群**同态** $f\colon G \to H$ 是满足条件 $f(xy) = f(x)f(y)$ 的映射，其中对所有 x，$y \in G$都成立。双射群同态称为**同构**。

将 $\mathbb{R}^n = \mathbb{R}^{n\times 1}$ 的标准基记为 $\{e_i\}_{i=1}^n$。对于 $\sigma \in S_n$，$n \times n$置换矩阵 E_σ 定义为 $E_\sigma = (e_{\sigma(1)}\, e_{\sigma(2)} \cdots e_{\sigma(n)})$。置换矩阵的集合 P_n 在矩阵乘法下构成一个群。于是定义从 S_n 到 P_n 的映射 Φ，其中对于每个 $\sigma \in S_n$，有 $\Phi(\sigma) = E_{\sigma^{-1}}$。可以验证，$\Phi$ 是一个群同构。

行列式映射 det 是从 P_n 到乘法群 $\{\pm 1\}$ 的群同态。因此，$\det\cdot\Phi$ 是从 S_n 到 $\{\pm 1\}$ 的群同态，并且 $sgn(\sigma) = \det(\Phi(\sigma))$。

设 $\sigma = \tau_1\tau_2\cdots\tau_k = \tau_1'\tau_2'\cdots\tau_l'$，其中 τ_i 和 τ_j' 是对换。那么

$$\begin{aligned}\det\Phi(\sigma) &= \det\Phi(\tau_1)\det\Phi(\tau_2)\cdots\det\Phi(\tau_k) = (-1)^k \\ &= \det\Phi(\tau_1')\det\Phi(\tau_2')\cdots\det\Phi(\tau_l') = (-1)^l.\end{aligned}$$

因此 $k-l$ 是偶数。所以置换的符号是良定义的。

Definition 1.2.1. n 次交错群 A_n 由 S_n 中那些可分解为偶数个对换之积的元素组成。

1.3. 群的构造

本节将介绍如何从已知群构造一些新的群。

1.3.1. 商群。 如果群 G 的子群 N 满足对每个 x（属于 G），$xN = Nx$，则称其为**正规**。记作 $N \trianglelefteq G$。定义 G/N 为 G中 N 的所有左陪集组成的集合。

Theorem 1.3.1。 若 $N \trianglelefteq G,$，则 G/N 在由$xN\cdot yN = xyN$给出的运算下构成一个群，其中 x、y属于 G。我们称 G/N为模 N的商群 G。

Proof. 首先，我们验证 $xN\cdot yN = xyN$ 是良定义的。也就是说，如果 $x_1N = x_2N$ 且 $y_1N = y_2N$，那么 $x_1y_1N = x_2y_2N$。这是因为，由于 N 的正规性，$(x_1y_1)^{-1}x_2y_2 = y_1^{-1}x_1^{-1}x_2y_2 = (y_1^{-1}y_2)(y_2^{-1}(x_1^{-1}x_2)y_2)$ 属于 N。

此外

- G/N 在二元运算下封闭；
- G/N 上的二元运算满足结合律；
- G/N 的单位元是 N；
- xN 的逆元是 $x^{-1}N$。

□

我们将映射 $\pi : G \to G/N$ given by $\pi(x) = xN$ for all x in G 称为**商映射**。

事实上，$\mathbb{Z}/n\mathbb{Z}$ 是 $\mathbb{Z}$ 模 $n\mathbb{Z}$所得的群。

设 $f\colon G \to H$是一个群同态。集合 $\{x \in G \mid f(x) = e\}$ 称为 f的**核**，记作 $\ker f$。集合 $\{f(x) \mid x \in G\}$ 称为 f的**像**，记作 $\mathrm{im} f$。因此，$\ker f$是 G的正规子群，而 $\mathrm{im} f$ 是 H的子群。

从 G到自身的群同构称为 G的**自同构**。如果群 G和 H之间存在同构，我们就称 G与 H同构。记作 $G \cong H$。

REMARK 1.3.1. 事实上，对于群 G，子群 N 是正规子群，当且仅当存在群同态 $f: G \to H$，使得 $N = \ker f$。

EXAMPLES 1.3.1.

(1) $G/G \cong 1$ 和 $G/1 \cong G$。(2) 商群 $\mathbb{R}/\mathbb{Z}$；(3) 对于正整数 n，商群 $\mathbb{Z}/n\mathbb{Z}$ 。

1.3.2. 群的直和与直积。

假设 $\{G_i\}_{i\in I}$ 是一族群，记作 $\Pi_{i\in I}G_i$，是集合 $\{(x_i)_{i\in I} \mid x_i \in G_i$，对每个 $i \in I\}$，其二元运算为 $(x_i)(y_i) = (x_iy_i)$，其中 (x_i)，(y_i) 属于 $\Pi_{i\in I}G_i$。G_i 的直积，记作 $\bigoplus_{i\in I} G_i$，由 $\Pi_{i\in I}G_i$ 中满足如下条件的元素 $(x_i)_{i\in I}$ 组成：对于 I 中除有限多个以外的所有 i，$x_i = e$；并且 $\bigoplus_{i\in I} G_i$ 上的二元运算与 $\Pi_{i\in I}G_i$ 上的相同。

群的直积和直和产生许多有趣的群。例如，$\bigoplus_{n=1}^{\infty} \mathbb{Z}/n\mathbb{Z}$ 这是一个无限群，其中每个元素都是有限阶的，且每个正整数都是某个元素的阶。

1.4. 同构定理

本节陈述并证明群的同构定理。

THEOREM 1.4.1（第一同构定理）。

设 $f: G \to H$ 是一个群同态。那么 $\ker f$ 是 G的一个正规子群，f的像 Imf 是 H 的一个子群，并且

$$G/\ker f \cong Imf.$$

PROOF. $\ker f \trianglelefteq G$ 和 $\mathrm{Im} f \leq H$ 的验证留作习题。

定义一个映射 $\tilde{f}: G/\ker f \to \mathrm{Im} f$ 通过

$$\tilde{f}(x \ker f) = f(x)$$

对每个 x属于 G。

容易验证

- $\tilde{f}$ 是良定义的群同态；
- f 是满射；
- f 是单射。

□

THEOREM 1.4.2（第二同构定理）。

设 H 是群 G 的子群，且 K 是 G 的正规子群。那么

(1) $HK = KH$，且 HK 是 G 的子群。(2) $H \cap K$ 是 H 的正规子群。(3) $HK/K \cong H/(H \cap K)$。

PROOF.

(1) 对于 h 属于 H 且 k 属于 K，有 $hk = hkh^{-1}h$ 属于 KH。因此 $HK \subseteq KH$。此外，$kh = hh^{-1}kh$ 属于 HK。所以 $KH \subseteq HK$。因此 $HK = KH$。

集合 HK 包含 G 的单位元。对于 h 属于 H 且 k 属于 K，元素 $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}hk^{-1}h^{-1}$ 属于 HK，因为 K 的正规性意味着 $hk^{-1}h^{-1}$ 属于 K。此外，对于 h_1，h_2 属于 H 且 k_1，k_2 属于 K，有 $h_1k_1h_2k_2 = h_1h_2(h_2^{-1}k_1h_2)k_2$ 属于 HK，这是由 K 的正规性得出的。因此 HK 是 G 的子群。

(2) 集合 $H \cap K$ 是 H 的子群。我们只需证明 $H \cap K$ 是 H 中的正规子群。对于任意 $h \in H$ 以及任意 $k \in H \cap K$，由于 K 是 G 中的正规子群，因此 $hkh^{-1} \in H \cap K$。

(3) 定义 $f\colon HK/K \to H/H \cap K$，令 $f(hkK) = hH \cap K$，其中任意 $h \in H$ 且 $k \in K$。

映射 f 是良定义的，因为若 $h_1k_1K = h_2k_2K$，则 $h_1K = h_2K$。因此 $h_1h_2^{-1} \in K$。于是 $h_1h_2^{-1} \in H \cap K$。这说明 $h_1H \cap K = h_2H \cap K$。

注意 $h_1k_1Kh_2k_2K = h_1Kh_2K = h_1h_2K$。最后一个等式是因为 K 是正规子群。因此

$$\begin{aligned} f(h_1k_1Kh_2k_2K) &= f(h_1h_2K) = h_1h_2H \cap K \\ &= (h_1H \cap K)(h_2H \cap K) = f(h_1k_1K)f(h_2k_2K). \end{aligned}$$

因此 f 是一个同态。

显然，f 是满射。若 h 属于 $H \cap K$，则有 $hkK = K$。因此，f 是单射。

□

对于 $G = \mathbb{Z}$，考虑 $H = m\mathbb{Z}$ 和 $K = n\mathbb{Z}$。则 $H + K =$ 最大公因式$(m, n)\mathbb{Z}$ 以及$H \cap K =$ 最小公倍数$(m, n)\mathbb{Z}$。由定理 1.4.2，我们有

$$\gcd(m,n)\mathbb{Z}/n\mathbb{Z} \cong m\mathbb{Z}/\mathrm{lcm}(m,n)\mathbb{Z}.$$

THEOREM 1.4.3（第三同构定理）。

若 $S \subseteq K$ 是群 G的正规子群，则

$$G/S/K/S \cong G/K.$$

PROOF. 定义一个映射 f，从 G/S 到 G/K，其定义为 $f(xS) = xK$，对 x 中的所有 G均成立。

映射 f 良定义，因为 $S \subseteq K$。

由于 S 和 K 是 G的正规子群，因此对所有 x，y属于 G，都有 $f(xSyS) = f(xyS) = xyK = xKyK = f(xS)f(yS)$。所以 f是一个同态。此外，f是满射。

注意，$\ker f = K/S$。应用第一同构定理，证明得证。

□

1.5. 群作用

本节中，我们介绍集合上的群作用，并将其作为证明 Sylow定理的工具。Sylow定理是有限群论中的一个基本定理 [Syl]。

DEFINITION 1.5.1. 若存在一个映射$\alpha\colon G \times X \to X$，将 (g, x) 映到 $\alpha_g(x)$，对所有 g属于 G 且 x 属于 X 均成立，并满足以下条件，则称群 G 作用在集合 X 上：

(1) 对所有 x 属于 X，$\alpha_e(x) = x$；(2) 对所有 g，h 属于 G 且 x 属于 X，$\alpha_{gh}(x) = \alpha_g(\alpha_h(x))$。

映射 α 称为 G 在 X 上的**作用**。用 $G \overset{\alpha}{\curvearrowright} X$ 表示群作用。

群 G 可以作用于集合 X，使得每个群元素都是 X上的恒等映射。此外，群还可以通过左平移作用于自身。

对于 X中的每个 x， x的**轨道** 记作 $\mathcal{O}_x$，是集合 $\{\alpha_g(x)\,|g\in G\}$。 x的**稳定子** 记作 G_x，是集合 $\{g\in G\,|\,\alpha_g(x)=x\}$。

若存在 $g\in G$，使得 $b=gag^{-1}$，则称 G中的 a 和 b **共轭**。集合 $C_a=\{gag^{-1}|\,g\in G\}$ 称为 a的**共轭类**。

下面列出轨道的一些性质，其证明留作习题。

PROPOSITION 1.5.1. 考虑一个群作用 $G\overset{\alpha}{\curvearrowright}X$。以下结论成立：

(1) 任意两个轨道要么不相交，要么相同。因此， X 是轨道的不交并。(2) 对于任意 G中的 x，稳定子 G_x 是 G的子群。(3) 对于任意 X中的 x，作为集合， $G/G_x\cong\mathcal{O}_x$，因此当 G 有限时， $|\mathcal{O}_x|$ 整除 $|G|$。

REMARKS 1.5.1.

- G 在 X 上的每个群作用都对应一个群同态 $\Phi: G\to S_X$，其定义为对所有 G 中的 g， $\Phi(g)=\alpha_g$。
- 命题 1.5.1(3) 称为**轨道-稳定子定理**。

下面介绍一种特别重要的群作用。

由 $\alpha_g(a)=gag^{-1}$ 定义的 G 在 G 上的群作用 α，其中 g,a 属于 G，称为 G [1]的**内自同构**作用。 a 的共轭类 C_a 是 a 在 G 的内自同构作用下的轨道 $\mathcal{O}_a$。 a 的稳定子称为 a 的**中心化子**或**换位子**，记作 $C_G(a)$。也就是说

$$C_G(a)=\{g\in G\,|\,gag^{-1}=a\}=\{g\in G\,|\,ga=ag\}.$$

G 的**圆心** $Z(G)$ 是所有 $C_G(a)$ 的交集。换句话说，对于所有 $a\,in\,G\}$，都有 $Z(G)=\{g\in G\,|\,ga=ag$。

当 G 是有限群时，由命题 1.5.1(3) 可得 $|C_a||C_G(a)|=|G|$。

设 G 是有限群， $|G|$ 的一个素因子为 p，且 $|G|=p^km$ 满足 p，并且 m 与其互素。若子群 H 是 G 的子群，且满足 $|H|=p^k$，则称其为 G 的**Sylow p-子群**；若子群 K 是 G 的子群，且满足 $|K|=p^l$，并且 $l\le k$，则称其为 G 的 **p-子群**。

以下关于 Sylow定理 部分内容的证明归功于 H. Wielandt。 [Wie59]

THEOREM 1.5.1. *[Sylow定理，第I部分*

有限群 G 具有一个 *Sylow* p-子群。

PROOF. 设 X 为 G 的含有 p^k 个元素的子集所组成的集合。群 G作用在 X 上，作用定义为：对 G 中的任意 g 和 X中的任意 A，有 $\alpha_g(A)=gA$。注意， $|X|=\binom{p^km}{p^k}$。因此， $p\nmid\binom{p^km}{p^k}$。集合 X 是不相交轨道的并集，所以存在 X 中的 B，使得 $p\nmid|\mathcal{O}_B|$。

接下来我们证明 $|G_B|=p^k$。

注意， $|\mathcal{O}_B|$ 整除 $|G|$ 和 $p\nmid|\mathcal{O}_B|$，因此 $|\mathcal{O}_B|$ 整除 m。由 $G/G_B\cong\mathcal{O}_B$可知， p^k 整除 $|G_B|$。特别地， $p^k\le|G_B|$。

此外，固定 b 属于 B。可以定义一个映射 φ： $G_B\to B$，其定义为 $\varphi(g)=gh$ 对所有 g属于 G_B成立。映射 φ 是一个良定义的单射。因此 $|G_B|\le|B|=p^k$。□

[1]映射 α_g： $G\to G$ 由 $\alpha_g(a)=gag^{-1}$ 对所有 a 属于 G 均成立，是一个称为内自同构的同构。

COROLLARY 1.5.1. （柯西）
如果素数 p 整除 $|G|$，那么 G 有一个阶为 p 的元素。

PROOF. 设 H 是 G 的一个 Sylow p-子群。则 $\mathrm{Ord}_h = p^l$，且对于每个属于 H 的 $h \neq e$， p^l 都整除 $|G|$。因此 $\mathrm{Ord}_{h^{p^{l-1}}} = p$。□

1.6. A_n 的简单性

注意，交错群 A_4 是简单群，因为

$$\{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \trianglelefteq A_4.$$

然而，当 $n \geq 5$ 时， A_n 是简单群。这一事实是本节的主定理，对于证明阿贝尔–鲁菲尼定理至关重要，也就是说，多项式$x^5 - 80x + 5$ 根式不可解。

THEOREM 1.6.1. A_n 对所有 $n \geq 5$ 都是单群。

定理 1.6.1 的证明分为两步：
步骤 1. A_5 是单群；
步骤 2. 对于 $n \geq 5$，通过假设 A_n 是单群，我们证明 A_{n+1} 是单群。

我们需要一些预备知识。

LEMMA 1.6.1. </style]如果 $(i_1\, i_2\, \cdots\, i_m)$ 是 S_n 中的一个 m-轮换，那么 γ 的一个共轭元，例如 $\sigma\gamma\sigma^{-1}$，是一个形如 $(\sigma(i_1)\, \sigma(i_2)\, \cdots\, \sigma(i_m))$ 的 m-轮换。

PROOF. 首先，对所有 $1 \leq k \leq m$，有 $\sigma\gamma\sigma^{-1}(\sigma(i_k)) = \sigma(i_{k+1})$。[2]
如果 $j \notin \{\sigma(i_1)\ \sigma(i_2)\ \cdots,\ \sigma(i_m)\}$，那么存在 $i \notin \{i_k\}_{k=1}^m$，使得 $j = \sigma(i)$。由此可得，$\sigma\gamma\sigma^{-1}(j) = \sigma\gamma\sigma^{-1}(\sigma(i)) = \sigma\gamma(i) = \sigma(i) = j$。
因此， $\sigma\gamma\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \cdots\, \sigma(i_m))$。 □

LEMMA 1.6.2. 交错群 A_n 由 3-循环生成。

PROOF. 只需证明两个对换的乘积可以表示为 3-循环的乘积。

有两种情况。
情形 1：$(a\,b)(a\,c) = (a\,c\,b)$。
情形 2：$(a\,b)(c\,d) = (a\,b)(b\,c)(b\,c)(c\,d) = (a\,b\,c)(b\,c\,d)$。 □

LEMMA 1.6.3. 若 A_n 的正规子群 H 含有一个 3-循环，则 H 包含所有 3-循环。因此 $H = A_n$。

PROOF. 假设 $\sigma = (a\,b\,c)$ 属于 H。
假设 $\gamma = (d\,e\,f)$，且 $\{d, e, f\} \cap \{a, b, c\} = \emptyset$。这只有在$n \geq 6$时才会发生。设 $\tau = (a\,d\,b\,e)(c\,f)$。那么 τ 属于 A_n，而 $\gamma = \tau\sigma\tau^{-1}$ 属于 H。
假设 $\gamma = (a\,e\,f)$，且 $\{e, f\} \cap \{b, c\} = \emptyset$。这只有在$n \geq 5$时才会发生。设 $\tau = (b\,e)(c\,f)$。那么 τ 属于 A_n，而 $\gamma = \tau\sigma\tau^{-1}$ 属于 H。
假设 $\gamma = (a\,b\,f)$，且满足 $c \neq f$。这只会在 $n \geq 4$ 时发生。令$\tau = (a\,b)(c\,f)$。那么 τ属于 A_n，而 $\gamma = \tau\sigma^2\tau^{-1}$属于 H。此外，$(a\,f\,b) = \gamma^2$属于 H。假设 $\gamma = (a\,c\,b)$。那么 $\gamma = \sigma^2$属于 H。

上述讨论涵盖了所有不同于 σ的3-循环可能性。

□

现在我们证明定理 1.6.1 的第 1 步。

[2]这里将 i_{m+1} 理解为 i_1。

PROPOSITION 1.6.1. A_5 是单群。

PROOF. 假设 $H \neq 1$ 是 A_5的正规子群。我们要证明$H = A_5$。根据引理 1.6.2，如果 H 包含所有 3-循环，这个结论就成立。根据引理 1.6.1，由于 H 是正规子群，只需证明 H 包含一个 3- 循环。

取 $\sigma \neq e$ 属于 H。

不失一般性， σ有以下三种情形。

情形 1： $\sigma = (1\,2\,3)$。若如此，则得证。

情形 2： $\sigma = (1\,2)(3\,4)$。取 $\tau = (1\,2)(4\,5)$。那么 $\tau\sigma\tau^{-1}\sigma$属于 H，因为 τ属于A_5。注意

$$\tau\sigma\tau^{-1}\sigma = (\tau(1)\,\tau(2))(\tau(3)\,\tau(4))(1\,2)(3\,4) = (1\,2)(3\,5)(1\,2)(3\,4) = (3\,5)(3\,4) = (5\,3\,4).$$

因此 H 也包含一个 3-循环。

情形 3： $\sigma = (1\,2\,3\,4\,5)$。取 $\tau = (2\,3\,4)$。那么 $\tau\sigma\tau^{-1}\sigma^{-1}$属于 H，因为 τ是 A_5。此外

$$\tau\sigma\tau^{-1}\sigma^{-1} = (\tau(1)\,\tau(2)\,\tau(3)\,\tau(4)\,\tau(5))\sigma^{-1} = (1\,3\,4\,2\,5)(1\,5\,4\,3\,2) = (2\,3\,5).$$

在这种情形下， H 包含一个 3-循环。 □

现在可以证明定理 1.6.1 了。

PROOF. [定理 1.6.1] 的证明

假设 A_{n-1} 是单群。我们将证明 A_n 是单群。

将 A_n 记作 G。那么 G 作用在 $X = \{1, 2, \cdots, n\}$上。

假设 H 是 G 的正规子群，且 $1 \subsetneq H$。

首先证明存在 $\sigma \neq \tau$ 属于 H，使得对于某个 i 属于 X，有 $\sigma(i) = \tau(i)$。

取一个非单位元 σ 属于 H。由于 σ 是不相交轮换的乘积， σ 有两种可能的形式。

1. σ 的分解中有一个 m-轮换 $(i_1\,i_2\,i_3\,\cdots\,i_m)$，且 $m \geq 3$ 属于其中。

在这种情况下，令 $\gamma = (i_3\,i_4\,i_5)$，其中 $i_4 \notin \{i_1, i_2, i_3\}$。那么 $\tau = \gamma\sigma\gamma^{-1}$ 属于 H 因为 γ 属于 A_n，并且

$$\tau = (\gamma(i_1)\,\gamma(i_2)\,\gamma(i_3)\,\cdots\,\gamma(i_m))\cdots = (i_1\,i_2\,i_4\,\cdots\,\gamma(i_m))\cdots.$$

注意， $\tau \neq \sigma$因为 $\tau(i_2) = i_4$且 $\sigma(i_2) = i_3$。然而 $\tau(i_1) = i_2 = \sigma(i_1)$。。。

2. σ 是由互不相交的对换构成的乘积，即 $\sigma = (i_1\,i_2)(i_3\,i_4)$

在这种情况下，令 $\gamma = (i_1\,i_2)(i_4\,i_5)$，其中 $i_5 \notin \{i_1, i_2, i_3, i_4\}$。那么 $\tau = \gamma\sigma\gamma^{-1}$ 属于H，因为 γ 属于 A_5，并且

$$\tau = (\gamma(i_1)\,\gamma(i_2))(\gamma(i_3)\,\gamma(i_4))\cdots = (i_1\,i_2)(i_3\,i_5)\cdots.$$

由 $\tau(i_3) = i_5$ 和 $\sigma(i_3) = i_4$ 可知 $\tau \neq \sigma$。但是 $\tau(i_1) = i_2 = \sigma(i_1)$。

因此，存在一个非单位元 σ 属于 H，使得对于某个 i 属于 X， $\sigma(i) = i$。

G_i 的稳定子 i 同构于 A_{n-1}，因此根据假设， G_i 是单群。此外， $G_i \cap H$是 G_i和 $G_i \cap H \neq 1$的正规子群。因此 $G_i \cap H = G_i$，这意味着 $G_i \subset H$。于是 H 包含一个 3-循环，因此 H 包含所有 3-循环。所以 $H = G$，由引理 1.6.2 得。□

1.7. 可解群

本节将研究可解群的概念，也就是对可解多项式的群论描述。

Definition 1.7.1. 若存在由 $\{G_i\}_{i=0}^n$ 构成的子群列 G ，使得.....，则称群 G **可解**。

$$1 = G_n \lhd G_{n-1} \lhd G_2 \cdots G_1 \lhd G_0 = G,$$

并且 G_i 是 G_{i-1} 的正规子群，且对于每个 $1 \leq i \leq n$， G_{i-1}/G_i 都是阿贝尔群。我们称 $\{G_i\}_{i=0}^n$ 为 G的**可解列**。

根据定义，我们立即得到以下结论。

Proposition 1.7.1. 可解群的子群也是可解群。因此，如果一个群包含不可解子群，那么该群本身也是不可解的。

Examples 1.7.1. [可解群的例子与反例]

(1) 每个阿贝尔群都是可解群。(2) 对于 $n \leq 4$， S_n 是可解的。令 $H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$。那么 H 是 S_4 的正规子群，因为对于 S_4中的每个 σ ，都有 $\sigma(a\,b)(c\,d)\sigma^{-1} = (\sigma(a)\,\sigma(b))(\sigma(c)\ \sigma(d))$ 。此外， $1 \lhd H \lhd A_4 \lhd S_4$ 是 S_4的可解列。(3) 每个非阿贝尔单群都是不可解的。因此，当 $n \geq 5$时， A_n 和 S_n都是不可解的。

Definition 1.7.2. 群的**交换子子群**是由元素 $[a,b] = ab(ba)^{-1}$ （其中 a, b 属于 G）生成的子群。将 G 的交换子子群记为 $[G,G]$。

交换子子群 $[G,G]$ 是 G 的最小正规子群，使得其商群是阿贝尔群。更准确地说，以下结论成立。

Theorem 1.7.1. 交换子子群 $[G,G]$ 是 G的正规子群，且 $G/[G,G]$ 是阿贝尔群。此外，若 H 是 G 的正规子群，且 G/H是阿贝尔群，则 $[G,G]$ 是 H的子群。

Proof. 对于所有属于 G的 a, b, c ，都有 $c[a,b]c^{-1} = [cac^{-1}, cbc^{-1}]$。因此 $[G,G]$ 是正规子群。

此外，若 H 是 G 的正规子群，且 G/H 是阿贝尔群，那么对于所有属于G的 a, b ，都有 $abH = baH$，这意味着 $[a,b]$ 属于 H。因此 H 包含 $[G,G]$。 □

记 $[G,G]$ 为 $G^{(1)}$ ，并记 $G^{(n)}$ 的交换子子群为 $G^{(n+1)}$ ，其中$n \geq 1$。

Theorem 1.7.2. *G is solvable iff $G^{(n)} = 1$ for some $n \geq 1$.*

Proof. 假设对于某个 $n \geq 1$，有 $G^{(n)} = 1$ 。

Then

$$1 = G^{(n)} \lhd G^{(n-1)} \lhd \cdots \lhd G^{(1)} \lhd G = G^{(0)}.$$

注意，对于所有 $1 \leq i \leq n$， $G^{(i-1)}/G^{(i)}$ 都是阿贝尔群，因此 G 是可解群。

反过来，假设 G 是可解群。

那么存在 G 的子群序列 $\{G_i\}_{i=1}^n$ ，使得

$$1 = G_n \lhd G_{n-1} \lhd G_{n-2} \lhd \cdots G_1 \lhd G_0 = G,$$

并且对于每个 $1 \leq i \leq n$， G_{i-1}/G_i 都是阿贝尔群。

由于 G_0/G_1 是阿贝尔群，根据定理 1.7.1，有 $G^{(1)} \leq G_1$。

所以 $G^{(2)} = [G^{(1)}, G^{(1)}] \leq [G_1, G_1] \lhd G_2$。归纳地， $G^{(n)} \leq G_n = 1$。

□

使得 $G^{(n)} = 1$ 对于可解群 G 成立的最小 n，称为 G 的**导出长度**。

本节最后介绍可解群的一些进一步性质。

PROPOSITION 1.7.2.

(1) 若 G 是可解群，且 N 是 G的正规子群，则 G/N 是可解群。(2)设 N 是 G的正规子群。若 N 是可解群且 G/N 是可解群，则 G 是可解群。

PROOF. **(1)** 设 $\{G_i\}_{i=0}^n$ 是 G 的一个子群列，满足

$$1 = G_n \lhd G_{n-1} \lhd G_{n-2} \lhd \cdots G_1 \lhd G_0 = G,$$

且对每个 $1 \le i \le n$， G_{i-1}/G_i 都是阿贝尔群。

令 $\pi : G \to G/N$ 为商映射。则 $\{\pi(G_iN)\}_{i=0}^n$ 是 G/N的一个可解列。

(2) 设 $\{\tilde{G}_i\}_{i=0}^m$ 是 G/N 的可解列，且 $\{N_j\}_{j=0}^k$ 是 N的可解列。则有如下可解列:

$$1 = N_k \lhd \cdots \lhd N_0 = N = \pi^{-1}(\tilde{G}_m) \lhd \pi^{-1}(\tilde{G}_{m-1}) \lhd \cdots \lhd \pi^{-1}(\tilde{G}_1) \lhd \pi^{-1}(\tilde{G}_0) = G,$$

其中 $\pi^{-1}(\tilde{G}_j)$ 是 $\tilde{G}_j$ 在商映射 $\pi : G \to G/N$ 下的原像（$0 \le j \le m$时）。 □

习题

EXERCISE 1.1. 证明 $\mathbb{Z}$ 的每个子群都是某个 $n \ge 0$。

EXERCISE 1.2. 在 $\mathbb{R} \setminus \{-1\}$ 上定义二元运算 $*$：对 $a, b \in \mathbb{R} \setminus \{-1\}$，有 $a * b = ab + a + b$。证明$(\mathbb{R} \setminus \{-1\}, *)$是一个群。

EXERCISE 1.3. 假设对每个 $\alpha \in \Lambda$， G_α 都是 X 的子集且是一个群。证明交集 $\bigcap_{\alpha\in\Lambda} G_\alpha$ 也是一个子群。并集 $\bigcup_{\alpha\in\Lambda} G_\alpha$ 又如何呢?

EXERCISE 1.4. 给出一个从正数乘法群 $\mathbb{R}^+$ 到实数加法群 $\mathbb{R}$ 的群同态。

EXERCISE 1.5. 设 a 和 b 属于群 G，且 阶$_a = m$ 和 阶$_b = n$。若 $ab = ba$，我们能对 阶$_{ab}$ 得出什么结论? 若 $ab \ne ba$，又会怎样?

EXERCISE 1.6. 证明：对于群 G 中的 a、 b ，阶$_{ab}$ = 阶$_{ba}$ 。

EXERCISE 1.7. 设 a 属于群 G ，且 阶$_a = n$。求$1 \le m \le n$ 时 阶$_{a^m}$ 。

EXERCISE 1.8. 证明费马小定理：若素数 p不能整除a，则 $a^{p-1} \equiv 1$ 模 p。

EXERCISE 1.9. 证明：子群 K 是 G 的正规子群，当且仅当存在群同态 $f\colon G \to H$，使得 $K =$核 f。

EXERCISE 1.10. 证明 $Z(G)$是 G的正规子群。

EXERCISE 1.11. 循环群的子群是循环群。

EXERCISE 1.12. 证明中国余式定理：若 m和 n是互素正整数，则 $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$。

EXERCISE 1.13. 写出从 $\mathbb{Z}$ 到 $\mathbb{Z}$的所有群同态。

EXERCISE 1.14. 写出从单位圆 $\mathbb{S}$到其自身的所有群同态。

EXERCISE 1.15. 列出 S_3 的所有子群，并找出其中的正规子群。

EXERCISE 1.16. 证明，对每个群 G，都存在一个集合 X，使得 G同构于对称群 S_X 的一个子群。特别地，每个有限群都同构于某个 $n \geq 1$对应的 S_n 的一个子群。（提示：取 $X = G$。）

EXERCISE 1.17. *Prove that* $\bigoplus_{i\in I} G_i$ *is a normal subgroup of* $\Pi_{i\in I} G_i$.

EXERCISE 1.18. 证明，一个*5*-循环和一个*2*-循环生成 S_5。

EXERCISE 1.19. 证明，对于 $n \geq 5$， A_n 由*5*-循环生成。

EXERCISE 1.20. 证明 $\mathbb{Q}$ 不是有限生成的。

EXERCISE 1.21. 设 $\sigma = (i_1\, i_2\, \cdots\, i_m)$ 是 S_n中的一个 m-轮换。证明 σ^k是 $gcd(m,k)$ 个 $^{m}\,_{\gcd(m,k)}$-轮换的乘积。

EXERCISE 1.22. 证明，商群 G/N 的每个子群 H 都由 G 的一个子群 H 给出，使得 $N \leq H$ 且 $H = \pi(H)$，其中 $\pi : G \to G/N$是商映射。更确切地说，G/N 的子群集合与 G 中大于 N的子群集合之间存在一一对应。

EXERCISE 1.23. 设 N 是 G的正规子群。$G \cong N \times G/N$是否成立？

EXERCISE 1.24. 设 M和 N是 G和 $G = MN$的正规子群。证明 $G/(M \cap N) \cong G/M \times G/N$。应用这一点证明，当 m和 n 互素时， $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ 。

EXERCISE 1.25. 证明 $SL_n(\mathbb{R})$ 是 $GL_n(\mathbb{R})$的正规子群，并且 $GL_n(\mathbb{R})/SL_n(\mathbb{R})$ 同构于 $\mathbb{R}^\times$。

EXERCISE 1.26. 考虑 $GL_n(\mathbb{R})$ 在 $\mathbb{R}^n$ 上的作用，其定义为：当 A 属于 $GL_n(\mathbb{R})$ 且 x 属于 $\mathbb{R}^n$时， $\alpha_A(x) = Ax$。求 x 属于 $\mathbb{R}^n$时的 $\mathcal{O}_x$ 。

EXERCISE 1.27. 假设 p是素数，且 m与 p互素。证明 p 与 $\binom{p^k m}{p^k}$互素。

EXERCISE 1.28. 对于 $n \geq 5$，假设 S_n 的一个正规子群 H 满足$H \cap A_n = 1$。关于 H，我们能得出什么结论？

EXERCISE 1.29. 证明非阿贝尔单群不可解。

EXERCISE 1.30. 证明对于 $n \geq 3$， A_n 是 S_n的交换子子群。

EXERCISE 1.31. 补全命题 *1.7.2* 证明中的细节。

EXERCISE 1.32. 证明有限群 G 可解，当且仅当存在 G 的子群序列 $\{G_i\}_{i=1}^n$，使得

$$1 = G_n \lhd G_{n-1} \lhd G_{n-2} \lhd \cdots G_1 \lhd G_0 = G,$$

并且对于每个 $1 \leq i \leq n$， G_{i-1}/G_i 都是循环的。

第2章

基础环论

环论与群论、域论是代数的支柱。直到 20 世纪第一个十年，人们才给出了环的抽象定义；同期，抽象环论在 E. Noether 和 E. Artin 的研究中逐渐形成，尽管一些特殊的环，例如多项式环和代数整数环，因其在数论和代数几何中的重要性，早已得到相当深入的研究。

本章重点讨论交换环论，特别是多项式环理论。

2.1 定义与例子

Definition 2.1.1. **环**是一个非空集合 R，并配备两个二元运算：加法“$+$”和乘法“$\cdot$”[1]，满足

(1) R 对这两个运算封闭。(2) $(R, +)$ 是阿贝尔群。(3) $(ab)c = a(bc)$ 对所有 $a, b, c \in R$ 成立。(4) $(a+b)c = ac + bc$ 且 $a(b+c) = ab + ac$ 对所有 $a, b, c \in R$ 成立。

如果对所有 a, b 均有 $ab = ba$，则称 R 为**交换环**。

如果 R 在乘法下有单位元，也就是说，存在 R 中的元素 1，使得$1a = a1 = a$ 对所有 a 均成立，则称 R 为**含幺环**。

如果环 R 是含幺环，且 $(R \setminus \{0\}, \cdot)$ 是阿贝尔群，则称 R 为**域**。

如果环 R 的一个子集本身是环，则称它为 R的**子环**。如果域 $\mathbb{F}$ 的一个子集本身是域，则称它为 $\mathbb{F}$的**子域**。

下面给出一些环的例子。

Examples 2.1.1.

(1) $\mathbb{Z}$、$\mathbb{Q}$、$\mathbb{R}$ 和 $\mathbb{C}$ 在数的加法与乘法下构成含幺交换环。此外，$\mathbb{Q}$、$\mathbb{R}$ 和 $\mathbb{C}$是域。(2) 对于 $n \geq 1$，$\mathbb{Z}/n\mathbb{Z}$ 在模 n的加法与乘法下构成含幺交换环。如果 p是素数，那么 $\mathbb{Z}/p\mathbb{Z}$ 是一个域，记作 $\mathbb{F}_p$。(3) $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ 在数的加法与乘法下构成含幺交换环。这个环称为**高斯整数环**，在数论中尤其受到关注。(4) 在矩阵加法与乘法下，$n \times n$ 阶实矩阵的集合 $\mathbf{M}_n(\mathbb{R})$ 是一个非交换含幺环。

[1]我们将 $a \cdot b$ 写作 ab，其中 a，b 属于 R。

$_n$(5) 含幺交换环 R 上的多项式集合 $R[x] = \{\sum a_i x^i =_{i=0} a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \,|\, a_i \in R$ 对所有 $0 \le i \le n\}$ 构成一个交换环，其加法与乘法定义为

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i$$

and

$$(\sum_{i=0}^{n} a_i x^i)(\sum_{j=0}^{m} b_j x^j) = \sum_{k=0}^{m+n} (\sum_{i=0}^{k} a_i b_{k-i}) x^k.$$

特殊情形包括 $\mathbb{Z}[x]$和 $\mathbb{F}[x]$ ，其中 $\mathbb{F}$是一个域。

环 R 中的元素 a 称为**单位**，如果存在 $b \in R$ 使得$ab = ba = 1$。元素 b 是唯一的，称为 a 的（乘法）逆元，记作 a^{-1}。将 R的单位群记为 $U(R)$。例如， $U(\mathbb{Z}) = \{\pm 1\}$以及 $U(\mathbf{M}_n(\mathbb{R})) = \mathbf{GL}_n(\mathbb{R})$。

交换环 R 中的非零元素 a 称为**零因子**，如果存在 R 中的非零元素 b 使得 $ab = 0$。

没有零因子的含幺交换环 R 称为**整环**。例如，域和 $\mathbb{Z}$是整环，而 $\mathbb{Z}/6\mathbb{Z}$ 不是整环。

THEOREM 2.1.1. 设 R 是一个含幺交换环。那么， R 是整环当且仅当 $R[x]$ 是整环。

PROOF. 假设 R 是一个整环。对于任意非零的 $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ 和 $g = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$（属于 $R[x]$），有 $fg \neq 0$，因为 $a_n b_m \neq 0$。

如果 $R[x]$ 是一个整环，那么 R 是 $R[x]$的含幺子环，因此也是一个整环。□

环 R 的非空子集 I 称为 R 的<tyle id='3'>理想，如果 I 是 R 的加法子群，并且对于每个属于 I 的 a 和属于 R的 b， ab 和 ba 都属于 I。R 的理想 I 称为真理想，如果 I 是 R的真子集。每个环 R 都有两个平凡理想：$\{0\}$、 R。

给定含幺交换环 R中的元素 a_1， a_2， $\cdots$， a_n，集合

$$\{\sum_{i=1}^{n} a_i b_i \,|\, b_i \in R \text{ for all } 1 \le i \le n\}$$

是 R 的一个理想，称为由 a_1、 a_2、 $\cdots$、 a_n 生成的理想。记作 $(a_1$、 $\cdots$、 $a_n)$。例如， $\mathbb{F}[x]$ 的子集 $I = \{\sum_{i=1}^{n} a_i x^i \,|\, a_i \in \mathbb{F}$（对所有 $1 \le i \le n\}$）是由多项式 x 生成的理想。稍后我们将证明， $\mathbb{F}[x]$ 的每个理想都由一个多项式生成。

设 I 和 J 是交换环 R的理想，则集合 $IJ = \{\sum_{i=1}^{n} a_i b_i \,|\, a_i \in I, b_i \in J\}$ 是 R的一个理想。

PROPOSITION 2.1.1. 如果环 R 的理想 I 含有一个单位，那么 $I = R$。

PROOF. 取 a 中的一个单位 I。 R 中的每个 b 都可以表示为 $b = b(a^{-1}a) = (ba^{-1})a$，因此属于 I。□

设 I 是环 R 的一个理想。定义集合 $R/I = \{a+I \mid a \in R\}$，在 R/I 上定义加法为 $(a+I)+(b+I) = a+b+I$，在 R/I 上定义乘法为 $(a+I)(b+I) = ab+I$，其中 a, b 属于 R。

THEOREM 2.1.2. R/I 是一个环。

PROOF. 若 $a_1+I = a_2+I$ 且 $b_1+I = b_2+I$，则 $a_1+b_1+I = a_2+b_2+I$，因为 $(a_1+b_1)-(a_2+b_2)$ 属于 I。因此，加法是良定义的。

此外，在加法下，R/I 是一个阿贝尔群：

- $(a+I)+(b+I) = a+b+I = b+a+I = (b+I)+(a+I)$.
- $((a+I)+(b+I))+c+I = (a+b)+c+I = a+(b+c)+I = a+I+((b+I)+(c+I))$.
- $(a+I)+I = a+0+I = I+(a+I)$.
- $(a+I)+(-a+I) = 0+I = I$.

若 $a+I = b+I$，则 $(a+I)(c+I) = ac+I = bc+I = (b+I)(c+I)$，因为 $ac-bc = (a-b)c$ 属于 I。因此，乘法是良定义的。

此外，我们还有如下结论：

- $((a+I)(b+I))(c+I) = (ab)c+I = a(bc)+I = (a+I)((b+I)(c+I))$.
- $((a+I)+(b+I))(c+I) = (a+b)c+I = (ac+I)+(bc+I) = (a+I)(c+I)+(b+I)(c+I)$.
- $(c+I)((a+I)+(b+I)) = c(a+b)+I = (ca+I)+(cb+I) = (c+I)(a+I)+(c+I)(b+I)$.

因此，R/I 在所定义的加法和乘法下是一个环。 □

R/I 称为 R 关于 I的**商环**。

环同态的定义与群同态类似。

DEFINITION 2.1.2. 若**环同态** φ：$R \to S$ 满足$\varphi(a+b) = \varphi(a)+\varphi(b)$且 $\varphi(ab) = \varphi(a)\varphi(b)$，则称其为环同态，其中任意 a, b 属于 R。

双射环同态称为**环同构**。

环同态 φ ： $R \to S$的**核**记为 $\ker\varphi$ ，是集合$\{a \in R \mid \varphi(a) = 0\}$。

与群论类似，环也有同构定理。

THEOREM 2.1.3. *[1*第一环同构定理*]*

设 $f\colon R \to S$ 是一个环同态。那么 $\ker f$ 是 R的一个理想，Imf是 S的一个子环，并且

$$R/\ker f \cong Imf.$$

第一同构定理的证明与第一群同构定理的证明类似。我们将其留作习题。

考虑由 $f(p) = p(0)$ 对所有 p 属于 $\mathbb{Z}[x]$定义的 $f\colon \mathbb{Z}[x] \to \mathbb{Z}$。那么 $\ker f = (x)$ 且 $\mathrm{Im}\, f = \mathbb{Z}$。第一同构定理表明 $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$。

THEOREM 2.1.4. *[2*第二环同构定理*]*

设 A 是 R 的一个子环，且 I 是 R的一个理想。那么 $A+I$ 是 R的一个子环，$A \cap I$ 是 A 的一个理想，并且

$$(A+I)/I \cong A/(A \cap I).$$

PROOF. 对于 a_1，a_2属于 A且 b_1，b_2属于 I的情况，有 $(a_1+b_1)+(a_2+b_2) = (a_1+a_2)+(b_1+b_2)$ 属于 $A+I$，而 $(a_1+b_1)(a_2+b_2) = a_1a_2+(b_1a_2+b_2a_1+b_1b_2)$ 属于 $A+I$。因此，$A+I$是 R的一个子环。

此外，对于任意属于 A 的 a 以及任意属于 $A\cap I$的 b，都有 ab 属于 $A\cap I$。因此，$A\cap I$ 是 A的一个理想。

定义 f: $A+I\to A/(A\cap I)$，其中 $f(a+b)=a+A\cap I$对所有 $a\in A$ 且 $b\in I$ 都成立。

- 若 $a_1+b_1=a_2+b_2$对 a_1，$a_2\in A$ 且 b_1，$b_2\in I$ 成立，则 $a_1-a_2=b_2-b_1$ 属于 $A\cap I$。因此 f 是良定义的。
- 对于 a_1，$a_2\in A$ 且 b_1，$b_2\in I$，$f((a_1+b_1)(a_2+b_2))=f(a_1a_2+a_1b_2+b_1(a_2+b_2))$ $=a_1a_2+A\cap I=f(a_1+b_1)f(a_2+b_2)$，因为 $a_1b_2+b_1(a_2+b_2)$属于 I，且 $f((a_1+b_1)+(a_2+b_2))$ $=f((a_1+a_2)+(b_1+b_2))=a_1+a_2+A\cap I=f(a_1+b_1)+f(a_2+b_2)$。因此 f 是一个环同态。
- f 是满射，因为对所有 a 属于 A，$f(a+0)=a+A\cap I$。
- 如果对 A 中的 a 和 I中的 b，$f(a+b)=0$，那么 a 属于 $A\cap I$，且 $a+b$ 属于 I。所以 $\ker f=I$。

由第一环同构定理，证明得证。 □

设 $R=\mathbb{Z}[x]$, $A=(x)$和 $I=(2)$。那么 $A+I=(x,\ 2)$，且 $A\cap I=(2x)$。第二环同构定理指出，$(x,\ 2)/(2)\cong(x)/(2x)$。

2.2. 整环的分式域

可以由一个整环定义出一个称为分式域的域。

设 R 是一个整环。定义 $R\times R$ 上的关系“$\sim$”如下：$(a,b)\sim(c,d)$ 当且仅当 $ad=bc$。

可以验证“$\sim$”是一个等价关系，也就是说，关系“$\sim$”满足

(1) $(a,b)\sim(a,b)$。(2) $(a,b)\sim(c,d)$ 蕴含 $(c,d)\sim(a,b)$。(3) $(a,b)\sim(c,d)$ 且 $(c,d)\sim(e,f)$ 蕴含 $(a,b)\sim(e,f)$。

对于 a,b，若 R 中有 $b\neq 0$，则用 ab^{-1} 表示 (a,b) 在 $R\times R$ 中的等价类，即，

$$ab^{-1}=\{(c,d)\in R\times R\,|\,(c,d)\sim(a,b)\}.$$

定义 Frac(R) 为 $R\times R$ 中等价类的集合。定义 Frac(R) 上的乘法和加法如下：$(ab^{-1})(cd^{-1})=ac\,(bd)^{-1}$ 和 $ab^{-1}+cd^{-1}=(ad+bc)(bd)^{-1}$。

THEOREM 2.2.1. 对于整环 R，集合 $Frac(R)$ 是一个域。

PROOF. 首先，我们验证 Frac(R) 上的加法和乘法是良定义的。

假设 $(a_1,b_1)\sim(a_2,b_2)$ 且 $(c_1,d_1)\sim(c_2,d_2)$。那么

$$(a_1c_1)(b_2d_2)=(a_1b_2)(c_1d_2)=(b_1a_2)(c_2d_1)=(a_2c_2)(b_1d_1).$$

也就是说，$(a_1c_1)(b_1d_1)^{-1}=(a_2c_2)(b_2d_2)^{-1}$。因此乘法是良定义的。此外

$$\begin{aligned}&(a_1d_1+b_1c_1)(b_2d_2)-(a_2d_2+b_2c_2)(b_1d_1)\\&=(a_1b_2d_1d_2+b_1b_2c_1d_2)-(a_2b_1d_2d_1+b_2b_1c_2d_1)\\&=(a_1b_2-a_2b_1)d_1d_2+b_1b_2(c_1d_2-c_2d_1)=0.\end{aligned}$$

也就是说，$(a_1d_1+b_1c_1)(b_1d_1)^{-1}=(a_2d_2+b_2c_2)(b_2d_2)^{-1}$。因此加法是良定义的。

此外，以下结论也成立：

- $ab^{-1}+cd^{-1}=(ad+bc)(bd)^{-1}=(cb+da)(db)^{-1}=cd^{-1}+ab^{-1}$.
- $(ab^{-1}+cd^{-1})+ef^{-1}=(ad+bc)(bd)^{-1}+ef^{-1}=(adf+bcf+bde)(bdf)^{-1}=ab^{-1}+(cf+de)(df)^{-1}=ab^{-1}+(cd^{-1}+ef^{-1})$.
- $ab^{-1}+0d^{-1}=(ad)(bd)^{-1}=ab^{-1}$，即 $0d^{-1}=0$ 属于 Frac(R)。
- $ab^{-1}+(-a)b^{-1}=0(b^2)^{-1}=0$.

因此，Frac(R) 在加法下是一个阿贝尔群。

注意， $ab^{-1}=0d^{-1}$ 当且仅当 $ad=0$，当且仅当 $a=0$，因为 $d\neq 0$，且 R 是一个整环。

考虑 Frac(R) 中的非零元素。我们有如下结论:

- If $ab^{-1}\neq 0$ and $cd^{-1}\neq 0$, then $(ac)(bd)^{-1}\neq 0$ since R is an integral domain.
- $(ab^{-1})(cd^{-1})=(ac)(bd)^{-1}=(ca)(db)^{-1}=(cd^{-1})(ab^{-1})$.
- $((ab^{-1})(cd^{-1}))ef^{-1}=((ac)(bd)^{-1})(ef^{-1})=(ace)(bdf)^{-1}=(ab^{-1})((ce)(df)^{-1})=ab^{-1}((cd^{-1})(ef^{-1}))$.
- $(ab^{-1})(dd^{-1})=ad(bd)^{-1}=ab^{-1}$, i.e., $dd^{-1}=1$ in Frac(R).
- $(ab^{-1})(ba^{-1})=ab(ab)^{-1}=1$.

这验证了 Frac(R) $\setminus\{0\}$ 在乘法下构成一个阿贝尔群。 □

Frac(R) 称为 R的**分式域**。

我们将下述定理的证明留作习题。

THEOREM 2.2.2. 整环 R 同构于 ***Frac***(R)的子环 $\{a1^{-1}\mid a\in R\}$。此外，若 R 是域 $\mathbb{F}$的子环，则 ***Frac***(R) 同构于 $\mathbb{F}$的一个子域。

PROOF. 定义 $f\colon R\to$ Frac(R)，使得对所有属于 R的 a，有 $f(a)=a1^{-1}$。那么

- f is well-defined.
- $f(ab)=(ab)1^{-1}=(a1^{-1})(b1^{-1})=f(a)f(b)$ for all a,b in R. That is, f is a ring homomorphism.
- If $f(a)=a1^{-1}=0$, i.e., $a1^{-1}\sim 01^{-1}$, then $a=0$. Hence f is injective.

根据第一同构定理， R 同构于 Imf，后者是 Frac(R) 的一个子环。

定理第 1 部分的证明到此结束。

第 2 部分的证明留作习题。 □

COROLLARY 2.2.1. 对于 ***Frac***(R)中的每个 c，都存在 R 中的 b，使得 cb 属于 R。这里， R 被视为 ***Frac***(R)的一个子环。

PROOF. 对于 a, R中的 b，将 c 记作 ab^{-1}。那么 $ab^{-1}b1^{-1}=(ab)b^{-1}=a1^{-1}$。也就是说， cb属于 R。□

EXAMPLES 2.2.1.

(1) Frac($\mathbb{Z}$)$\cong\mathbb{Q}$。(2) Frac($\mathbb{Z}[\sqrt{5}]$)$\cong\mathbb{Q}[\sqrt{5}]=\{\bar{a}+b\sqrt{5}\mid \bar{a},b\in\mathbb{Q}\}$。(3) Frac($\mathbb{F}[x]$)$\cong\{\frac{f}{g}\mid f,g\in\mathbb{F}[x],\bar{g}\neq 0\}$。

2.3. 素理想与极大理想

DEFINITION 2.3.1. 环 R 的真理想 I 称为**素**理想，如果 $ab\in I$ 蕴含 $a\in I$ 或 $b\in I$。

环 R 的真理想 I 称为**极大**，如果 R 是唯一一个严格大于 I 的理想。

Examples 2.3.1.

(1) 域 $\mathbb{F}$有唯一的素（极大）理想 $\{0\}$。(2) 对于素数 p， $p\mathbb{Z}$ 是 $\mathbb{Z}$的一个素（极大）理想。(3) 由 x 生成的理想是 $\mathbb{F}[x]$的一个素（极大）理想。

Theorem 2.3.1.

含幺交换环 R 的每个真理想 I 都包含于 R的一个极大理想中。

Proof. 证明依赖于佐恩引理，该引理指出：如果偏序集的每个全序子集都有一个上界，那么该偏序集就有一个极大元。

假设 I 是 R的一个真理想。

现在考虑包含 I 的 R 的真理想集合 $\mathcal{A}$，并按包含关系排序；也就是说，在 $\mathcal{A}$ 中，我们定义 $J \prec J'$ 为 $J \subseteq J'$。对于 $\mathcal{A}$ 的一个全序子集 $\mathcal{B}$，令 $J_0 = \bigcup_{J\in\mathcal{B}} J$。

对于 J_0 中任意的 a, b，存在 $\mathcal{B}$ 中的 J_1, J_2，使得 $a \in J_1$ 且 $b \in J_2$。由于 $\mathcal{B}$ 是全序的，因此我们有 $J_1 \prec J_2$ 或 $J_2 \prec J_1$。a 和 b 都只属于 J_1 和 J_2 中的一个，$a+b$ 也一样。对于 R 中任意的 c， ac 都属于 J_1。因此， J_0 是 R 的一个理想。注意到 $1 \notin J_0$，所以 $J_0 \subsetneq R$。因此， J_0 属于 $\mathcal{A}$ 和 $J \prec J_0$，也就是说， J_0 是 $\mathcal{B}$ 的一个上界。因此， $\mathcal{A}$ 中存在一个极大元，它是包含 I 的 R 的一个极大理想。□

Corollary 2.3.1. 含幺交换环 R 中的每个非单位元都包含在 R的某个极大理想中。

Proof. 将定理 2.3.1 应用于由该非单位元生成的理想。 □

Theorem 2.3.2。

设 R 是一个含幺交换环。

(1) I 是 R 的素理想，当且仅当 R/I 是整环。(2) I 是 R 的极大理想，当且仅当 R/I 是域。

Proof.

(1) R/I是整环，当且仅当对 a，b中的任意元素，若 $(a+I)(b+I) = ab+I = 0$，则 $a+I = 0$或 $b+I = 0$。等价地，若 ab属于 I，则 a或 b属于 I。

(2) 假设 R/I 是一个域。设 I 是理想 J的真子集。因此， J/I 是 R/I的非零理想。由于 R/I 是一个域， $J/I = R/I$。因此 $R = J$。所以， I 是 R的极大理想。

反过来，假设 I 是 R的极大理想。对于任意 $a \notin I$，由 I和 a生成的理想 $I + (a) = \{b + ac \,|\, b \in I, c \in R\}$是一个满足 $I \subsetneq I + (a)$ 的理想。因此 $I + (a) = R$。所以存在 c 属于 I 以及 b 属于 R，使得 $c + ab = 1$。也就是说， $a + I$是 R/I的单位。因此 R/I是一个域。

□

Corollary 2.3.2. 含幺交换环的极大理想是素理想。

Remark 2.3.1. 素理想未必是极大理想。例如，(x) 是 $\mathbb{Z}[x]$ 的素理想，因为 $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$，但 (x) 不是极大理想，因为 $(x) \subsetneq (x,2) \subsetneq \mathbb{Z}[x]$。

2.4. 多项式环

本节研究域 $\mathbb{F}$ 上的多项式环。特别地，我们介绍多项式的欧几里得算法。

顾名思义，多项式欧几里得算法是整数欧几里得算法的类似物。

多项式 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$的**次数** 是满足 $a_n \neq 0$的最大非负整数 n。记作 $\deg f$。例如，在 $\mathbb{R}[x]$中，$\deg(x^3 - 1) = 3$，且 $\deg(x^2 - x + 5) = 2$。

THEOREM 2.4.1. 给定 f 以及 $\mathbb{F}[x]$中的非零 g，存在唯一的 h 和 r属于 $\mathbb{F}[x]$，使得 $f = gh + r$，且$\deg(r) < \deg(g)$。

PROOF. 我们可以假设 $\deg f \geq \deg g$，否则 $h = 0$且 $f = r$。

将 f记作 $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$，将 g记作 $b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$且 $\deg f = n \geq m = \deg g$。

设 $h_1 = a_n b_m^{-1} x^{n-m}$和 $r_1 = f - gh_1$。那么 $\deg(r_1) \leq n - 1 < n = \deg(f)$。若 $\deg r_1 < \deg g$，则得到 $h = h_1$和 $r = r_1$。若 $\deg r_1 \geq \deg g$，则对 r_1 和 g 重复上述过程，得到 r_2。经过有限步，设为 k 步，要么 $r_k = 0$，要么 $\deg r_k < \deg g$。然后，我们可以从下往上反复代入这些恒等式，得到所需的 h 和 r。更确切地说，$h = h_1 + h_2 + \cdots + h_{k-1}$和$r = r_k$。

总结一下，我们所做的如下：

$$\begin{aligned} f &= gh_1 + r_1 \\ r_1 &= gh_2 + r_2 \\ &\cdots\cdots\cdots \\ r_{k-1} &= gh_{k-1} + r_k \end{aligned}$$

and

$$f = g(h_1 + h_2 + \cdots + h_{k-1}) + r_k.$$

我们证明了 h 和 r的存在性。

对于唯一性，若 $f = gh + r = gh + \tilde{r}$且 $\deg r < \deg g$，并且 $\deg \tilde{r} < \deg g$，那么 $g(h - h) = \tilde{r} - r$。有 $h = h$和 $r = \tilde{r}$成立；否则 $\deg(g(h - h)) \geq \deg g > \deg(\tilde{r} - r)$，这将导致矛盾。 □

r 多项式称为 f 除以 g所得的**余式**。

如果 $f = gh$ 属于 $\mathbb{F}[x]$，那么我们称 g 整除 f，或者称 g 是 f 的**因子**，记作$g|f$。

f 和 g 的**公因式**是指满足 h同时整除 f和 g的多项式 h。

如果 f 和 g 的一个公因式 h 满足：f和 g 的任意其他公因式都是 h的因子，那么称其为 f 和 g的**最大公因式**。

f 和 g 的最大公因式在相差标量倍数的意义下是唯一的。因此，我们称其为 f 和 g 的最大公因式，并记作 $\gcd(f, g)$。

如果 $\gcd(f, g) = 1$，那么我们称 f 和 g **互素**，或者称 f 与 g互素。

LEMMA 2.4.1. 设 f和 g属于 $\mathbb{F}[x]$。那么 最大公因式$(f, g) = fp + gq$，其中p, q属于 $\mathbb{F}[x]$。换言之，由 f和 g生成的理想(f, g)是(最大公因式(f, g))，即由最大公因式(f, g)生成的理想。

PROOF. 不失一般性，我们假设 $\deg\ g \leq \deg\ f$。

根据定理 2.4.1，$f = gh_0 + r_0$，且 $\deg r_0 < \deg g$。若 $r_0 \neq 0$，则 $g = h_1 r_0 + r_1$，且 $\deg\ r_1 < \deg r_0$。同样，若 $r_1 \neq 0$，则 $r_0 = h_2 r_1 + r_2$。每当 $r_i \neq 0$ 时，都按此归纳进行；经过有限步后，我们得到 $r_{k-2} = h_{k-1} r_{k-1} + r_k$ 和 $r_{k-1} = h_k r_k$。

注意，r_0 属于 (f, g)。归纳地，对 $0 \leq i \leq k$，每个 r_i 都属于 (f, g)。此外，若 r 整除 f 和 g，则 r 整除 r_k，因为 r_k 属于 (f, g)。因此，$r_k =$ 是 $\gcd(f, g)$，且 r_k 的形式为 $h = fp + gq$，其中某个 p, q 属于 $\mathbb{F}[x]$。□

REMARK 2.4.1. 在定理 2.4.1 和引理 2.4.1 的证明中，用于求 f 除以 g 所得的余式 r 以及 $\gcd(f,\ g)$的算法称为多项式的**欧几里得算法**。

2.5. 主理想整环

含幺交换环 R 中的非零非单位元 f 称为**不可约**，如果$f = gh$ 蕴含 g 或 h 是 R中的单位。否则称 f 为**可约**。

DEFINITION 2.5.1. **主理想整环**是一个整环 R ，其中每个理想都是**主理想**，也就是说，是由 R中的单个元素生成的理想。

$\mathbb{Z}$是一个主理想整环。

$\mathbb{Z}[x]$ 不是主理想整环，因为真理想 $(x,\ 2)$ 不是主理想。

THEOREM 2.5.1. $\mathbb{F}[x]$ 是主理想整环。

PROOF. 设 I 是 $\mathbb{F}[x]$的一个非零理想。假设 f 是 I 中次数最小的非零元素。

任取 $g \in I$。由定理 2.4.1，存在 h和 $r \in \mathbb{F}[x]$，使得$g = fh + r$，且 $\deg(r) < \deg(f)$。那么 $r = 0$，否则 r就是 I 中的一个非零元素，其次数小于 f 的次数，这与假设矛盾。因此$I = (f)$。□

THEOREM 2.5.2. 在主理想整环中，非零理想是素理想当且仅当它是极大理想。

PROOF. 必要性由推论 2.3.2 得出。

我们证明充分性。

假设 I 是主理想整环 R 中的素理想。

设理想 $J = (b) \supsetneq I = (a)$。则存在 c 属于 R，使得 $a = bc$。由于 I 是素理想且 b 不属于 I，元素 c 属于 I。存在 d 属于 R，使得 $c = ad$。因此 $a(bd - 1) = 0$。元素 a 非零，因为 $I = (a)$ 是 R 的非零理想。因此 $bd = 1$，这意味着 b 是单位。所以 $J = R$，这意味着 I 是极大理想。□

PROPOSITION 2.5.1. 如果整环 R 中的主理想(a) 是素理想，那么 a 是不可约元。如果 a 是主理想整环 R 中的不可约元，那么理想(a) 是素理想。

PROOF. 设 $a = bc$ for b，c 属于 R。那么，要么 b，要么 c 属于 (a)。假设b 属于 (a)。那么 $b = ad$ for d 属于 R。由此可得 $a = bc = adc$，这意味着$dc = 1$。因此 c 是一个单位，而 a 是 R中的一个不可约元。

假设 a 是主理想整环 R中的一个不可约元。设 (a) 是理想 $J=(b)$ 的真子集。那么，对于某个 c 属于 R，有 $a=bc$。由于 a不可约，因此 b 或 c 是一个单位。但 c 不可能是单位，否则 $(a)=(b)$。因此 b 是一个单位，且 $J=R$。这表明 (a) 是一个极大理想，因此也是一个素理想。□

由此可得以下结论：主理想整环中的不可约元 R 的性质与整数环 $\mathbb{Z}$ 中的素数类似。

Corollary 2.5.1. </style>在主理想整环 R中，设 p 是一个不可约元。若 $p|ab$, 则 $p|a$或 $p|b$。

Definition 2.5.2. 环 R 的理想序列 $\{I_n\}_{n=1}^{\infty}$ 称为**升链**，如果对所有 $1\leq i\leq n$ 都有 $I_n\subseteq I_{n+1}$。若存在 K 使得对所有 $k\geq K$都有 $I_k=I_{k+1}$，则称理想升链 $\{I_n\}_{n=1}^{\infty}$ 满足**升链条件**。

Lemma 2.5.1. 主理想整环中的每个理想升链都满足升链条件。

Proof. 设 $\{I_n=(a_n)\}_{n=1}^{\infty}$ 是主理想整环 R中的理想升链。定义 $J=\bigcup I_n$。那么 J 是一个理想，并且对某个$n=1b$，有 $J=(b)$ R。

由此可知，对于某个 $K\geq 1$， b属于 I_K。因此，$(b)\subseteq I_K\subseteq I_{K+1}\subseteq\cdots\subseteq(b)$。于是我们得到，对所有 $k\geq K$， $I_k=I_{k+1}$。□

Lemma 2.5.2. 设 R 是一个整环。

(1) 若 a、 b 和 c 是 R 和 $a=bc$中的非零非单位元，则 $(a)\subsetneqq(b)$。(2) $(f)=(g)$ 当且仅当对于某个单位 h， $f=gh$。

Proof. (1) 假设 $(a)=(b)$。我们得到，对于某个 d， $b=ad$ 属于 R。于是 $a=bc=adc$，这意味着 c 是一个单位。这与假设矛盾。

(2) 由 (1) 可得。 □

Theorem 2.5.3. 在相差一个单位的意义下，主理想整环中的每个非零非单位元都可以唯一地写成有限多个不可约元的乘积。

Proof. 设 a是主理想整环 R中的非零非单位元。

根据推论 2.3.1，元素 a 属于 R中的某个素（极大）理想。根据命题 2.5.1，存在 R 中的不可约元 p_1，使得对于某个 R中的 a_1，有 $a=p_1a_1$。归纳地，当 a_i 为非单位元时，对于所有 $i\geq 1$，我们得到 $a_i=p_{i+1}a_{i+1}$。然而，这一过程会在有限步后终止；否则根据引理 2.5.2，我们可以得到一个理想升链

$$(a)\subsetneqq(a_1)\subsetneqq(a_2)\subsetneqq\cdots\subsetneqq(a_n)\subsetneqq(a_{n+1})\subsetneqq\cdots$$

该理想升链不满足升链条件，这与引理 2.5.1矛盾。因此， a 可以写成

$$\underbrace{\text{p}}_{\text{有限个}}\quad\underbrace{\text{y many}}_{\text{不可约元的乘积。}}$$

若 $a=p_1p_2\cdots p_k=q_1q_2\cdots q_l$ 对于 $p_i's$ 和 $q_j's$ 都是不可约的，那么根据推论 2.5.1，每个 p_i 都整除某个 q_j，这意味着对于某个单位 b_i，有 $p_i=b_iq_j\in R$。因此 $k=l$，并且 a 分解为不可约多项式乘积的方式在相差一个单位的乘法意义下是唯一的。□

2.6. 艾森斯坦判别法与高斯引理

本节将介绍艾森斯坦判别法和高斯引理。简而言之，它们是用于在 $\mathbb{F}[x]$ 中寻找不可约多项式的工具。

设 R 是含幺交换环。在 $R[x]$ 中，不可约元称为**不可约多项式**。

定理 2.5.1 告诉我们， $\mathbb{F}[x]$ 是主理想整环。将我们对主理想整环所得的结论应用于 $\mathbb{F}[x]$，可得:

THEOREM 2.6.1.

(1) 对于 $\mathbb{F}[x]$ 中的不可约 p，若 $p|fg$，则 $p|f$ 或 $p|g$。(2) $\mathbb{F}[x]$ 中每个次数大于 0 的多项式，除相差数乘外，均可唯一地写成不可约多项式的乘积。(3) $\mathbb{F}[x]$ 的非零理想(f) 是素理想，当且仅当 f 不可约。

艾森斯坦判别法与高斯引理是判断 $\mathbb{F}[x]$ 中的多项式不可约的充分条件，尤其适用于 $\mathbb{Q}[x]$ 。 [Eis]

THEOREM 2.6.2（艾森斯坦判别法）。设 R 是一个整环， P 是 R 的一个素理想。若 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ 属于 $R[x]$，且满足：a_n 不属于 P，a_0、a_1、$\cdots$、a_{n-1} 属于 P，而 a_0 不属于 P^2，则 f 在 $R[x]$ 中不可约。

PROOF. 设 $f(x) = g(x)h(x)$，其中 g, h 属于 $R[x]$，$\deg(g) = k < n$，且 $\deg(h) = l < n$。假设 $g(x) = c_k x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c_0$ 且$h(x) = d_l x^l + d_{l-1}x^{k-1} + \cdots + d_1 x + d_0$，其中 c_i 和 d_j 的系数均属于 R。我们将证明 c_0 和 d_0 属于 P，这与 $a_0 = c_0 d_0$ 不属于 P^2 矛盾。

注意， $R[x]/P[x] \cong (R/P)[x]$。参见练习2.21。

因此，根据假设， $f+P[x] = a_n x^n + P[x] = (a_n + P)x^n$。此外， $g+P[x] = (c_k + P)x^k + (c_{k-1} + P)x^{k-1} + \cdots + (c_1 + P)x + c_0 + P$， $h + P[x] = (d_l + P)x^l + (d_{k-1} + P)x^{l-1} + \cdots + (d_1 + P)x + d_0 + P$，且 $f + P[x] = (g + P[x])(h + P[x])$。

因此

$$
\begin{aligned}
&c_0 d_0 + P = 0\\
&c_1 d_0 + c_0 d_1 + P = 0\\
&\cdots \quad \cdots \quad \cdots\\
&c_0 d_l + c_1 d_{l-1} + \cdots + c_l d_0 + P = 0
\end{aligned}
$$

如果 $c_0 + P$ 和 $d_0 + P$ 中有一个为零，不妨设为 $c_0 + P \neq 0$，那么 $d_0 + P = 0$，并且归纳可得 $d_1 + P = d_2 + P = \cdots = d_{l-1} + P = d_l + P = 0$。这与 $c_k d_l + P = a_n + P \neq 0$ 矛盾。因此 $c_0 + P$ 和 $d_0 + P$ 为零，这意味着 $c_0 d_0$ 属于 P^2。□

THEOREM 2.6.3（高斯引理）。设 R 是一个主理想整环，其分式域为 $\mathbb{F}$。那么， f 在 $R[x]$ 中不可约，当且仅当 f 在$\mathbb{F}[x]$中不可约。

PROOF. 设 f 是 $R[x]$ 中的一个不可约多项式，并且对于 $g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ 和 $h(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ 于 $\mathbb{F}[x]$。

由推论 2.2.1，存在 a，b 属于 R，使得 $g_1 = ag$ 和 $h_1 = bh$ 属于 $R[x]$。记 ab 为 c，并由定理 2.5.3 得知 $c = p_1 p_2 \cdots p_k$ 是 p_j在 R 中的不可约元。

我们有

$$p_1p_2\cdots p_kf = g_1h_1 =(\tilde{a}_nx^n + \tilde{a}_{n-1}x^{n-1} + \cdots + \tilde{a}_1x + \tilde{a}_0)$$
$$(\tilde{b}_mx^m + \tilde{b}_{m-1}x^{m-1} + \cdots + \tilde{b}_1x + \tilde{b}_0),$$

~其中 $\tilde{a}_i = a_ia$ 且 $b_j = b_jb$ 对所有 $1 \le i \le n$ 和 $1 \le j \le m$均成立。由归纳法，p_1 整除~的所有 $\tilde{a}_i$ 或所有 b_j。

因此可以约去 p_1，得到 $p_2\cdots p_k = h_2g_2$，其中 g_2，h_2属于 $R[x]$，deg $g_2 =$deg g 且 deg $h_2 =$deg h。

重复这一过程，我们得到 $f = g_kh_k$，其中 g_k，h_k属于 $R[x]$，deg $g_k =$ deg g且 deg $h_k =$deg h。由于 f在 $R[x]$中不可约，我们有 deg $g_k = 0$或 deg $h_k = 0$。因此，deg $g = 0$或 deg $h = 0$。所以 f在$\mathbb{F}[x]$中不可约。□

Remark 2.6.1。

(1) 根据艾森斯坦判别法和高斯引理，对每个$n \ge 1$，在 $\mathbb{Q}[x]$中都存在一个次数为 n 的不可约多项式，例如 $x^n - 2$。

（2）高斯引理适用于唯一分解整环上的多项式环，其适用范围比主理想整环更广。感兴趣的读者可参阅 [DF04] 和 [Lan02]了解详情。

习题

Exercise 2.1. 设 $C_0(\mathbb{R}) = \{f\colon \mathbb{R} \to \mathbb{R} | f$连续且$\lim_{x\to\infty} f(x) = 0\}$。在 $C_0(\mathbb{R})$ 上的加法和乘法定义为函数的逐点加法和乘法。证明 $C_0(\mathbb{R})$ 是一个非含幺交换环。

Exercise 2.2. 设 I 和 J 是交换环 R的理想。证明 IJ 是 R的理想，且 $IJ \subseteq I \cap J$。$IJ = I \cap J$是否成立?

Exercise 2.3. 证明环同态的核是一个理想。

Exercise 2.4. 证明固定实数的环 $\mathbb{C}$只有两个自同构。

Exercise 2.5. 证明第一环同构定理。

Exercise 2.6. 设 $\mathbb{F}$ 为一个域。U（$\mathbb{F}[x]$）是什么？请证明你的答案。

Exercise 2.7. 假设 $n \ge 2$。写出 U（$\mathbb{Z}/n\mathbb{Z}$）。$\mathbb{Z}/n\mathbb{Z}$ 成为整环的充要条件是什么？请证明你的答案。

Exercise 2.8. 证明定理 *2.2.2* 的第二部分。

Exercise 2.9. 在环 $\mathbb{Z}\times\mathbb{Z}$ 中找出一个是素理想但不是极大理想的理想。

Exercise 2.10. 证明 $\mathbb{Z}$ 的每个素理想都具有 $p\mathbb{Z}$的形式，其中p为素数。

Exercise 2.11. 写出 $\mathbb{Z}[\frac{1+\sqrt{5}}{2}] = \{a + b\frac{1+\sqrt{5}}{2} \mid a, b \in\mathbb{Z}\}$的所有素理想。

Exercise 2.12. 设 a 不可约，且 b 是含幺交换环 R 中的单位。证明 ab 也不可约。

Exercise 2。13. f 在 $\mathbb{F}[x]$ 中不可约，当且仅当 f 不能写成两个次数都小于 f的多项式的乘积。

Exercise 2.14。 设 f 和 g 属于 $\mathbb{F}[x]$。证明： f 整除 g 且 g整除 f，当且仅当存在 $\mathbb{F}$中的非零 α 使得 $f=\alpha g$ 。

Exercise 2.15. 求 x^3-2x^2+1 和 x^2-x-3 在 $\mathbb{Q}[x]$ 中的最大公因式，并将其表示为它们的线性组合。

Exercise 2.16. 求 x^4+1 和 $x^4+x^3+3x^2+2x+2$ 在 $\mathbb{F}_5[x]$ 中的最大公因式，并将其表示为它们的线性组合。

Exercise 2.17. 证明两个互不相同的首一不可约多项式互素。

Exercise 2.18. 设 p 是 $\mathbb{F}[x]$ 中的一个不可约多项式。证明，对于任意 f 属于 $\mathbb{F}[x]$, $\gcd(p,f)=1$ 或 p。

Exercise 2.19. 证明， $\mathbb{F}[x]$ 中的多项式 $p(x)$ 满足 $\deg(p)\leq 3$ 时，当且仅当 $p(x)$ 在 $\mathbb{F}$ 中没有根，它才是不可约的。对于满足 $\deg(p)>3$ 的 p，结论是否仍然成立？

Exercise 2.20. 证明：对于任意素数 p，多项式 x^p+p-1 在 $\mathbb{Q}[x]$ 中不可约。

Exercise 2.21. 设 P 是主理想整环 R 中的素理想。证明 $P[x]$ 是 $R[x]$ 中的素理想，并且

$$R[x]/P[x]\cong(R/P)[x].$$

第3章

基础域论

尽管域是环的特殊情形，但域的定义却早于环的定义。本章将讨论域扩张理论，特别是有理数域 $\mathbb{Q}$的有限扩张，为伽罗瓦理论基本定理服务。

3.1 有限域

回忆一下，域是一个含幺交换环，其中每个非零元素都是单位。

下面是一些有限域的例子。

EXAMPLES 3.1.1. 对于一个素数 p， $\mathbb{Z}/p\mathbb{Z}$是一个域。将它记作 $\mathbb{F}_p$。

给定域 $\mathbb{F}_p[x]$ 上次数为 n 的不可约多项式 f，则 $\mathbb{F}_p[x]/(f)$ 是一个域，因为 (f) 是 $\mathbb{F}_p[x]$ 的极大理想。此外， $|\mathbb{F}_p[x]/(f)| = p^n$，因为对于所有 $1 \leq i \leq n-1\}$., $\mathbb{F}_p[x]/(f) = \{a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0+(f) \mid a_i \in \mathbb{F}_p$。例如， x^2+x+1 是 $\mathbb{F}_2[x]$ 中的不可约多项式，则域 $\mathbb{F}_2[x]/(x^2+x+1)$ 有 4 个元素：(x^2+x+1)、 $1+(x^2+x+1)$、 $x+(x^2+x+1)$ 和 $x+1+(x^2+x+1)$。因此， $|\mathbb{F}_2[x]/(x^2+x+1)| = 4$。

DEFINITION 3.1.1. 域 $\mathbb{F}$ 的<strong?characteristic 是使得 $n = 0$ 成立的最小正整数 n 。记作 Ch$\mathbb{F}$。如果每个正整数都非零，则称 $\mathbb{F}$ 的特征为 0。

可以作为习题验证，对于任意域 $\mathbb{F}$，Ch$\mathbb{F} = 0$ 或 Ch$\mathbb{F}$ 是素数。

若 Ch$\mathbb{F} = p$，则对 $\mathbb{F}$ 中的每个 a，都有 $pa = 0$ 。

有限域具有有限特征。稍后我们将看到一些具有有限特征的无限域的例子。

可以看出， $\mathbb{Q}$、 $\mathbb{R}$、 $\mathbb{C}$ 的特征均为零，且 Ch$\mathbb{F}_p = p$。

THEOREM 3.1.1. 若 $\mathbb{F}$ 是有限域且 $\mathrm{Ch}\mathbb{F} = p$，则对于某个正整数 n，有 $|\mathbb{F}| = p^n$ 。

PROOF. 设对于某个与 p 互素的正整数 m，有 $|\mathbb{F}| = p^n m$ 。若 $m > 1$，则 m 有一个不同于 p的素因子 q。对加法群 $\mathbb{F}$应用柯西定理。于是 $\mathbb{F}$ 中存在一个阶为 q的元素 a 。因此 $qa = 0$。

由于 q 与 p互素，因此我们有 $p = lq + r$，且 $0 < r < q$。由此可得 $0 = pa = lqa + ra = ra$，这与 a 的阶为 q矛盾。证明完毕。□

3.2. 向量空间

在线性代数中，我们研究以 $\mathbb{R}$ 或 $\mathbb{C}$为底域的向量空间。实际上，向量 r 向量空间可以定义在任意域上。

Definition 3.2.1. 域上的**向量空间** V是一个非空集合，在其上定义了加法和数乘运算。具体来说，对于 V中的任意一对元素 x 和 y，都可以唯一确定一个同样属于 V的元素$x+y$；对于 V中的任意元素 x 以及 $\mathbb{F}$中的任意 α，都可以唯一确定一个属于 V的元素 αx。此外，还满足以下条件：

(1) $(V,+)$是一个阿贝尔群。(2) 对每个 $x\in V$以及所有 $\alpha,\beta\in\mathbb{F}$，都有$(\alpha\beta)x=\alpha(\beta x)$。(3) 对所有 $x,y\in V$以及所有 $\alpha,\beta\in\mathbb{F}$，都有 $\alpha(x+y)=\alpha x+\alpha y$且$(\alpha+\beta)x=\alpha x+\beta x$。(4) 对每个 $x\in V$，都有 $1x=x$。

向量空间中的元素称为**向量**。域 $\mathbb{F}$ 称为 V的**标量域**。

向量空间的**子空间** 是一个本身也是向量空间的子集。

对于向量空间 V中的向量 $v_1,v_2,\cdots,v_n$ 以及 $\mathbb{F}$中的 $\alpha_1,\alpha_2,\cdots,\alpha_n$，表达式 $\alpha_1v_1+\alpha_2v_2+\cdots+\alpha_nv_n$ 称为 $v_1,v_2,\cdots,v_n$的线性组合。 $v_1,v_2,\cdots,v_n$ 的所有线性组合构成的集合称为 $v_1,v_2,\cdots,v_n$的线性张成，记作$\mathrm{Span}(v_1,v_2,\cdots,v_n)$。

向量 $v_1,\ v_2,\ \cdots,\ v_n$ 在向量空间 V中称为**线性无关**，如果$\alpha_1v_1+\alpha_2v_2+\cdots+\alpha_nv_n=0$ 蕴含 $\alpha_1=\alpha_2=\cdots=\alpha_n=0$。否则$v_1,\ v_2,\ \cdots,\ v_n$ 称为**线性相关**。

向量空间的子集 A 称为线性无关，如果其中任意向量$v_1,\ v_2,\ \cdots,\ v_n$ 都线性无关。如果向量空间 V有一个极大的线性无关有限子集，那么 V 称为**有限维**；否则称为**无限维**。

有限维向量空间 V中的向量集合 $\{v_1,v_2,\cdots,v_n\}$ 称为 V的一组**基**，如果它们线性无关且 $V=\mathrm{Span}(v_1,\ v_2,\ \cdots,\ v_n)$。

以下定理的证明与线性代数中的类似结果相同。我们将其留作习题。

Theorem 3.2.1. 向量空间的任意两个基具有相同的基数。

对于域 $\mathbb{F}$ 上的有限维向量空间 V，V 的基的基数称为 V 的**维数**，记作 $\dim_{\mathbb{F}}V$。当 V 是无限维时，记 $\dim_{\mathbb{F}}V=\infty$。例如，$\dim_{\mathbb{F}}\{0\}=0$、$\dim_{\mathbb{R}}\mathbb{C}=2$、$\dim_{\mathbb{C}}\mathbb{C}=1$和 $\dim_{\mathbb{Q}}\mathbb{R}=\infty$。

若 $\mathbb{F}$ 是 $\mathbb{E}$ 的子域，则 $\mathbb{E}$ 是 $\mathbb{F}$ 上的向量空间。将 $\dim_{\mathbb{F}}\mathbb{E}$ 记作 $[\mathbb{E}:\ \mathbb{F}]$。

Theorem 3.2.2. 若 $\mathbb{F}\subseteq\mathbb{E}\subseteq\mathbb{K}$ 是域，则

$$[\mathbb{K}:\mathbb{F}]=[\mathbb{K}:\mathbb{E}][\mathbb{E}:\mathbb{F}].$$

Proof. 我们可以假设 $[\mathbb{K}:\ \mathbb{E}]$ 和 $[\mathbb{E}:\ \mathbb{F}]$ 是有限的，因为 $[\mathbb{K}:\ \mathbb{F}]\geq[\mathbb{K}:\ \mathbb{E}]$且 $[\mathbb{K}:\ \mathbb{F}]\geq[\mathbb{E}:\ \mathbb{F}]$。

设 $\{v_i\}_{i=1}^n$ 是 $\mathbb{F}$ 上 $\mathbb{E}$ 的一组基，$\{w_j\}_{j=1}^m$ 是 $\mathbb{E}$上 $\mathbb{K}$ 的一组基。

假设 $\sum_{j=1}^{m}\sum_{i=1}^{n}\alpha_{ij}v_iw_j=0$ 对 α_{ij}属于 $\mathbb{F}$成立。那么 $\sum_{j=1}^{m}(\sum_{i=1}^{n}\alpha_{ij}v_i)w_j=0$。由于$\{w_j\}_{j=1}^m$ 在 $\mathbb{E}$上线性无关，因此对于每个 $1\leq j\leq m$，都有 $\sum_{i=1}^{n}\alpha_{ij}v_i=0$。此外，由于 $\{v_i\}_{i=1}^m$ 在 $\mathbb{F}$上线性无关，因此对于所有$1\leq i\leq n$ 和 $1\leq j\leq m$，都有 $\alpha_{ij}=0$。所以$\{v_iw_j\}_{1\leq i\leq n,\ 1\leq j\leq m}$ 在 $\mathbb{F}$上线性无关。

$_m$对于 $\mathbb{K}$中的每个 v ，当 $\beta_j's$ 属于 $\mathbb{E}$时，都有 $v=\sum\beta_j w_j$ 。此外，对于 α_{ji}属于 $\mathbb{F}$，每个 β_j $=_{j=1_n}\sum\alpha_{ji}v_i$。因此 $v=\sum\alpha_{ji}v_iw_j$，也就是说，集合 $\{v_iw_j\}_{1\le i\le n,\ 1\le j\le m}$ $_{i=1}$ $_{i,\ j}$张成 $\mathbb{K}$。

因此 $\{v_iw_j\}_{1\le i\le n,\ 1\le j\le m}$ 是 $\mathbb{K}$ 在 $\mathbb{F}$上的一个基。由此

$$[\mathbb{K}:\mathbb{F}]=mn=[\mathbb{K}:\mathbb{E}][\mathbb{E}:\mathbb{F}].$$

□

3.3. 域扩张

3.3.1. 含有多项式的根的域扩张。如果 $\mathbb{F}$同构于 $\mathbb{E}$的一个子域，那么 $\mathbb{E}$ 称为 $\mathbb{F}$ 的**扩张**。如果 $[\mathbb{E}:\ \mathbb{F}]<\infty$，那么$\mathbb{E}$ 称为 $\mathbb{F}$的**有限扩张**；否则称为 $\mathbb{F}$的**无限扩张**。

设 $\mathbb{F}$是 $\mathbb{E}$的一个子域，且 α_1、α_2、$\cdots$、α_n属于 $\mathbb{E}$。记$\mathbb{F}(\alpha_1,\alpha_2,\cdots,\alpha_n)$为包含 $\mathbb{F}$ 以及 α_1、α_2、$\cdots$、α_n的 $\mathbb{E}$的最小子域。称$\mathbb{F}(\alpha_1,\alpha_2,\cdots,\alpha_n)$为 $\mathbb{F}$上由 α_1、α_2、$\cdots$、α_n生成的域。

例如，域 $\mathbb{Q}(\sqrt{2})$是 $\mathbb{R}$ 中由 $\sqrt{2}$ 在 $\mathbb{Q}$上生成的子域。可以看出，$\mathbb{Q}(\sqrt{2})$ $=\{a+b\sqrt{2}\,|\,a,b\in\mathbb{Q}\}$，且 $[\mathbb{Q}(\sqrt{2}):\ \mathbb{Q}]=2$。

THEOREM 3.3.1.

设 p 是 $\mathbb{F}[x]$中的不可约多项式，则存在 $\mathbb{F}$ 的扩张$\mathbb{E}$，使得 $\mathbb{E}$ 包含 p的一个根。

PROOF. 由于 (p) 是极大理想，$\mathbb{F}[x]/(p)$ 是一个域。将其记为 $\mathbb{E}$。

定义 $\varphi:\ \mathbb{F}\to\mathbb{E}$，令 $\varphi(a)=a+(p)$，其中所有 a 属于 $\mathbb{F}$。则 φ 是非零同态，因而是单射。因此，$\mathbb{F}$ 同构于 $\mathrm{Im}\varphi=\varphi(\mathbb{F})=\{a+(p)\,|\,a\in\mathbb{F}\}$，后者是 $\mathbb{E}$ 的一个子域。

现在，我们可以将 $\mathbb{F}[x]$ 中的 $p=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 与 $\tilde{p}=(a_n+(p))x^n+(a_{n-1}+(p))x^{n-1}+\cdots+(a_1+(p))x+(a_0+(p))$ 识别为 $\varphi(\mathbb{F})[x]$中的元素。此外

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

因此，$\tilde{p}$ 在 $\mathbb{E}$中有一个根 $x+(p)$。 □

LEMMA 3.3.1. 设 $\mathbb{F}$ 是 $\mathbb{E}$ 的一个子域，且 α 是 $\mathbb{E}$ 中不可约多项式 p 的一个根。则 $\mathbb{F}(\alpha)=\{f(\alpha)\,|\,f\in\mathbb{F}[x]\}$。

PROOF. 记 $\{f(\alpha)\,|\,f\in\mathbb{F}[x]\}$ 为 $\mathbb{K}$。显然，$\mathbb{K}$ 是 $\mathbb{F}(\alpha)$的一个含幺交换子环。此外，若 $f(\alpha)\neq0$，则 f 与 p 互素，因为 p 不可约。存在 g,h属于 $\mathbb{F}[x]$，使得 $fg+ph=1$。因此，$f(\alpha)g(\alpha)=1$。这说明 $\mathbb{K}$ 是一个域。因此，$\mathbb{F}(\alpha)\subseteq\mathbb{K}$。

因此，$\mathbb{F}(\alpha)=\mathbb{K}$。 □

THEOREM 3.3.2. 设 $\mathbb{F}$ 是 $\mathbb{E}$ 的子域，且 α 是 $\mathbb{E}$ 中一个在 $\mathbb{F}[x]$上的不可约多项式 p 的根。那么 $\mathbb{F}(\alpha)\cong\mathbb{F}[x]/(p)$。

PROOF. 根据引理 3.3.1， $\mathbb{F}(\alpha) = \mathbb{K} = \{f(\alpha) \mid f \in \mathbb{F}[x]\}$。

定义 φ： 对所有 $f \in \mathbb{F}[x]$, 令 $\mathbb{K} \to \mathbb{F}[x]/(p)$= $\varphi(f(\alpha)) = f + (p)$。

- 若 $f_1(\alpha) = f_2(\alpha)$, 则 $(f_1 - f_2)(\alpha) = 0$。要么 $f_1 - f_2$ 与 p 互素，要么 p 整除 $f_1 - f_2$。由于 $p(\alpha) = 0$, 所以 $f_1 - f_2$ 与 p 不可能互素。因此 p 整除 $f_1 - f_2$, 这意味着 $f_1 + (p) = f_2 + (p)$。所以 φ 是良定义的。
- $\varphi(f_1(\alpha)f_2(\alpha)) = \varphi(f_1 f_2(\alpha)) = f_1 f_2 + (p) = (f_1 + (p))(f_2 + (p)) = \varphi(f_1(\alpha))\varphi(f_2(\alpha))$, 并且 $\varphi(f_1(\alpha)+f_2(\alpha)) = \varphi((f_1+f_2)(\alpha)) = f_1+f_2+(p) = (f_1 + (p)) + (f_2 + (p)) = \varphi(f_1(\alpha)) + \varphi(f_2(\alpha))$。因此 φ 是一个环同态。
- 如果 $f + (p) = 0$, 那么 f属于 (p), 也就是说， p整除 f。因此 $f(\alpha) = 0$。故 φ 是单射。
- 显然， φ 是满射。

因此 $\mathbb{F}(\alpha) \cong \mathbb{F}[x]/(p)$。 □

如果多项式 f 属于域 $\mathbb{F}[x]$ ，且在**分裂**，那么称其在该域上分裂；若 f 的所有根都属于$\mathbb{E}$, 则称多项式 f 在域 $\mathbb{F}[x]$ 上分裂。

如果多项式 f 属于 $\mathbb{F}[x]$ ，且首项系数为 1，也就是说 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$，则称其为**首一**多项式。

THEOREM 3.3.3. 对于每个非零首一多项式 f 属于 $\mathbb{F}[x]$, 都存在 $\mathbb{F}$ 的一个扩张 $\mathbb{E}$, 使得 f 在该扩张上分裂。

PROOF. 我们对 $\deg f$ 使用归纳法。

如果 $\deg f = 1$, 那么 f 在 $\mathbb{F}$上分裂。

假设该结论对次数小于 n的任意多项式都成立。因此， $\mathbb{F}[x]$中次数小于 n 的每个多项式都在 $\mathbb{F}$的某个扩域上分裂。

假设 f 是次数为 $\deg f = n$的不可约首一多项式。

根据定理 3.3.1，存在 $\mathbb{F}$ 的一个扩张 $\mathbb{K}$ ，其中包含 f的一个根 α ，这意味着， $f(x) = (x - \alpha)g(x)$, 其中 α属于 $\mathbb{K}$，且 g属于 $\mathbb{K}[x]$。根据假设，存在 $\mathbb{K}$ 的一个扩张 $\mathbb{E}$ ，使得 g 在其上分裂。因此， f 在 $\mathbb{E}$上分裂。

证明至此完成。 □

3.3.2. 代数扩张。 假设 $\mathbb{F}$是 $\mathbb{E}$的一个子域。若元素 α属于 $\mathbb{E}$ ，且它是 $\mathbb{F}[x]$中的某个非零多项式的根，则称它在 $\mathbb{F}$ 上是**代数的** 。例如， $\sqrt{2}$ 在 $\mathbb{Q}$ 上是代数的，因为它是 $x^2 - 2$的一个根。

THEOREM 3.3.4. 如果 α 属于 $\mathbb{E}$，且在 $\mathbb{F}$上是代数的，那么存在唯一一个 $\mathbb{F}[x]$ 中的首一不可约多项式 p ，使得 $p(\alpha) = 0$。

PROOF. 我们先证明 p的存在性。

由于 α 在 $\mathbb{F}$上是代数的，因此存在 $\mathbb{F}[x]$ 中的首一多项式 f ，使得$f(\alpha) = 0$。将 f写成首一不可约多项式的乘积： $f = p_1 p_2 \cdots p_m$。那么，对于某个 $1 \le i \le m$，有 $p_i(\alpha) = 0$ 。

设 p 和 q 是 $\mathbb{F}[x]$ 中具有公共根 α 的互不相同的首一不可约多项式。由于 p 和 q 互素，存在 g， h 属于 $\mathbb{F}$，使得 $pg+qh = 1$。于是 $0 = p(\alpha)g(\alpha) + q(\alpha)h(\alpha) = 1$，这就产生了矛盾。这证明了 p 的唯一性。

□

称 p 为 α 在 $\mathbb{F}$ 上的**最小多项式**，并记作$m_{\alpha,\mathbb{F}}(x)$。

COROLLARY 3.3.1。设 α 属于 $\mathbb{E}$，且在 $\mathbb{F}$ 上是代数的。若 f 属于 $\mathbb{F}[x]$，满足 $f(\alpha)=0$，则 $m_{\alpha,\mathbb{F}}(x)$ 整除 f。也就是说，在所有以 α 为根的 $\mathbb{F}[x]$ 中的非零多项式里，$m_{\alpha,\mathbb{F}}(x)$ 的次数最小。

PROOF. 由于$m_{\alpha,\mathbb{F}}(x)$是不可约的，因此要么$m_{\alpha,\mathbb{F}}(x)$整除 f，要么$m_{\alpha,\mathbb{F}}$ 与 f 互素。正如定理 3.3.4 的证明中的论证所示，$m_{\alpha,\mathbb{F}}$ 与 f互素是不可能的。□

$m_{\alpha,\mathbb{F}}(x)$的次数称为 α 在 $\mathbb{F}$上的**代数次数** 。

COROLLARY 3.3.2. 设 α 属于 $\mathbb{E}$，且在 $\mathbb{F}$上代数。则 $\mathbb{F}(\alpha)\cong\mathbb{F}[x]/(m_{\alpha,\mathbb{F}})$。

PROOF. 这可由定理 3.3.2 和定理 3.3.4 得出。 □

THEOREM 3.3.5. α 在 $\mathbb{F}$ 上代数，当且仅当 $[\mathbb{F}(\alpha):\mathbb{F}]<\infty$。此外，当 α 在 $\mathbb{F}$上代数时，$[\mathbb{F}(\alpha):\mathbb{F}]$等于 α 的代数次数。

PROOF. 设 α 在 $\mathbb{F}$ 上代数，其最小多项式为$m_{\alpha,\mathbb{F}}$，且 $\deg m_{\alpha,\mathbb{F}}=n$。

根据引理 3.3.1，$\mathbb{F}(\alpha)=\mathbb{K}=\{f(\alpha)\mid f\in\mathbb{F}[x]\}$。因此，$\mathbb{F}(\alpha)=\mathrm{Span}(1,\alpha,\cdots,\alpha^{n-1})$。由此可得，$[\mathbb{F}(\alpha):\mathbb{F}]\le n<\infty$。此外，$\{1,\alpha,\cdots,\alpha^{n-1}\}$ 在 $\mathbb{F}$ 上线性无关；否则，可以找到一个 $\mathbb{F}[x]$ 中的非零多项式 f，其次数小于 n，使得 $f(\alpha)=0$，这与 $\deg m_{\alpha,\mathbb{F}}=n$矛盾。因此，$[\mathbb{F}(\alpha):\mathbb{F}]=n$。

假设 $[\mathbb{F}(\alpha):\mathbb{F}]=n$。那么 $\{1,\alpha,\cdots,\alpha^{n-1},\alpha^n\}$ 在 $\mathbb{F}$上线性无关。因此，存在一个 $\mathbb{F}[x]$ 中的非零多项式 f，其次数不大于 n，使得 $f(\alpha)=0$，这意味着 α 在 $\mathbb{F}$上是代数的。

□

THEOREM 3.3.6. 若 α,β 属于 $\mathbb{E}$，且它们在 $\mathbb{F}$ 上是代数的，那么 $\alpha\pm\beta$, $\alpha\beta$ 和 α^{-1} 在 $\mathbb{F}$ 上也都是代数的。也就是说，$\mathbb{F}$ 上的代数元素构成 $\mathbb{E}$ 的一个子域。

PROOF. 由于 $\mathbb{F}(\alpha+\beta)$ 是 $\mathbb{F}(\alpha,\beta)$ 的一个子域，并且 $[\mathbb{F}(\alpha,\beta):\mathbb{F}]=[\mathbb{F}(\alpha,\beta):\mathbb{F}(\alpha)][\mathbb{F}(\alpha):\mathbb{F}]<\infty$，由定理 3.3.5，$\alpha+\beta$ 在 $\mathbb{F}$ 上是代数的。同理，$\alpha-\beta$ 和 $\alpha\beta$ 在 $\mathbb{F}$ 上也都是代数的。

此外，$\mathbb{F}(\alpha^{-1})$ 是 $\mathbb{F}(\alpha)$ 的一个子域，因此 $[\mathbb{F}(\alpha):\mathbb{F}]<\infty$ 意味着 $[\mathbb{F}(\alpha^{-1}):\mathbb{F}]<\infty$。由定理 3.3.5，$\alpha^{-1}$ 在 $\mathbb{F}$ 上是代数的。□

令 $\mathbb{F}$ 为 $\mathbb{E}$的子域。若 $\mathbb{E}$ 中的每个元素都是 $\mathbb{F}$上的代数元，则称 $\mathbb{E}$是 $\mathbb{F}$ 的**代数扩张**。

$\mathbb{F}$ 的每个有限扩张都是 $\mathbb{F}$上的代数扩张。
下面的定理通过代数扩张刻画有限扩张。

THEOREM 3.3.7. $\mathbb{E}$ 是 $\mathbb{F}$ 的有限扩张，当且仅当在 $\mathbb{E}$中存在 $\mathbb{F}$ 上的代数α_1、α_2、$\cdots$、α_n，使得 $\mathbb{E}=\mathbb{F}(\alpha_1,\alpha_2,\cdots,\alpha_n)$。

PROOF. 设 $\mathbb{E}$ 是 $\mathbb{F}$的有限扩张。令 $\{\alpha_i\}_{i=1}^n$ 为 $\mathbb{E}$ 在$\mathbb{F}$上的一组基。由于对所有 $1\le i\le n$，$[\mathbb{F}(\alpha_i):\mathbb{F}]\le[\mathbb{E}:\mathbb{F}]<\infty$，因此每个 α_i 都是 $\mathbb{F}$上的代数元。此外，$\mathbb{E}=\mathbb{F}(\alpha_1,\alpha_2,\cdots,\alpha_n)$。

反之，若存在代数的 $\{\alpha_i\}_{i=1}^n$ in $\mathbb{E}$，使得 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 在 $\mathbb{F}$ 上代数，且 $\mathbb{E}=\mathbb{F}(\alpha_1,\alpha_2,\cdots,\alpha_n)$。因此，对于每个 $1\le i\le n$，α_{i+1} 都是

在 $\mathbb{F}(\alpha_1,\cdots,\alpha_i)$ 上代数的，也就是说， $[\mathbb{F}(\alpha_1,\alpha_2,\cdots,\alpha_i,\alpha_{i+1}):\mathbb{F}(\alpha_1,\alpha_2,\cdots,\alpha_i)]<\infty$。因此

$$[\mathbb{E}:\ \mathbb{F}]=[\mathbb{F}(\alpha_1,\alpha_2,\cdots,\alpha_n):\ \mathbb{F}]=[\mathbb{F}(\alpha_1,\alpha_2,\cdots,\alpha_{n-1},\alpha_n):\ \mathbb{F}(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})]$$
$$[\mathbb{F}(\alpha_1,\alpha_2,\cdots,\alpha_{n-1}):\ \mathbb{F}(\alpha_1,\alpha_2,\cdots,\alpha_{n-2})]\cdots[\mathbb{F}(\alpha_1,\alpha_2):\ \mathbb{F}(\alpha_1)]<\infty.$$

因此， $\mathbb{E}$ 是 $\mathbb{F}$的有限扩张。 □

下面的定理说明代数扩张具有传递性。

THEOREM 3.3.8. 设 $\mathbb{K}$ 是 $\mathbb{E}$ 的代数扩张，且 $\mathbb{E}$ 是 $\mathbb{F}$的代数扩张。那么 $\mathbb{K}$ 是 $\mathbb{F}$的代数扩张。

PROOF. 任取 $\mathbb{K}$中的一个 a 。

由于 a 在 $\mathbb{E}$上是代数的，因此存在一个非零多项式 $f=a_0+a_1x+\cdots+a_nx^n$ 属于 $\mathbb{E}[x]$，使得 $f(a)=0$。

因此 $[\mathbb{F}(a,a_0,a_1,\cdots,a_n):\mathbb{F}(a_0,a_1,\cdots,a_n)]<\infty$。注意到 $a_0,a_1,\cdots,a_n$都在 $\mathbb{F}$上是代数的，因此 $[\mathbb{F}(a_0,a_1,\cdots,a_n):\mathbb{F}]<\infty$。由此

$$\begin{aligned}[\mathbb{F}(a):\mathbb{F}]&\le[\mathbb{F}(a,a_0,a_1,\cdots,a_n):\mathbb{F}]\\&=[\mathbb{F}(a,a_0,a_1,\cdots,a_n):\ \mathbb{F}(a_0,a_1,\cdots,a_n)][\mathbb{F}(a_0,a_1,\cdots,a_n):\ \mathbb{F}]<\infty.\end{aligned}$$

这表明 a 在 $\mathbb{F}$上是代数的。由于 a 是在 $\mathbb{K}$中任意选取的，这意味着 $\mathbb{K}$ 是 $\mathbb{F}$的代数扩张。

□

3.4. 分裂域

3.4.1. 分裂域的存在性与唯一性。

DEFINITION 3.4.1. 域 $\mathbb{F}$ 的扩域 $\mathbb{E}$ 被称为 $\mathbb{F}[x]$ 中 f 的分裂域，如果

(1) $f(x)$ 在 $\mathbb{E}$ 上完全分解，即 $\mathbb{E}$ 包含 f 的每一个根。(2) $f(x)$ 不在包含 $\mathbb{F}$ 的 $\mathbb{E}$ 的任何真子域上完全分解。

LEMMA 3.4.1. 设 $\varphi:\ \mathbb{F}_1\to\mathbb{F}_2$ 是一个域同构，且 $f_1(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 属于 $\mathbb{F}_1[x]$。定义 f_2 在 $\mathbb{F}_2[x]$ 中为 $f_2(x)=\varphi(a_n)x^n+\varphi(a_{n-1})x^{n-1}+\cdots+\varphi(a_1)x+\varphi(a_0)$。如果 $\mathbb{E}_1\supseteq\mathbb{F}_1$ 是 f_1 的分裂域，且 $\mathbb{E}_2\supseteq\mathbb{F}_2$ 是 f_2 的分裂域，那么存在一个同构 $\sigma:\ \mathbb{E}_1\to\mathbb{E}_2$，使得对于所有 a 属于 $\mathbb{F}_1$，均有 $\varphi(a)=\sigma(a)$。

PROOF. 我们对 $\deg f_1$ 进行归纳。

若 $\deg f_1=1$，则 $\mathbb{F}_1$ 是 f_1 的分裂域，而 $\mathbb{F}_2$ 是 f_2的分裂域。所需的同构 $\sigma:\mathbb{F}_1\to\mathbb{F}_2$ 是 φ。

假设当 f_1 在 $\mathbb{F}_1[x]$ 中的次数小于 n时，命题成立。

设 $\deg f_1=n$，且 $\mathbb{E}_1\supseteq\mathbb{F}_1$ 和 $\mathbb{E}_2\supseteq\mathbb{F}_2$ 分别是 f_1 和 f_2的分裂域。

注意， f_1 在 $\mathbb{E}_1$上分裂，因此 $\mathbb{E}_1$ 包含 α f_1的一个根。由于 α 在 $\mathbb{F}_1$上代数，存在一个不可约多项式 $p_1(x)=a_kx^k+\cdots+a_1x+a_0$属于 $\mathbb{F}_1[x]$，它是 f_1的一个因子，并且 $p_1(\alpha)=0$。因此， $p_2(x)=\varphi(a_k)x^k+\cdots+\varphi(a_1)x+\varphi(a_0)$是 $\mathbb{F}_2[x]$ 中的一个不可约多项式，它是 f_2 的一个因子，并且在 $\mathbb{E}_2$上分裂。此外，$\beta=\varphi(\alpha)$是 p_2的一个根。由定理 3.3.2，得到 $\mathbb{F}_1(\alpha)\supseteq\mathbb{F}_1$、 $\mathbb{F}_2(\beta)\supseteq\mathbb{F}_2$，并且

$$\mathbb{F}_1(\alpha)\cong\mathbb{F}_1[x]/(p_1)\cong\mathbb{F}_2[x]/(p_2)\cong\mathbb{F}_2(\beta).$$

此外，存在一个同构 $\psi\colon \mathbb{F}_1(\alpha) \to \mathbb{F}_2(\beta)$，使得对 $\mathbb{F}_1$中的所有a，都有 $\psi(a) = \varphi(a)$。

此外，$f_1 = (x-\alpha)g_1$ 和 $f_2 = (x-\beta)g_2$，其中 g_1 属于 $\mathbb{F}_1(\alpha)[x]$，而 g_2 属于$\mathbb{F}_2(\beta)[x]$。注意，g_1 可通过 φ与 g_2 等同；$\mathbb{E}_1 \supseteq \mathbb{F}_1(\alpha)$是 g_1 的一个分裂域，而 $\mathbb{E}_2 \supseteq \mathbb{F}_2(\beta)$是 g_2的一个分裂域。由于 $\deg g_1 = \deg g_2 = n-1$，根据假设，存在同构 $\sigma\colon \mathbb{E}_1 \to \mathbb{E}_2$，使得对所有属于 $\mathbb{F}_1(\alpha)$ 的 b，都有 $\sigma(b) = \psi(b)$。因此，对所有属于 $\mathbb{F}_1$的 a，都有 $\sigma(a) = \psi(a) = \varphi(a)$。□

接下来我们证明分裂域的存在性和唯一性。

THEOREM 3.4.1. 在同构意义下，对于每个属于 $\mathbb{F}[x]$ 且满足 次数 $f \geq 1$ 的f，都存在唯一的分裂域。

PROOF. 根据定理 3.3.3，存在一个 $\mathbb{K}$ $\mathbb{F}$ 上的扩张，使得 f 在其中分裂。因此，对于 α_1、α_2、$\cdots$、α_n，$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$。它们都属于 $\mathbb{K}$。[1]于是$\mathbb{F}(\alpha_1$、$\cdots$、$\alpha_n)$是 f的一个分裂域。这证明了分裂域的存在性。

分裂域的唯一性由引理 3.4.1 得出。 □

3.4.2. 一些多项式的分裂域。我们计算一些多项式的分裂域，为计算伽罗瓦群作准备。

(1) 域 $\mathbb{Q}(\sqrt{2})$ 是 $f(x) = x^2 - 2$ 在 $\mathbb{Q}[x]$ 上的分裂域，并且 $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$。[2]

代数学基本定理指出，每个 $\mathbb{C}[x]$ 中的多项式都在 $\mathbb{C}$上分裂。因此，x^2-2 的分裂域 $\mathbb{E}$ 是 $\mathbb{C}$ 的一个子域。由于 $\sqrt{2}$ 是x^2-2的一个根，我们有 $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{E}$。由于 x^2-2 在 $\mathbb{Q}(\sqrt{2})$上分裂，我们有 $\mathbb{E} = \mathbb{Q}(\sqrt{2})$。

此外，$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ 和 $\{1, \sqrt{2}\}$ 在 $\mathbb{Q}$ 上线性无关。因此，$\{1, \sqrt{2}\}$ 是 $\mathbb{Q}(\sqrt{2})$ 在 $\mathbb{Q}$ 上的一组基，且 $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$。

(2) 域 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 是 $\mathbb{Q}[x]$ 中 $f(x) = (x^2-2)(x^2-3)$ 的分裂域，且 $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$。

类似于前面的论证可知，$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 是 $f(x) = (x^2-2)(x^2-3)$ 的分裂域。

接下来我们证明 $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$，这将推出 $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$。

只需证明 x^2-3 在 $\mathbb{Q}(\sqrt{2})[x]$ 中不可约，也就是说，对于所有 a, b，$\mathbb{Q}$ 都不可能是 x^2-3 的根。

假设对于某个 a, b，有 $(a + b\sqrt{2})^2 = 3$。

于是 $a^2 + 2b^2 - 3 = -2ab\sqrt{2}$。由于左边是有理数，因此有$ab = 0$。

当 $a = 0$ 时，我们得到 $2b^2 - 3 = 0$，这不可能，因为 b 是有理数。

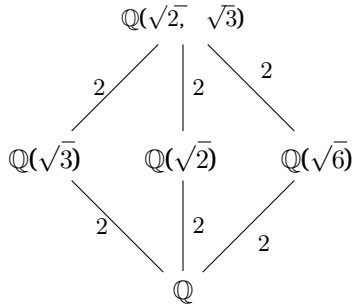
当 $b = 0$ 时，我们得到 $a^2 - 3 = 0$，这同样不可能，因为 a 是有理数。

综上所述，这导致了矛盾。

我们有如下关于 $\mathbb{Q}$ 与 $\mathbb{Q}$（$\sqrt{2}$，$\sqrt{3}$）之间中间域的图示。

---

[1]我们可以假设 f 是首一的。[2]$\mathbb{R}$ 不是分裂域，尽管 f 在 $\mathbb{R}$上分裂。



这里，两个域之间的数字表示上方域关于下方域的维数。例如，$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$。

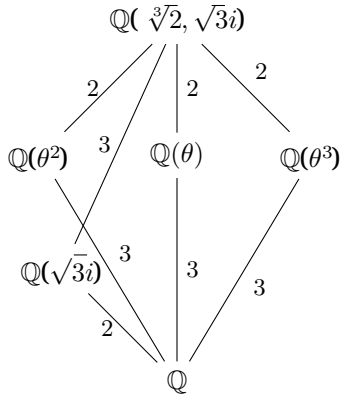
(3) x^3-2 的分裂域是 $\mathbb{Q}(\sqrt[3]{2},\sqrt{3}i)$ 和 $[\mathbb{Q}(\sqrt[3]{2},\sqrt{3}i):\mathbb{Q}]=6$。

设 $\mathbb{E}\subseteq\mathbb{C}$ 是 x^3-2 的分裂域。注意，x^3-2 在 $\mathbb{C}$ 中有 3 个根：$\theta=\sqrt[3]{2}(-\frac{1}{2}+\frac{\sqrt{3}}{2}i)$、$\theta^2=\sqrt[3]{2}(-\frac{1}{2}-\frac{\sqrt{3}}{2}i)$ 和 $\theta^3=\sqrt[3]{2}$。因此，$\sqrt[3]{2}$ 和 $\sqrt{3}i=\theta-\theta^2$ 都属于 $\mathbb{E}$，且 $\mathbb{Q}(\sqrt[3]{2},\sqrt{3}i)\subseteq\mathbb{E}$。此外，$x^3-2$ 在 $\mathbb{Q}(\sqrt[3]{2},\sqrt{3}i)$ 上分裂。因此，$\mathbb{Q}(\sqrt[3]{2},\sqrt{3}i)=\mathbb{E}$。

注意，$[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$，因为 x^3-2 是 $\mathbb{Q}[x]$ 中的不可约多项式；并且 x^2+3 在 $\mathbb{Q}(\sqrt[3]{2})$ 中没有根，因为 $\mathbb{Q}(\sqrt[3]{2})$ 包含于 $\mathbb{R}$。所以，x^2+3 是 $\mathbb{Q}(\sqrt[3]{2})[x]$ 中的不可约多项式，这意味着 $[\mathbb{Q}(\sqrt[3]{2},\sqrt{3}i):\mathbb{Q}(\sqrt[3]{2})]=2$。

最后 $[\mathbb{Q}(\sqrt[3]{2},\sqrt{3}i):\mathbb{Q}]=[\mathbb{Q}(\sqrt[3]{2},\sqrt{3}i):\mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=6$。

下面是 $\mathbb{Q}$ 与 $\mathbb{Q}(\sqrt[3]{2},\sqrt{3}i)$ 之间中间域的示意图。



(4) x^4+4 的分裂域是 $\mathbb{Q}(i)$。

由此可得，x^4+4 在 $\mathbb{C}$ 中的根是 $\pm1\pm i$。

(5) 设 p 为素数。x^p-1 在 $\mathbb{Q}[x]$ 上的分裂域是 $\mathbb{Q}(\zeta_p)$，其中 $\zeta_p=e^{\frac{2\pi i}{p}}$ 且 $[\mathbb{Q}(\zeta_p):\mathbb{Q}]=p-1$，因为 x^p-1 的每个根都是某个 $1\le i\le p$ 的 ζ_p^i，而且 ζ_p 是 $\Phi_p(x)=\frac{x^p-1}{x-1}$ 的一个根，它是 $\mathbb{Q}[x]$ 上的一个次数为 $p-1$ 的不可约多项式。

(6) 在与前一个例子相同的设定下，x^p-2 在 $\mathbb{Q}[x]$ 上的分裂域是 $\mathbb{Q}(\zeta_p,\sqrt[p]{2})$ 和 $[\mathbb{Q}(\zeta_p,\sqrt[p]{2}):\mathbb{Q}]=p(p-1)$。

不难证明，$\mathbb{Q}(\zeta_p,\sqrt[p]{2})$ 是 x^p-2 的分裂域。

由于 Φ_p 属于 $\mathbb{Q}[x] \subseteq \mathbb{Q}(\sqrt[p]{2})[x]$，且 $\Phi_p(\zeta_p) = 0$，我们有

$$[\mathbb{Q}(\zeta_p, \sqrt[p]{2}) : \mathbb{Q}(\sqrt[p]{2})] = [\mathbb{Q}(\sqrt[p]{2})(\zeta_p) : \mathbb{Q}(\sqrt[p]{2})] \leq \deg \Phi_p = p - 1.$$

另外，由于 $\sqrt[p]{2}$ 是 $\mathbb{Q}[x]$ 上的不可约多项式 $x^p - 2$ 的根，因此 $[\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] = \deg(x^p - 2) = p$。

$[\mathbb{Q}(\zeta_p, \sqrt[p]{2}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_p, \sqrt[p]{2}) : \mathbb{Q}(\sqrt[p]{2})][\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] \leq p(p-1)$。

另一方面，$p = [\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}]$ 和 $p - 1 = [\mathbb{Q}(\zeta_p) : \mathbb{Q}]$ 都整除 $[\mathbb{Q}(\zeta_p, \sqrt[p]{2}) : \mathbb{Q}]$。由于 p 与 $p-1$ 互素，我们得到 $p(p-1)$ 是 $[\mathbb{Q}(\zeta_p, \sqrt[p]{2}) : \mathbb{Q}]$ 的一个因子。最后，$[\mathbb{Q}(\zeta_p, \sqrt[p]{2}) : \mathbb{Q}] = p(p-1)$。

(7) $\mathbb{Q}[x]$ 中 $x^n - 1$ 的分裂域是 $\mathbb{Q}(\zeta_n)$，且 $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$，其中 $\zeta_n = e^{\frac{2\pi i}{n}}$，而 $\phi(n)$ 是小于 n 且与之互素的正整数的个数。[3]

$x^n - 1$ 的根集合是一个乘法循环群 $\langle \zeta_n \rangle$，同构于 $\mathbb{Z}_n$，其生成元为 ζ_n^m，其中 $1 \leq m \leq n$ 与 n 互素。因此，$\langle \zeta_n \rangle$ 有 $\phi(n)$ 个生成元。

Define $\Phi_n(x) = \prod_{\substack{1 \leq m \leq n \\ \gcd(m,n)=1}} (x - \zeta_n^m)$ which is called **the n-th cyclotomic polynomial**.

名称i l

我们列出 Φ_n 的一些：

- $\Phi_p(x) = \dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$ when p is prime.
- $\Phi_1(x) = x - 1$.
- $\Phi_4(x) = (x - i)(x + i) = x^2 + 1$.
- $\Phi_6(x) = (x - \zeta_6)(x - \zeta_6^5) = x^2 - x + 1$.
- $\Phi_8(x) = (x - \zeta_8)(x - \zeta_8^3)(x - \zeta_8^5)(x - \zeta_8^7) = x^4 + 1$.
- $\Phi_9(x) = (x - \zeta_9)(x - \zeta_9^2)(x - \zeta_9^4)(x - \zeta_9^5)(x - \zeta_9^7)(x - \zeta_9^8) = x^6 + x^3 + 1$.
- $\Phi_{10}(x) = (x - \zeta_{10})(x - \zeta_{10}^3)(x - \zeta_{10}^7)(x - \zeta_{10}^9) = x^4 - x^3 + x^2 - x + 1$.
- $\Phi_{12}(x) = (x - \zeta_{12})(x - \zeta_{12}^5)(x - \zeta_{12}^7)(x - \zeta_{12}^{11}) = x^4 - x^2 + 1$.

下面的定理将推出 $\mathbb{Q}(\zeta_n) \cong \mathbb{Q}[x]/(\Phi_n)$，因此 $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(\Phi_n) = \phi(n)$。

THEOREM 3.4.2. 对于 $\Phi_n(x)$，以下结论成立：

(i) $\Phi_n(x)$ 属于 $\mathbb{Z}[x]$，且常数项为 ± 1。(ii)

$\Phi_n(x)$ 在 $\mathbb{Q}[x]$ 中不可约。

在继续证明定理之前，我们先介绍一些有关可分多项式的背景知识。

DEFINITION 3.4.2. 若多项式 f 属于 $\mathbb{F}[x]$，且没有重根，则称其为**可分**；否则称其为**不可分**。

EXAMPLES 3.4.1.

(1) 任何一次多项式都是可分的。(2) $x^2 - 3$

属于 $\mathbb{Q}[x]$，且是可分的。

DEFINITION 3.4.3. 多项式 $f(x)$ 的**导数** $= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ 属于 $\mathbb{F}[x]$，定义为多项式 $D(f) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + 2a_2 x + a_1$，属于 $\mathbb{F}[x]$。

导数具有以下性质。

[3] 定义在正整数集合上的函数 ϕ 称为**欧拉 φ 函数**。

Proposition 3.4.1. 对于 f、g 属于 $\mathbb{F}[x]$,

(1) $D(f+g) = D(f) + D(g)$;

(2) $D(fg) = D(f)g + fD(g)$。

下面通过导数给出可分多项式的一个刻画。

Theorem 3.4.3. </style}多项式 在 中可分，当且仅当 与 (f)互素。

Proof. 不失一般性，我们可以假设 f 在 $\mathbb{F}$上分裂。

可以看出， f 与 $D(f)$不互素，当且仅当 f 和 $D(f)$有公共根。接着我们证明， f和 $D(f)$的任一公共根都是 f的重根，由此完成证明。

假设 α 是 f 和 $D(f)$ 的公共根。那么对于 $g\in\mathbb{F}[x]$， $f(x) = (x-\alpha)g(x)$。于是 $D(f) = g+(x-\alpha)D(g)$。由此可得 $g(\alpha) = 0$。因此，对于 $h \in \mathbb{F}[x]$， $g(x) = (x-\alpha)h$。所以 $f(x) = (x-\alpha)^2 h(x)$，这意味着 α 是 f 的重根。

反过来，假设 α 是 f 的重根。那么对于 $h \in \mathbb{F}[x]$， $f(x) = (x-\alpha)^2 h(x)$。于是 $D(f) = 2(x-\alpha)h(x) + (x-\alpha)^2 D(h)$，这意味着 α 也是 $D(f)$ 的根，因此是 f 和 $D(f)$ 的公共根。

□

定理 3.4.3 有一些直接的应用。

(1) $x^{p^n} - x \in \mathbb{F}_p[x]$ 是可分的，因为 $D(x^{p^n} - x) = -1$。(2) 对任意满足特征 $\mathrm{Ch}\mathbb{F}$ 不整除 n 的域 $\mathbb{F}$， $x^n - 1$ 都是可分的，因为$D(x^n - 1) = nx^{n-1}$ 且$1 = \frac{1}{n}x(nx^{n-1}) - (x^n - 1)$，也就是说， $x^n - 1$ 与 $D(x^n - 1)$ 互素。(3) 如果 $\mathrm{Ch}\mathbb{F}$ 整除 n，那么 $x^n - 1$ 不可分，因为 $D(x^n - 1) = nx^{n-1} = 0$。

现在我们已经准备好证明定理 3.4.2。

Proof of Theorem 3.4.2.

（i）我们对 n进行归纳法。

$\Phi_1(x) = x - 1$ 属于 $\mathbb{Z}[x]$，且常数项为 -1。

假设对于每个 $m < n$， Φ_m 属于 $\mathbb{Z}[x]$，且常数项为 ± 1。

在 $\langle\zeta_n\rangle$中，每个元素的阶都是 d 的某个 d，其中 d整除 n；而阶为 d 的元素具有 $\zeta_n^{m\frac{n}{d}} = \zeta_d^m$的形式，其中 $1 \le m \le n$ 与 d互素。

因此

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = \Phi_n(x) \prod_{\substack{1\le d<n \\ d|n}} \Phi_d(x).$$

由假设可知， $\Phi_n(x)$ 属于 $\mathbb{Q}[x]$。

Define $\mathrm{F}_n(x) = \prod_{\substack{1\le d<n \\ d|n}} \Phi_d(x)$.

于是 $x^n - 1 = \mathrm{F}_n\Phi_n$。根据假设，对于所有 $1 \le d < n$ 和 $d|n$，每个 $\Phi_d(x)$ 都属于 $\mathbb{Z}[x]$，且常数项为 ± 1，因此 F_n。

因此， $\Phi_n(x)$ 的常数项为 ± 1。归纳可得， $\Phi_n(x)$ 的每个系数都是整数。

(ii)根据高斯引理，只需证明 $\Phi_n(x)$ 在$\mathbb{Z}[x]$中不可约。

设 f 是 $\mathbb{Z}[x]$ 中的一个不可约首一多项式，它整除 $\Phi_n(x)$。我们将证明每个 ζ_n^m都是 f 的根，由此可知 $f=\Phi_n$ 和 Φ_n不可约。

对于 f 的任意根 ζ，我们证明对任意素数 $p\nmid n$， $f(\zeta^p)=0$，这意味着对任意与 n 互素的 $1\le m\le n$， $f(\zeta_n^m)=0$。

假设存在 $p\nmid n$，使得对 f 的某个根 ζ， $f(\zeta^p)\neq 0$。由于 ζ^p 是 Φ_n 的一个根，因此存在 $\mathbb{Z}[x]$ 中的 g，使得 $\Phi_n=fg$ 且 $g(\zeta^p)=0$。也就是说， ζ 是多项式 $g(x^p)$ 的一个根。于是，对于 $\mathbb{Z}[x]$ 中的 h，有 $g(x^p)=f(x)h(x)$，因为 f 不可约且 ζ 是 f 的一个根。

考虑从 $\mathbb{Z}[x]$ 到 $\mathbb{F}_p[x]$ 的环同态，映射 $q=a_0+a_1x+\cdots+a_kx^k$ 从 $\mathbb{Z}[x]$ 到 $\bar{q}=\bar{a}_0+\bar{a}_1x+\cdots+\bar{a}_kx^k$ 属于 $\mathbb{F}_p[x]$。对于 $g(x)=b_0+b_1x+\cdots+b_lx^l$，有

$$\bar{f}(x)\bar{h}(x)=\bar{g}(x^p)=\bar{b}_0+\bar{b}_1x^p+\cdots+\bar{b}_lx^{lp}=\bar{b}_0^p+\bar{b}_1^px^p+\cdots+\bar{b}_l^px^{lp}=(\bar{g}(x))^p.$$

这里的 $\bar{b}_i^p=\bar{b}_i$ 对 $0\le i\le l$ 可由费马小定理得出。

因此， $f(x)$ 和 $\bar{g}(x)$ 有一个公共根。于是， $\Phi_n=\overline{f\bar{g}}$在$\mathbb{F}_p[x]$中不可分。然而，由于 x^n-1 在 $\overline{\mathbb{F}_p}[x]$中可分， Φ_n 在 $\mathbb{F}_p[x]$ 中可分。这是一个矛盾。

□

域 $\mathbb{Q}(\zeta_n)$ 称为 $\mathbb{Q}$的**分圆扩张**。

3.5. 可分扩张

本节讨论可分扩张，为后续讨论伽罗瓦扩张铺平道路。

PROPOSITION 3.5.1. 假设 $\mathrm{Ch}\mathbb{F}=0$。那么， $\mathbb{F}[x]$ 中的每个不可约多项式都是可分的。此外， $\mathbb{F}[x]$ 中的一个首一多项式可分，当且仅当它是互不相同的首一不可约多项式之积。

PROOF. 如果 $\mathrm{Ch}\mathbb{F}=0$，那么 $D(p)\neq 0$，并且对于 $\mathbb{F}[x]$ 中的每个不可约多项式，$\deg(D(p))<\deg p$。因此， p 与 $D(p)$ 互素。

f 中的每个 f 都是若干不可约多项式的乘积，而 f 的一个根是重根，当且仅当该根是其中至少两个不可约多项式的公共根。然而，不同的不可约多项式没有公共根。这说明， f 可分当且仅当 f 是互不相同的不可约多项式的乘积。□

LEMMA 3.5.1. 设 $\mathbb{F}$ 是一个特征为 $\mathrm{Ch}\mathbb{F}=p$ 的域。那么， $\varphi:\mathbb{F}\to\mathbb{F}$ 定义为：对所有 $a\in\mathbb{F}$，$\varphi(a)=a^p$，这是一个单射环同态。此外，如果 $\mathbb{F}$ 是有限域，那么 φ 是一个同构。

PROOF. 对于所有 $a,b\in\mathbb{F}$，我们有 $\varphi(a+b)=(a+b)^p=\sum_{i=0}^p\binom{p}{i}a^ib^{p-i}=a^p+b^p$，因为对于所有 $1\le i\le p-1$， p 都整除 $\binom{p}{i}$的各项；并且 $\varphi(ab)=(ab)^p=a^pb^p=\varphi(a)\varphi(b)$。因此，$\varphi$是一个环同态。此外， $\varphi(1)=1$，也就是说， φ 是域之间的非零环同态，因此 φ是单射。

当 $\mathbb{F}$ 有限时，注入映射 φ 也是满射，因此是同构。□

DEFINITION 3.5.1. 域 $\mathbb{K}$ 称为**完美**，如果 $\mathrm{Ch}\mathbb{K}=0$ 或者 $\mathbb{K}=\mathbb{K}^p$ 当 $\mathrm{Ch}\mathbb{K}=p$；否则称为**非完美**。

除特征为零的域外，根据引理 3.5.1，有限域也是完美域。

$\mathbb{F}_2[t]$ 的分式域 Frac($\mathbb{F}_2$[t]) $= \{\mathrm{p\,q} \mid \mathrm{p},\ \mathrm{q} \in \mathbb{F}_2[\mathrm{t}], \mathrm{q} \neq 0\}$ 是非完美的，因为不存在 p，q 属于 $\mathbb{F}_2[t]$，使得 $(\frac{p}{q})^2 = t$。

THEOREM 3.5.1. 完美域上的每个不可约多项式都是可分的。此外，完美域上的多项式是可分的，当且仅当它是互不相同的不可约多项式的乘积。

PROOF. 对于特征为零的域，我们已经在命题 3.5.1 中证明了这些结论。

假设 Ch$\mathbb{K} = p$and $\mathbb{K} = \mathbb{K}^p$，这意味着环同态$\varphi : \mathbb{F} \to \mathbb{F}$ 由 $\varphi(a) = a^p$ 定义，对所有属于 $\mathbb{F}$ 的 a 都是满射。

假设 f 在 $\mathbb{F}$ 上不可约。若 f 不可分，则 f 与$D(f)$不互素，也就是说，f 整除 $D(f)$。这只有在 $D(f) = 0$ 时才会发生。因此$f = a_m x^{mp} + a_{m-1}x^{(m-1)p} + \cdots + a_1 x^p + a_0$。由于 φ 是满射，对于所有 $0 \le i \le m$，我们都有 $a_i = b_i^p$。因此

$$\begin{aligned} f &= a_m x^{mp} + a_{m-1}x^{(m-1)p} + \cdots + a_1 x^p + a_0 \\ &= b_m^p x^{mp} + b_{m-1}^p x^{(m-1)p} + \cdots + b_1^p x^p + b_0^p \\ &= (b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0)^p, \end{aligned}$$

这与 f 不可约相矛盾。因此，$\mathbb{F}$上的每个不可约多项式都是可分的。

第二个结论由第一个结论推出，论证与命题3.5.1中的类似。□

DEFINITION 3.5.2. 若域扩张 $\mathbb{K}/\mathbb{F}$ 中每个元素都是 $\mathbb{F}[x]$中某个可分多项式的根，则称域扩张 $\mathbb{K}/\mathbb{F}$ 为**可分扩张** 。

COROLLARY 3.5.1. 完美域的每个有限扩张都是可分扩张。

在非完美域上，存在不可约的不可分多项式。

令 $\mathbb{F} =$ Frac($\mathbb{F}_2$[t])。多项式 $x^2 - t$ 在 $\mathbb{F}[x]$ 中不可约，因为 $x^2 - t$在 $\mathbb{F}$中没有根。此外，$D(x^2 - t) = 2x = 0$，所以最大公因式$(x^2 - t, D(x^2 - t)) = x^2 - t$，这说明 $x^2 - t$ 是不可分的。

习题

EXERCISE 3.1. 证明，$\{v_1, v_2, \cdots, v_n\}$ 是向量空间 V的一个基，当且仅当 $\{v_1, v_2, \cdots, v_n\}$ 是 V的极大线性无关子集。

EXERCISE 3.2. 证明维数$_{\mathbb{Q}}\,\mathbb{R} = \infty$。

EXERCISE 3.3. 证明定理 *3.2.1*。

EXERCISE 3.4. 证明，当一个域的特征非零时，它是素数。

EXERCISE 3.5. 证明 $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$。

EXERCISE 3.6. 设 α 属于 $\mathbb{E}$，且在 $\mathbb{F}$ 上是代数的；p 是 $\mathbb{F}[x]$ 中次数最低的非零首一多项式，使得 $p(\alpha) = 0$。证明$p = m_{\alpha,\mathbb{F}}$。

EXERCISE 3.7. 求 $\mathbb{Q}[x]$ 中 $\sqrt[5]{7} - \sqrt[3]{2}$ 的最小多项式。

EXERCISE 3.8. 证明有限扩张是代数扩张，但反之不成立。

EXERCISE 3.9. 求以下多项式在 $\mathbb{Q}[x]$ 中的分裂域:
(1) $(x^2+2x-2)(x^2-3)$;
(2) x^4-4;(3) x^3+5.

EXERCISE 3.10. 设 p 是素数。证明 $\Phi_p(x) = \dfrac{x^p-1}{x-1}$ 在 $\mathbb{Q}[x]$ 中不可约。

EXERCISE 3.11. 求 x^2+x+1 在 $\mathbb{F}_2[x]$ 中的分裂域。

EXERCISE 3.12. 证明 $\mathbb{Q}[x]$ 中任意形如 x^n+a 的多项式都是可分的。

EXERCISE 3.13. 设 $\mathbb{F}=\mathbb{F}_2(t)$。证明 x^2-t 在 $\mathbb{F}[x]$ 中没有根属于 $\mathbb{F}$。

EXERCISE 3.14. 证明 $\mathbb{Q}(\sqrt{2}+\sqrt{3})^{-} = \mathbb{Q}(\sqrt{2},\sqrt{3})$。求 $\sqrt{2}+\sqrt{3}$ 在 $\mathbb{Q}$上的最小多项式。

EXERCISE 3.15. 确定 $[\mathbb{Q}(\sqrt[3]{2}+\sqrt{2}):\mathbb{Q}]$。

EXERCISE 3.16. 证明对于任意正整数 n, $\mathbb{Q}(\sqrt[3]{2})$ 都不是 $\mathbb{Q}(\zeta_n)$ 的子域。

EXERCISE 3.17. 证明如果 $[\mathbb{F}(\alpha):\mathbb{F}]$ 为奇数，则 $\mathbb{F}(\alpha)=\mathbb{F}(\alpha^2)$。然后证明以下推广：如果 $n\nmid[\mathbb{F}(\alpha):\mathbb{F}]$，则 $[\mathbb{F}(\alpha):\mathbb{F}(\alpha^n)]<n$。

EXERCISE 3.18. 设 $\mathbb{Q}$ 为 $\mathbb{Q}$上的代数数域。证明 $\mathbb{Q}[x]$ 中的每个多项式都在 $\mathbb{Q}$上分裂。也就是说，$\mathbb{Q}$ 是代数闭的。

EXERCISE 3.19. 证明：如果一个子域 $\mathbb{F}$ 包含 ζ_n （其中 n为奇数），那么 $\mathbb{F}$包含 ζ_{2n}。

EXERCISE 3.20. 证明： $\mathbb{K}$ 是 $\mathbb{F}[x]$ 中 f 的分裂域，当且仅当 $\mathbb{F}[x]$ 中的每个在 $\mathbb{K}$ 中有一个根的不可约多项式都在 $\mathbb{K}$上分裂。

EXERCISE 3.21. 证明：如果 $\mathbb{K}_1$ 和 $\mathbb{K}_2$ 是 $\mathbb{F}$上的分裂域，那么 $\mathbb{K}_1\mathbb{K}_2$和 $\mathbb{K}_1\cap\mathbb{K}_2$ 也分别是 $\mathbb{F}$上的分裂域。

EXERCISE 3.22. 证明：对于非零的 a， x^p-x+a 是 $\mathbb{F}_p[x]$中的不可约可分多项式。

第4章

伽罗瓦理论及其应用

4.1. 伽罗瓦扩张的刻画

DEFINITION 4.1.1. 设 $\mathbb{K}$是一个域。

(1) 同构 $\sigma:\mathbb{K}\to\mathbb{K}$ 称为 $\mathbb{K}$的**自同构**。用 Aut($\mathbb{K}$) 表示 $\mathbb{K}$的自同构集合。

(2) 若自同构 σ 满足 $\sigma(a)=a$，则称它固定了 $\mathbb{K}$ 中的元素 a 。(3) 设 $\mathbb{K}/\mathbb{F}$ 是一个域扩张。对于 $\mathbb{F}$}中的所有 a，Aut($\mathbb{K}/\mathbb{F}$) $=\{\sigma\,|\,\sigma(a)=a$。

显然，Aut($\mathbb{K}$)在映射的复合运算下构成一个群，而 Aut($\mathbb{K}/\mathbb{F}$) 是 Aut($\mathbb{K}$) 的子群。对于 Aut($\mathbb{K}/\mathbb{F}$) 的子群 G，定义 $\mathbb{K}^G=\{a\in\mathbb{K}\,|\,\sigma(a)=a$，其中 σ属于 $G\}$。显然， $\mathbb{K}^G$是 $\mathbb{F}$与 $\mathbb{K}$ 之间的一个中间域。

以下说明，自同构群 Aut($\mathbb{K}/\mathbb{F}$) 中的元素是 $\mathbb{F}[x]$ 中多项式根的置换。

PROPOSITION 4.1.1. 设 $\mathbb{K}/\mathbb{F}$ 是一个域扩张，且 α 属于 $\mathbb{K}$，在 $\mathbb{F}$ 上代数。则对于任意 σ 属于 $\mathrm{Aut}(\mathbb{K}/\mathbb{F})$， $\sigma(\alpha)$ 在 $\mathbb{F}$ 上也代数，且与 α 具有相同的最小多项式。

PROOF. 设 $p(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 属于 $\mathbb{F}[x]$，是 α 的最小多项式。那么

$$\begin{aligned}p(\sigma(\alpha))&=\sigma(\alpha)^n+a_{n-1}\sigma(\alpha)^{n-1}+\cdots+a_1\sigma(\alpha)+a_0\\&=\sigma(\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0)=\sigma(p(\alpha))=0.\end{aligned}$$

因此， $\sigma(\alpha)$ 在 $\mathbb{F}$ 上代数，其最小多项式也是 p。 □

伽罗瓦理论主要关注一种特殊类型的域扩张，称为伽罗瓦扩张，它有许多种刻画。下面给出其中一些。

THEOREM 4.1.1. 设 $\mathbb{K}$ 是 $\mathbb{F}$ 的有限扩张。

以下各条件等价:

(1) $\mathbb{K}$ 是可分多项式 $f(x)$ 在 $\mathbb{F}[x]$中的分裂域；(2) $|\mathrm{Aut}(\mathbb{K}/\mathbb{F})|=[\mathbb{K}:\mathbb{F}]$;

(3) $\mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}=\mathbb{F}$；(4) $\mathbb{K}$ 是 $\mathbb{F}$的正规可分扩张，即 $\mathbb{K}$ 的每个元素都是 $\mathbb{F}[x]$中一个可分不可约多项式的根，且该多项式在 $\mathbb{K}$上分裂。

PROOF. 我们证明 (1)⇒(2)⇒(3)⇒(4)⇒(1)。

(1)⇒(2)。

我们对 $[\mathbb{K}:\mathbb{F}]$进行归纳。

设 $[\mathbb{K}:\mathbb{F}]=1$。那么 $\mathbb{K}=\mathbb{F}$。因此 Aut($\mathbb{K}/\mathbb{F}$) $=\{e\}$ 且 $|$Aut($\mathbb{K}/\mathbb{F}$)$|=1=[\mathbb{K}:\mathbb{F}]$。

假设每当 $[\mathbb{K}:\mathbb{E}]<n$ 且 $\mathbb{K}$ 是域 $\mathbb{E}[x]$ 中可分多项式 $g(x)$ 的分裂域时，我们都有 $|$ Aut($\mathbb{K}/\mathbb{E}$)$|=[\mathbb{K}:\mathbb{E}]$。

现在假设 $[\mathbb{K}:\ \mathbb{F}]=n$。

设 α in $\mathbb{K}$ 是 $f(x)$ 的一个根，其中 $\deg(m_{\alpha,\mathbb{F}}(x)=m\geq 2$。注意，$\mathbb{K}$ 也是 $f(x)$ 在 $\mathbb{F}(\alpha)[x]$ 中的一个分裂域。由归纳法可得 $|\mathrm{Aut}(\mathbb{K}/\mathbb{F}(\alpha))|=[\mathbb{K}:\ \mathbb{F}(\alpha)]$。

为方便起见，记 $\mathrm{Aut}(\mathbb{K}/\mathbb{F})$ 为 G，记 $\mathrm{Aut}(\mathbb{K}/\mathbb{F}(\alpha))$ 为 G_α。显然，G_α 是 G 的一个子群。

接下来我们构造一个双射 ψ_α，将 G/G_α 映 onto X_α，其中 X_α 是 $m_{\alpha,\mathbb{F}}(x)$ 的所有根组成的集合。由于 $m_{\alpha,\mathbb{F}}(x)$ 是 $f(x)$ 的一个因子，且 $f(x)$ 是可分的，因此有 $|X_\alpha|=\deg(m_{\alpha,\mathbb{F}}(x))$。所以，该双射给出 $[G:\ G_\alpha]=\deg(m_{\alpha,\mathbb{F}}(x))=[\mathbb{F}(\alpha):\mathbb{F}]$，这意味着 $|G|=|G_\alpha|[G:G_\alpha]=[\mathbb{K}:\ \mathbb{F}(\alpha)][\mathbb{F}(\alpha):\ \mathbb{F}]=[\mathbb{K}:\mathbb{F}]$。

对于 G中的每个 σ，双射 ψ_α 都将 σG_α 映射到 $\sigma(\alpha)$。

每个 $\sigma\in G$ 都会将$m_{\alpha,\mathbb{F}}(x)$ 的根 α映射到$m_{\alpha,\mathbb{F}}(x)$ 的一个根。

如果对 $\sigma,\tau\in G$有 $\sigma G_\alpha=\tau G_\alpha$，那么 $\tau^{-1}\sigma\in G_\alpha$，这意味着 $\tau^{-1}\sigma(\alpha)=\alpha$。因此 $\sigma(\alpha)=\tau(\alpha)$，且 ψ_α 良定义。

如果 $\sigma(\alpha)=\tau(\alpha)$，那么 $\tau^{-1}\sigma(\alpha)=\alpha$，这意味着 $\tau^{-1}\sigma\in G_\alpha$且 $\sigma G_\alpha=\tau G_\alpha$。所以 ψ_α 是单射。

为了证明 ψ_α的满射性，我们需要以下引理。

LEMMA 4.1.1. 设 $\mathbb{K}$ 是域$\mathbb{F}[x]$上可分多项式 f 的分裂域，且 $\mathbb{K}$ 中的 α、β是 f 的一个不可约因子 p 的根。那么存在 $\sigma\in\mathrm{Aut}(\mathbb{K}/\mathbb{F})$，使得 $\sigma(\alpha)=\beta$。

PROOF. 首先，存在一个同构 φ，它在 $\mathbb{F}(\alpha)$ 与 $\mathbb{F}(\beta)$ 之间建立对应，将α 映到 β，并固定 $\mathbb{K}$中的所有元素。由于 f 属于 $\mathbb{F}(\alpha)[x]$ 和 $\mathbb{F}(\beta)[x]$，且 $\mathbb{K}$是 f的分裂域，根据引理 3.4.1，存在一个同构 $\sigma:\ \mathbb{K}\to\mathbb{K}$，使得对所有属于 $\mathbb{F}(\alpha)$ 的 a，都有$\sigma(a)=\varphi(a)$。由此可得，σ 属于自同构群 $\mathrm{Aut}(\mathbb{K}/\mathbb{F})$，且 $\sigma(\alpha)=\beta$。□

根据引理 4.1.1，对每个 $\beta\in X_\alpha$，都可以找到 $\sigma\in G$，使得 $\sigma(\alpha)=\beta$。

因此，ψ_α 是满射。

(2)⇒(3)。

目标是证明 $[\mathbb{K}:\ \mathbb{K}^{\mathrm{Aut}}(\mathbb{K}/\mathbb{F})]\geq|\mathrm{Aut}(\mathbb{K}/\mathbb{F})|$。若能证明这一点，注意到 $\mathbb{F}$ 是 $\mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}$的子域，则

$$[\mathbb{K}:\mathbb{F}]\geq[\mathbb{K}:\mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}]\geq|\mathrm{Aut}(\mathbb{K}/\mathbb{F})|=[\mathbb{K}:\mathbb{F}],$$

这意味着 $\mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}=\mathbb{F}$。

不等式 $[\mathbb{K}:\mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}]\geq|\mathrm{Aut}(\mathbb{K}/\mathbb{F})|$ 是下述定理的特例 [Art44，定理 13]。

THEOREM 4.1.2. 设 $\{\sigma_1,\sigma_2,\cdots,\sigma_n\}$ 是 $Aut(\mathbb{K})$ 的一个子集，且 $\mathbb{E}=\{a\in\mathbb{K}|\,\sigma_i(a)=a$对所有$1\leq i\leq n\}$成立，它的不动域为 $[\mathbb{K}:\ \mathbb{E}]\geq n$。

我们首先需要一个关于群特征的预备结果，其适用的背景比我们所需的更一般。

DEFINITION 4.1.2. 从群 G到 $\mathbb{F}^\times$（域 $\mathbb{F}$中非零元素构成的乘法群）的群同态称为**特征**。若 σ_1，$\cdots$，σ_n在 $\mathbb{F}$上**线性无关**，是指在 $\mathbb{F}$中满足对所有 $x\in G$ 都有 $\sum_{i=1}^n\lambda_i\sigma_i(x)=0$的 $\lambda_i's$全为零；否则称 σ_1，$\cdots$，σ_n在 $\mathbb{F}$上**线性相关**。

THEOREM 4.1.3. 一组（互不相同的）特征 $\{\sigma_1,\sigma_2,\cdots,\sigma_n\}$ 线性无关。

PROOF. 显然，$\{\sigma_1\}$ 线性无关，因为 σ_1 非零。

假设任意少于 n 个不同特征的集合都是线性无关的。

现在假设 $\{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ 线性相关。那么存在非零的 a_1、a_2、$\cdots$、a_n，使得对所有 $x \in G$，$\sum_{i=1}^{n} a_i\sigma_i(x) = 0$。注意，每个 a_i 都必须非零，否则会与假设矛盾。因此，对 G 中的每个 x，都有 $a_1a_n^{-1}\sigma_1(x) + a_2a_n^{-1}\sigma_2(x) + \cdots + a_{n-1}a_n^{-1}\sigma_{n-1}(x) + \sigma_n(x) = 0$。由于 $\sigma_1 \neq \sigma_n$，对于某个 y，有 $\sigma_1(y) \neq \sigma_n(y)$。于是，对 G 中的每个 x，都有 $a_1a_n^{-1}\sigma_1(yx) + a_2a_n^{-1}\sigma_2(yx) + \cdots + a_{n-1}a_n^{-1}\sigma_{n-1}(yx) + \sigma_n(yx) = 0$。由此可得，对 G 中的每个 x，$a_1a_n^{-1}\sigma_n(a^{-1})\sigma_1(y)\sigma_1(x) + a_2a_n^{-1}\sigma_n(y^{-1})\sigma_2(y)\sigma_2(x) + \cdots + a_{n-1}a_n^{-1}\sigma_n(y^{-1})\sigma_{n-1}(y)\sigma_{n-1}(x) + \sigma_n(x) = 0$。因此

$$a_1a_n^{-1}(\sigma_1(y)\sigma_n(y^{-1}) - 1)\sigma_1(x) + (a_2a_n^{-1}\sigma_n(y^{-1})\sigma_2(y) - a_2a_n^{-1})\sigma_2(x) + \cdots + (a_{n-1}a_n^{-1}\sigma_n(y^{-1})\sigma_{n-1}(y) - a_{n-1}a_n^{-1})\sigma_{n-1}(x) = 0$$

对每个 x 都属于 G。但是 $a_1a_n^{-1}(\sigma_1(y)\sigma_n(y^{-1}) - 1) \neq 0$，这与 $\{\sigma_1, \cdots, \sigma_{n-1}\}$ 在 $\mathbb{F}$上线性无关相矛盾。□

PROOF. [定理 4.1 的证明。2]

设 $r = [\mathbb{K}: \mathbb{E}] < n$。令 $\{v_1, v_2, \cdots, v_r\}$ 为 $\mathbb{K}$ 在 $\mathbb{E}$上的一组基。考虑齐次线性方程组

$$\begin{aligned} x_1\sigma_1(v_1) + x_2\sigma_2(v_1) + \cdots + x_n\sigma_n(v_1) &= 0 \\ x_1\sigma_1(v_2) + x_2\sigma_2(v_2) + \cdots + x_n\sigma_n(v_2) &= 0 \\ \cdots \qquad\qquad \cdots \qquad\qquad \cdots & \\ x_1\sigma_1(v_r) + x_2\sigma_2(v_r) + \cdots + x_n\sigma_n(v_r) &= 0. \end{aligned}$$

注意到该方程组的未知数多于方程数，因此它有一个非零解，记为 x_1，x_2，$\cdots$，x_n属于 $\mathbb{K}$。$\mathbb{K}$中的每个 a都是 v_1，v_2，$\cdots$，v_n的线性组合，因此 $x_1\sigma_1(a) + x_2\sigma_2(a) + \cdots + x_n\sigma_n(a) = 0$。这意味着 $\{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ 在 $\mathbb{K}$上线性无关。这与定理 4.1 矛盾。3 □

（3）⇒（4）。

设 α in $\mathbb{K}$ 是 $p(x)$ 在 $\mathbb{F}[x]$ 中的一个不可约多项式的根。令 G =Aut($\mathbb{K}/\mathbb{F}$) $= \{\sigma_1, \sigma_2, \cdots, \sigma_n\}$。设 $\{\alpha, \alpha_1, \alpha_2, \cdots, \alpha_r\}$ 是 $\{\sigma_1(\alpha)\ \sigma_2(\alpha)\ \cdots,\ \sigma_n(\alpha)\}$ 的所有互不相同的元素。

考察 $q(x) = (x-\alpha)(x-\alpha_1)\cdots(x-\alpha_r)$。注意到，对于所有 $1 \leq i \leq n$，q 都被 σ_i 固定，因为每个 σ_i 都是 $\{\alpha, \alpha_1, \alpha_2, \cdots, \alpha_r\}$ 的一个置换。因此，q 的所有系数都被 G 固定。根据（3），$\mathbb{K}^G = \mathbb{F}$。所以 q 的所有系数都在 $\mathbb{F}$ 中，也就是说，q 在 $\mathbb{F}[x]$ 中。注意到 $q(\alpha) = 0$，且 deg(q) $\leq$ deg(p)。因此我们得到 $q = p$。

因此，p 是可分的，并且 p 的所有根都在 $\mathbb{K}$中。

（4）⇒（1）。

设 $\{v_1, v_2, \cdots, v_n\}$ 是 $\mathbb{K}$ 在 $\mathbb{F}$上的一组基。

因此，可以找到首一可分不可约多项式 p_i（x），它们属于 $\mathbb{F}[x]$，使得对于每个 $1 \leq i \leq n$，都有 p_i（v_i）$= 0$。设 f（x）是所有互不相同的 $p_i's$的乘积。因此，f 是可分的，因为每个 p_i 都是可分的，并且 $\mathbb{K}$ 是 f（x）的分裂域。

□

REMARK 4.1.1. 引理 4.1.1 表明，自同构群 Aut（$\mathbb{K}/\mathbb{F}$）在 $\mathbb{F}[x]$ 中一个在 $\mathbb{K}$上分裂的不可约多项式 p（x）的根上作用是传递的；也就是说，任意一个 p 的根在自同构群 Aut（$\mathbb{K}/\mathbb{F}$）作用下的轨道包含 p的所有根。

DEFINITION 4.1.3. 如果有限扩张 $\mathbb{K}$ 是 $\mathbb{F}$，且满足定理 4.1.1 中的四个条件之一，则称其为**伽罗瓦扩张**。此时，用 Gal($\mathbb{K}/\mathbb{F}$) 表示 Aut($\mathbb{K}/\mathbb{F}$)。

考虑域扩张 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$。$\mathrm{Aut}(\mathbb{Q}(\sqrt{2}))$ 中的每个 σ 都满足$\sigma(1) = 1$。因此，$\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2}))$。$\sqrt{2}$ 的最小多项式是$x^2 - 2$，其根为 $\pm\sqrt{2}$。$\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{e, \sigma\}$，其中对于 $\mathbb{Q}$中的所有 a, b， $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$。于是 $|\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = 2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$。因此， $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 是伽罗瓦扩张。

考虑域扩张 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$。此外，$\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}))$。$\sqrt[3]{2}$ 的最小多项式是 $x^3 - 2$，其根为 $\sqrt[3]{2}$、 $\sqrt[3]{2}(-\frac{1}{2} + \frac{\sqrt{3}}{2}i)$ 和 $\sqrt[3]{2}(-\frac{1}{2} - \frac{\sqrt{3}}{2}i)$。对于$\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ 中的每个 σ， $\sigma(\sqrt[3]{2})$ 不可能是 $\sqrt[3]{2}(-\frac{1}{2} + \frac{\sqrt{3}}{2}i)$ 或 $\sqrt[3]{2}(-\frac{1}{2} - \frac{\sqrt{3}}{2}i)$；否则 $\sqrt{3}i$ 属于 $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$，这就产生了矛盾。因此 $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$。所以 $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ 只包含恒等映射，这意味着 $|\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1 < [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$。因此 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 不是伽罗瓦扩张。

4.2. 伽罗瓦理论基本定理

本节将证明伽罗瓦理论基本定理。设 $\mathbb{K}$ 是一个域， H 是 $\mathrm{Aut}(\mathbb{K})$ 的一个子群。定义

$$\mathbb{K}^H = \{a \in \mathbb{K} \mid \sigma(a) = a \text{ for all } \sigma \text{ in } H\}.$$

LEMMA 4.2.1. $\mathbb{K}^H$ 是 $\mathbb{K}$ 的一个子域。

PROOF. 如果 a, b 属于 $\mathbb{K}^H$，那么对于 H 中的每个 σ，都有 $\sigma(a - b) = \sigma(a) - \sigma(b) = a - b$，这意味着 $a - b$ 属于 $\mathbb{K}^H$。

如果 a, b 属于 $\mathbb{K}^H$ 和 $b \neq 0$，那么对于 H 中的所有 σ，都有 $\sigma(ab^{-1}) = \sigma(a)\sigma(b^{-1}) = \sigma(a)\sigma(b)^{-1} = ab^{-1}$，这意味着 ab^{-1} 属于 $\mathbb{K}^H$。

由上可知， $\mathbb{K}^H$ 是 $\mathbb{K}$ 的一个子域。 □

EXAMPLES 4.2.1.

(1) Recall that $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{e, \sigma\}$ where σ is given by $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$ for all a, b in $\mathbb{Q}$. If $\sigma(a + b\sqrt{2}) = a + b\sqrt{2}$, then $b = 0$. Hence $\mathbb{Q}(\sqrt{2})^{\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})} = \mathbb{Q}$.

(2) $\mathbb{Q}(\sqrt[3]{2})^{\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})} = \mathbb{Q}(\sqrt[3]{2})^{\{e\}} = \mathbb{Q}(\sqrt[3]{2})$.

THEOREM 4.2.1 伽罗瓦理论的基本定理。 f G l Th)

设 $\mathbb{K}$ 是 $\mathbb{F}$ 的伽罗瓦扩张。

映射 Φ： $\mathcal{IF} = \{\text{包含 } \mathbb{K}\text{的子域 } \mathbb{F}\} \to \mathcal{SG} = \{\mathrm{Gal}(\mathbb{K}/\mathbb{F})\}$由 $\Phi(\mathbb{E}) = \mathrm{Aut}(\mathbb{K}/\mathbb{E})$ 给出，是一个双射，其逆映射 Ψ： $\mathcal{SG} \to \mathcal{IF}$ 由 $\Psi(H) = \mathbb{K}^H$给出。此外，以下结论成立。

(1) $\mathbb{K}$ 始终是 $\mathbb{E}$ 的伽罗瓦扩张，且 $[\mathbb{E} : \mathbb{F}] = |\mathit{Gal}(\mathbb{K}/\mathbb{F}) : \mathit{Gal}(\mathbb{K}/\mathbb{E})|$; *(2)* $\mathbb{E}$ 是 $\mathbb{F}$ 的伽罗瓦扩张，当且仅当 $\mathit{Gal}(\mathbb{K}/\mathbb{E})$ 是 $\mathit{Gal}(\mathbb{E}/\mathbb{F})$ 的正规子群，并且 $\mathit{Gal}(\mathbb{E}/\mathbb{F}) \cong \mathit{Gal}(\mathbb{K}/\mathbb{F})/\mathit{Gal}(\mathbb{K}/\mathbb{E})$； *(3)* 对于 $\mathbb{E}_1$ 和 $\mathbb{E}_2$，若它们属于 $\mathcal{IF}$，则有 $\mathbb{E}_1 \subseteq \mathbb{E}_2$ 当且仅当 $\mathit{Gal}(\mathbb{K}/\mathbb{E}_1) \supseteq \mathit{Gal}(\mathbb{K}/\mathbb{E}_2)$。此外，$\mathit{Gal}(\mathbb{K}/\mathbb{E}_1 \cap \mathbb{E}_2) = \mathit{Gal}(\mathbb{K}/\mathbb{E}_1) \vee \mathit{Gal}(\mathbb{K}/\mathbb{E}_2)$ [1]，且 $\mathit{Gal}(\mathbb{K}/\mathbb{E}_1\mathbb{E}_2) = \mathit{Gal}(\mathbb{K}/\mathbb{E}_1) \cap \mathit{Gal}(\mathbb{K}/\mathbb{E}_2)$。

为了证明定理 4.2.1，我们需要一些预备知识。

THEOREM 4.2.2. 设 G 是 $\mathrm{Aut}(\mathbb{K})$ 的有限子群。那么 $[\mathbb{K} : \mathbb{K}^G] = |G|$.

[1]对于群 G 的子群 H_1 和 H_2，记号 $H_1 \vee H_2$ 表示包含 H_1 和 H_2 的 G 的最小子群。

PROOF. 根据定理 4.1.2，我们有 $[\mathbb{K}\colon \mathbb{K}^G] \geq |G|$。我们通过反证法证明 $[\mathbb{K}:\mathbb{K}^G] \leq |G|$。将群 G 记为 $\{\sigma_1, \sigma_2, \cdots, \sigma_n\}$，并假设 $[\mathbb{K}:\mathbb{K}^G] > n$。设 $\{v_1, v_2, \cdots, v_{n+1}\}$ 是 $\mathbb{K}$ 在 $\mathbb{K}^G$上的一个线性无关集。考虑齐次线性方程组

$$\begin{aligned} &x_1\sigma_1(v_1) + x_2\sigma_1(v_2) + \cdots + x_{n+1}\sigma_1(v_{n+1}) = 0 \\ &x_1\sigma_2(v_1) + x_2\sigma_2(v_2) + \cdots + x_{n+1}\sigma_2(v_{n+1}) = 0 \\ &\cdots \qquad\qquad \cdots \qquad\qquad \cdots \\ &x_1\sigma_n(v_1) + x_2\sigma_n(v_2) + \cdots + x_{n+1}\sigma_n(v_{n+1}) = 0. \end{aligned} \tag{4.1}$$

这个方程组的未知数多于方程，因此在 $\mathbb{K}$中有非零解。设（y_1，y_2，$\cdots$，y_{n+1}）是非零项最少的一个解。不失一般性，可以假设（y_1，y_2，$\cdots$，y_{m-1}，1，0，$\cdots$，0）就是这样的解。显然，$m \geq 2$。此外

$$\begin{aligned} &y_1\sigma_1(v_1) + y_2\sigma_1(v_2) + \cdots + y_{m-1}\sigma_1(v_{m-1}) + \sigma_1(v_m) = 0 \\ &y_1\sigma_2(v_1) + y_2\sigma_2(v_2) + \cdots + y_{m-1}\sigma_2(v_{m-1}) + \sigma_2(v_m) = 0 \\ &\cdots \qquad\qquad \cdots \qquad\qquad \cdots \\ &y_1\sigma_n(v_1) + y_2\sigma_n(v_2) + \cdots + y_{m-1}\sigma_n(v_{m-1}) + \sigma_n(v_m) = 0. \end{aligned} \tag{4.2}$$

并非每个 y_j for $1 \leq j \leq m$都属于 $\mathbb{K}^G$，否则将与 $\{v_1, v_2, \cdots, v_m\}$的线性无关性矛盾。为方便起见，假设 $y_1 \notin \mathbb{K}^G$。那么存在 σ_{k_0}，使得 $\sigma_{k_0}(y_1) \neq y_1$。

令 σ_{k_0} 作用于 4.2 的两边。于是得到σ_{k_0} y_1）$\sigma_{k_0}\sigma_1$（v_1）$+\sigma_{k_0}$（y_2）$\sigma_{k_0}\sigma_1$（v_2）$+\cdots+\sigma_{k_0}$（y_{m-1}）$\sigma_{k_0}\sigma_1$（v_{m-1}）$+\sigma_{k_0}\sigma_1$（v_m）$=0\sigma_{k_0}$（y_1）$\sigma_{k_0}\sigma_2$（v_1）$+\sigma_{k_0}$（y_2）$\sigma_{k_0}\sigma_2$（v_2）$+\cdots+\sigma_{k_0}$（y_{m-1}）$\sigma_{k_0}\sigma_2$（v_{m-1}）$+\sigma_{k_0}\sigma_2$（v_m）$=0$。。。。。。。。。。 (4.3)

$$\sigma_{k_0}(y_1)\sigma_{k_0}\sigma_n(v_1) + \sigma_{k_0}(y_2)\sigma_{k_0}\sigma_n(v_2) + \cdots + \sigma_{k_0}(y_{m-1})\sigma_{k_0}\sigma_n(v_{m-1}) + \sigma_{k_0}\sigma_n(v_m) = 0$$

由于 G是一个群，因此有 $\{\sigma_{k_0}\sigma_1, \sigma_{k_0}\sigma_2, \cdots, \sigma_{k_0}\sigma_n\} = \{\sigma_1, \sigma_2, \cdots, \sigma_n\}$。

因此，$\{\sigma_{k_0}(y_1)\ \sigma_{k_0}(y_2)\ \cdots,\ \sigma_{k_0}(y_{m-1})\ 1,\ 0,\ \cdots,\ 0\}$ 也是线性方程组 4.1 的一个解。由 $y_1 - \sigma_{k_0}(y_1) \neq 0$ 可知，$\{\sigma_{k_0}(y_1) - y_1,\ \sigma_{k_0}(y_2) - y_2,\ \cdots,\ \sigma_{k_0}(y_{m-1}) - y_{m-1},\ 0,\ 0,\ \cdots,\ 0\}$ 是 4.1 的一个非零解，而 4.1 至多只有 $m-1$ 个非零项。

这与 4.1 的解至少有 m 个非零项相矛盾。 □

PROOF OF THEOREM 4.2.1. 根据定理 4.1.1(1)，$\mathbb{K}$是域 $\mathbb{F}[x]$中可分多项式 $f(x)$的分裂域。对于每个包含 $\mathbb{F}$且位于 $\mathbb{K}$ 中的子域 $\mathbb{E}$，$\mathbb{K}$ 也是域 $\mathbb{E}[x]$中多项式 $f(x)$的分裂域。因此，$\mathbb{K}$ 是 $\mathbb{E}$ 的伽罗瓦扩张。

对于 $\mathcal{IF}$中的每个 $\mathbb{E}$，都有 $\Psi\Phi(\mathbb{E}) = \Psi$(自同构群($\mathbb{K}/\mathbb{E}$)) $= \mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{E})} = \mathbb{E}$，因为 $\mathbb{K}/\mathbb{E}$ 是伽罗瓦扩张。

对于 $\mathcal{SG}$中的每个 H，都有 $\Phi\Psi(H) = \Phi(\mathbb{K}^H)$ =自同构群($\mathbb{K}/\mathbb{K}^H$)。显然，H是自同构群($\mathbb{K}/\mathbb{K}^H$)的子群。此外，由于 $\mathbb{K}/\mathbb{K}^H$ 是伽罗瓦扩张，我们得到 |自同构群($\mathbb{K}/\mathbb{K}^H$)| = $[\mathbb{K}\colon \mathbb{K}^H]$。由定理 4.2.2可知 $[\mathbb{K}\colon \mathbb{K}^H] = |H|$。因此 |自同构群($\mathbb{K}/\mathbb{K}^H$)| = $|H|$，这意味着 H =自同构群($\mathbb{K}/\mathbb{K}^H$)。

总而言之，我们已经证明 $\Psi\Phi$ 是 $\mathcal{IF}$ 上的恒等映射，且 $\Phi\Psi$ 是 $\mathcal{SG}$ 上的恒等映射。

(1) 我们已经证明 $\mathbb{K}$ 是 $\mathbb{E}$ 的伽罗瓦扩张。此外，$[\mathbb{K}:\mathbb{F}] = [\mathbb{K}:\mathbb{E}][\mathbb{E}:\mathbb{F}]$。注意，$[\mathbb{K}:\mathbb{F}] = |\mathrm{Gal}(\mathbb{K}/\mathbb{F})|$ 且 $[\mathbb{K}:\mathbb{E}] = |\mathrm{Gal}(\mathbb{K}/\mathbb{E})|$。因此，$[\mathbb{E}:\mathbb{F}] = |\mathrm{Gal}(\mathbb{K}/\mathbb{F}) : \mathrm{Gal}(\mathbb{K}/\mathbb{E})|$。

(2) 假设 $\mathrm{Gal}(\mathbb{K}/\mathbb{E})$ 是 $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ 的正规子群。可以定义 $\varphi : \mathrm{Gal}(\mathbb{K}/\mathbb{F})/\mathrm{Gal}(\mathbb{K}/\mathbb{E}) \to \mathrm{Aut}(\mathbb{E}/\mathbb{F})$，其中 $\varphi(\sigma\mathrm{Gal}(\mathbb{K}/\mathbb{E})) = \sigma|_{\mathbb{E}}$ 对 $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ 中的每个 σ 都成立。

为验证 φ 是良定义的，需要验证对于每个 $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$，都有 $\sigma(\mathbb{E}) = \mathbb{E}$。

注意到 $\mathbb{K}$ 是 $\mathbb{E}$ 的伽罗瓦扩张，因此根据定理 4.1.1(3)，有 $\mathbb{E} = \mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{E})}$。此外，我们还有

Claim 4.2.2.1. *$\sigma(\mathbb{E}) = \mathbb{K}^{\sigma\mathrm{Gal}(\mathbb{K}/\mathbb{E})\sigma^{-1}}$ for every $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$.*

Proof. 对于 $\mathbb{E}$ 中的每个 a 以及 $\mathrm{Gal}(\mathbb{K}/\mathbb{E})$ 中的每个 $\tau \in$，都有 $\sigma\tau\sigma^{-1}(\sigma(a)) = \sigma(a)$。因此，$\sigma(\mathbb{E}) \subseteq \mathbb{K}^{\sigma\mathrm{Gal}(\mathbb{K}/\mathbb{E})\sigma^{-1}}$。
另一方面，对于每个 $b \in \mathbb{K}^{\sigma\mathrm{Gal}(\mathbb{K}/\mathbb{E})\sigma^{-1}}$，都有 $\sigma\tau\sigma^{-1}(b) = b$ 对于每个$\tau \in \mathrm{Gal}(\mathbb{K}/\mathbb{E})$。因此，$\sigma^{-1}(b)$ 属于 $\mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{E})} = \mathbb{E}$，也就是说，$b$ 属于 $\sigma(\mathbb{E})$。所以$\sigma(\mathbb{E}) \supseteq \mathbb{K}^{\sigma\mathrm{Gal}(\mathbb{K}/\mathbb{E})\sigma^{-1}}$。□

由于 $\mathrm{Gal}(\mathbb{K}/\mathbb{E})$ 是 $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ 的正规子群，我们得到对于每个 $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$，都有 $\sigma(\mathbb{E}) = \mathbb{E}$。
不难验证，φ 是一个单射群同态。
对于每个 $\tau \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$，都可以找到 $\mathbb{K}$ 上的一个自同构 $\hat{}\tau$，使得 $\hat{}\tau|_{\mathbb{E}} = \tau$，因为 $\mathbb{K}$ 是 $\mathbb{F}[x]$ 中某个可分多项式的分裂域。这说明 φ是满射。

因此 $|\mathrm{Aut}(\mathbb{E}/\mathbb{F})| = |\mathrm{Gal}(\mathbb{K}/\mathbb{F}) : \mathrm{Gal}(\mathbb{K}/\mathbb{E})| = \frac{[\mathbb{K}:\mathbb{F}]}{[\mathbb{K}:\mathbb{E}]} = [\mathbb{E}:\mathbb{F}]$。因此，根据定理 4.1.1(2)，$\mathbb{E}$是 $\mathbb{F}$ 的伽罗瓦扩张。
假设 $\mathbb{E}$ 是 $\mathbb{F}$的伽罗瓦扩张。我们将证明，对于每个 $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$，都有 $\sigma(\mathbb{E}) = \mathbb{E}$。

证明这一点后，我们可以定义一个从 $\mathrm{Gal}(\mathbb{K}/\mathbb{F}) \to \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ 到群同态，将 σ 映射到 $\sigma|_{\mathbb{E}}$。该同态的核是 $\mathrm{Gal}(\mathbb{K}/\mathbb{E})$。因此，$\mathrm{Gal}(\mathbb{K}/\mathbb{E})$ 是 $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ 的正规子群。

根据假设，$\mathbb{E}$ 是 $\mathbb{F}[x]$ 中可分多项式 f 的分裂域。设α_1、α_2、$\cdots$、$\alpha_n \in \mathbb{E}$是 $f(x)$ 的所有根。因此 $\mathbb{E} = \mathbb{F}(\alpha_1, \cdots, \alpha_n)$，且 $\sigma(\mathbb{E}) = \mathbb{F}(\sigma(\alpha_1) \cdots, \sigma(\alpha_n))$。由于 σ属于 $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$，$\sigma(\alpha_1) \cdots$、$\sigma(\alpha_n)$都是$f(x)$ 的根。因此 $\sigma(\mathbb{E}) \subseteq \mathbb{E}$。注意，$[\sigma(\mathbb{E}) : \mathbb{F}] = [\sigma(\mathbb{E}) : \sigma(\mathbb{F})] = [\mathbb{E}:\mathbb{F}]$。因此 $\sigma(\mathbb{E}) = \mathbb{E}$。

(3) 显然 's obvious that $\mathbb{E}_1 \subseteq \mathbb{E}_2$ 蕴含 $\mathrm{Gal}(\mathbb{K}/\mathbb{E}_1) \supseteq \mathrm{Gal}(\mathbb{K}/\mathbb{E}_2)$。
反向结论由 $\mathbb{E}_1 = \mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{E}_1)}$ 和 $\mathbb{E}_2 = \mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{E}_2)}$ 得出。
由此可知，$\mathrm{Gal}(\mathbb{K}/\mathbb{E}_1)$ 和 $\mathrm{Gal}(\mathbb{K}/\mathbb{E}_2)$ 是 $\mathrm{Gal}(\mathbb{K}/\mathbb{E}_1 \cap \mathbb{E}_2)$ 的子群。因此，$\mathrm{Gal}(\mathbb{K}/\mathbb{E}_1) \vee \mathrm{Gal}(\mathbb{K}/\mathbb{E}_2)$ 也是 $\mathrm{Gal}(\mathbb{K}/\mathbb{E}_1 \cap \mathbb{E}_2)$ 的子群。
另一方面，$\mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{E}_1)\vee\mathrm{Gal}(\mathbb{K}/\mathbb{E}_2)}$ 是 $\mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{E}_1)} = \mathbb{E}_1$ 和$\mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{E}_2)} = \mathbb{E}_2$的子域。因此，$\mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{E}_1)\vee\mathrm{Gal}(\mathbb{K}/\mathbb{E}_2)}$ 是 $\mathbb{E}_1 \cap \mathbb{E}_2$ 的子域。因此，$\mathrm{Gal}(\mathbb{K}/\mathbb{E}_1)\vee\mathrm{Gal}(\mathbb{K}/\mathbb{E}_2) = \mathrm{Gal}(\mathbb{K}/\mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{E}_1)\vee\mathrm{Gal}(\mathbb{K}/\mathbb{E}_2)})$是$\mathrm{Gal}(\mathbb{K}/\mathbb{E}_1\cap\mathbb{E}_2)$的子群。

由于 $\mathbb{E}_1$和 $\mathbb{E}_2$ 是 $\mathbb{E}_1\mathbb{E}_2$的子域，$\mathrm{Gal}(\mathbb{K}/\mathbb{E}_1\mathbb{E}_2) \subseteq \mathrm{Gal}(\mathbb{K}/\mathbb{E}_1)\cap\mathrm{Gal}(\mathbb{K}/\mathbb{E}_2)$。此外，如果 σ 属于 $\mathrm{Gal}(\mathbb{K}/\mathbb{E}_1)\cap\mathrm{Gal}(\mathbb{K}/\mathbb{E}_2)$，那么它会固定 $\mathbb{E}_1$ 和 $\mathbb{E}_2$。因此，σ 固定$\mathbb{E}_1\mathbb{E}_2$。所以 $\mathrm{Gal}(\mathbb{K}/\mathbb{E}_1\mathbb{E}_2) \supseteq \mathrm{Gal}(\mathbb{K}/\mathbb{E}_1)\cap\mathrm{Gal}(\mathbb{K}/\mathbb{E}_2)$。□

4.3. 伽罗瓦群的计算

可分多项式的伽罗瓦群 $f(x)$ 在 $\mathbb{F}[x]$ 中表示伽罗瓦群 $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$，其中 $\mathbb{K}$ 是 f的分裂域。

(1) $\mathbb{Q}(\sqrt{2},\ \sqrt{3})/\mathbb{Q}$的伽罗瓦群：

$\mathbb{Q}(\sqrt{2},\sqrt{3})$ 是 $(x^2-2)(x^2-3)$ 在 $\mathbb{Q}[x]$ 中的分裂域，因此 $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$是一个伽罗瓦扩张。此外，$G=\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})=\{e,\sigma,\tau,\sigma\tau\}$ 其中σ：$\mathbb{Q}(\sqrt{2},\sqrt{3})\to\mathbb{Q}(\sqrt{2},\sqrt{3})$ 由 $\sigma(\sqrt{2})=-\sqrt{2}$ 给出，且 $\sigma(\sqrt{3})=\sqrt{3}$，而$\tau$：$\mathbb{Q}(\sqrt{2},\sqrt{3})\to\mathbb{Q}(\sqrt{2},\sqrt{3})$ 由 $\tau(\sqrt{2})=\sqrt{2}$ 给出，且 $\sigma(\sqrt{3})=-\sqrt{3}$。

将 $\mathbb{Q}(\sqrt{2},\ \sqrt{3})$ 记作 $\mathbb{K}$。

G 的子群与 $\mathbb{Q}$ 和 $\mathbb{K}$ 之间的中间域之间的对应关系如下图所示：

H	$\mathbb{K}^H$
$\{e\}$	$\mathbb{Q}(\sqrt{2},\ \sqrt{3})$
$\{e,\sigma\}$	$\mathbb{Q}(\sqrt{3})$
$\{e,\tau\}$	$\mathbb{Q}(\sqrt{2})$
$\{e,\sigma\tau\}$	$\mathbb{Q}(\sqrt{6})$
G	$\mathbb{Q}$

(2) $\mathbb{Q}(\sqrt[3]{2},\ \sqrt{3}i)/\mathbb{Q}$ 的伽罗瓦群：$\mathbb{Q}(\sqrt[3]{2},\ \sqrt{3}i)$ 是不可约多项式 x^3-2 在 $\mathbb{Q}[x]$ 中的分裂域，因此 $\mathbb{Q}(\sqrt[3]{2},\ \sqrt{3}i)/\mathbb{Q}$ 是伽罗瓦扩张。多项式 x^3-2 有 3 个根：$\omega_1=\sqrt[3]{2}$、$\omega_2=\sqrt[3]{2}(-\frac{1}{2}+\frac{\sqrt{3}}{2}i)$ 和 $\omega_3=\sqrt[3]{2}(-\frac{1}{2}-\frac{\sqrt{3}}{2}i)$。

$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\ \sqrt{3}i)/\mathbb{Q})$ 中的每个元素都是这 3 个根的一个置换，因此 $G=\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\ \sqrt{3}i)/\mathbb{Q})$ 是 S_3 的一个子群。由于 $|\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\ \sqrt{3}i)/\mathbb{Q})|=[\mathbb{Q}(\sqrt[3]{2}:\ \sqrt{3}i)/\mathbb{Q}]=6$，我们有 $G=S_3$。

令 $\mathbb{K}=\mathbb{Q}(\sqrt[3]{2},\ \sqrt{3}i)$。

G 的子群与$\mathbb{Q}$ 和 $\mathbb{K}$ 之间的中间域之间的对应关系如下所列：

H	$\mathbb{K}^H$
$\{e\}$	$\mathbb{Q}(\sqrt[3]{2},\ \sqrt{3}i)$
$\{e,(1\ 2)\}$	$\mathbb{Q}(\omega_3)$
$\{e,(1\ 3)\}$	$\mathbb{Q}(\omega_2)$
$\{e,(2\ 3)\}$	$\mathbb{Q}(\omega_1)$
$\{e,(1\ 2\ 3),\ (1\ 3\ 2)\}$	$\mathbb{Q}(\sqrt{3}i)$
G	$\mathbb{Q}$

(3) x^n-a 的伽罗瓦群，定义在 $\mathbb{F}[x]$中：

THEOREM 4.3.1. 假设 $\mathbb{F}$ 是一个特征为 $\mathrm{Ch}\mathbb{F}\nmid n$ 的域，且 $\mathbb{K}$ 是x^n-1 分裂的一个扩域。那么 $X_n=\{a\in\mathbb{K}\,|\,a^n-1=0\}$ 是一个阶为 n的循环群。

PROOF. 首先，由于 $\mathrm{Ch}\mathbb{F}\nmid n$，$D(x^n-1)=nx^{n-1}\neq 0$。因此，$\gcd(x^n-1,nx^{n-1})=1$。所以 $x^n-1=0$ 是可分的。

因此，X_n是一个阶为 n的阿贝尔群。设 $n=p_1^{n_1}\cdots p_k^{n_k}$，其中 $p_1,\cdots,p_k$是互不相同的素数，$n_1,\cdots,n_k$是正整数。根据 Sylow定理，存在 X_n的子群 $G_1,G_2,\cdots,G_k$，其阶分别为 $p_1^{n_1},\cdots,p_k^{n_k}$。由于$X_n$ 是阿贝尔群，每个 G_i 都是 x_n的正规子群。根据群的第二同构定理，我们有 $X_n=G_1G_2\cdots G_k$。

要证明 X_n 是循环的，只需证明每个 G_i 都是循环的。

设 $m = \text{为 } \alpha\}$的最大 $\underset{\alpha\in G_i}{\{}$阶。如果 $m = p_i^d$对某个 $d < n_i$成立，那么对于 G_i中的每个 α，都有 $\alpha^m = 1$；也就是说，G_i 中的每个元素都是 $x^m - 1 = 0$的根。注意，$x^m - 1 = 0$在 $\mathbb{K}$中至多有 m 个不同的根，但 G_i 有 $p_i^{n_i} > m$ 个不同的元素。这就产生了矛盾。因此，G_i 中存在一个阶为 $p_i^{n_i} = |G_i|$的元素，也就是说，G_i 是循环的。□

PROPOSITION 4.3.1. 设 $\mathbb{F}$ 是一个具有 $\mathrm{Ch}\mathbb{F} \nmid n$ 的域。那么，$x^n - 1$ 在 $\mathbb{F}[x]$ 中的伽罗瓦群与 $\mathbb{Z}_n^\times$同构。

PROOF. 设 $\mathbb{K}$ 是 $x^n - 1$的一个分裂域。将 $x^n - 1 = 0$的根所组成的集合记为 X_n。

根据定理 4.3.1，$\mathbb{K} = \mathbb{F}(\zeta)$，其中 ζ 是循环群 X_n的一个生成元。

那么，Gal($\mathbb{K}/\mathbb{F}$)中的每个 σ 都由 $\sigma(\zeta)$ 完全确定。容易看出，$\sigma(\zeta)$也是 X_n 的一个生成元，因此我们可以定义映射 $\Phi : \mathrm{Gal}(\mathbb{K}/\mathbb{F}) \to \mathbb{Z}_n^\times$，使得 $\sigma(\zeta) = \zeta^{\Phi(\sigma)}$。

可以验证以下结论。

(1) 对所有 σ，τ属于 Gal($\mathbb{K}/\mathbb{F}$)，$\zeta^{\Phi(\tau\sigma)} = \tau\sigma(\zeta) = \tau(\zeta^{\Phi(\sigma)}) = \tau(\zeta)$ $^{\Phi(\sigma)} = \zeta^{\Phi(\tau)\Phi(\sigma)}$，这意味着 Φ 是群同态。(2) 若 $\Phi(\sigma) = \Phi(\tau)$ 属于 $\mathbb{Z}_n^\times$，则 $\sigma(\zeta)$ $= \tau(\zeta)$。因此，Φ 是单射。(3) 对每个属于 $\mathbb{Z}_n^\times$的 m，我们都可以在 $\mathbb{K}$ 上定义一个自同构，将每个属于 $\mathbb{F}[x]$ [2] 的 p 下的$p(\zeta)$映射为 $p(\zeta^m)$。因此，Φ 是满射。

因此，Gal($\mathbb{K}/\mathbb{F}$) 同构于 $\mathbb{Z}_n^\times$。 □

我们将证明以下结论。

THEOREM 4.3.2。设 $\mathbb{F}$ 是一个特征为 $\mathrm{Ch}\mathbb{F} \nmid n$ 的域，且 $x^n - 1$ 的所有根都在 $\mathbb{F}$ 中。那么，$x^n - a$ 在 $\mathbb{F}[x]$ 中的伽罗瓦群是一个阶整除 n 的循环群。反过来，若 $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ 是一个阶为 k 的循环群，且 k 整除 n，则对于某个 $a \in \mathbb{F}$，有 $\mathbb{K} = \mathbb{F}(\sqrt[k]{a})$。

PROOF. 设 $\mathbb{K}$ 是多项式 $x^n - a$ 的分裂域。我们将定义一个从 Gal($\mathbb{K}/\mathbb{F}$) 到 $\mathbb{Z}_n$ 的单射同态。

设 $\sqrt[n]{a} \in \mathbb{K}$ 是 $x^n - a = 0$ 的一个根，ζ 是 $x^n - 1 = 0$ 的一个本原根。那么 $\{\sqrt[n]{a}\zeta^j\}_{j=0}^{n-1}$ 包含 $x^n - a = 0$ 的所有根。每个 $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ 都将 $\sqrt[n]{a}$ 映射为某个 $0 \le j \le n-1$ 的 $\sqrt[n]{a}\zeta^j$，并将 j 记为 m_σ。定义映射 $\Phi : \mathrm{Gal}(\mathbb{K}/\mathbb{F}) \to \mathbb{Z}_n$，使得 $\Phi(\sigma) = m_\sigma$。

我们验证 Φ 是一个单射同态 sm.

首先，对所有 σ，$\tau \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$，$\sigma\tau(\sqrt[n]{a}) = \sqrt[n]{a}\zeta^{m_{\sigma\tau}}$。另一方面

$$\sigma\tau(\sqrt[n]{a}) = \sigma(\tau(\sqrt[n]{a})) = \sigma(\sqrt[n]{a}\zeta^{m_\tau}) = \zeta^{m_\tau}\sigma(\sqrt[n]{a}) = \sqrt[n]{a}\zeta^{m_\tau}\zeta^{m_\sigma} = \sqrt[n]{a}\zeta^{m_\tau + m_\sigma}.$$

因此 Φ 是一个群同态。

其次，若 $m_\sigma = m_\tau$，则 $\sigma = \tau$，因为 $\mathbb{K} = \mathbb{F}(\sqrt[n]{a})$。所以 Φ 是单射。因此 Gal($\mathbb{K}/\mathbb{F}$) 同构于 $\mathbb{Z}_n$ 的一个子群，而 $\mathbb{Z}_n$ 是一个阶整除n的循环群。

现在设 $\mathbb{K}$ 是 $\mathbb{F}$ 的伽罗瓦扩张，且 Gal($\mathbb{K}/\mathbb{F}$) $= \{1, \sigma, \sigma^2, \cdots, \sigma^{n-1}\}$ 为循环群。令 $\zeta \in \mathbb{F}$ 为 $x^n - 1 = 0$ 的本原根。

[2]注意，$\mathbb{F}(\zeta) = \mathbb{F}[\zeta]$。

由于 $\{1, \sigma, \sigma^2, \cdots, \sigma^{k-1}\}$ 在 $\mathbb{F}$ 上线性无关，存在 α 属于 $\mathbb{K}$，使得 [3]

$$(\alpha, \zeta) := \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{k-1}\sigma^{k-1}(\alpha) \neq 0.$$

$\sigma(\alpha, \zeta) = \sigma(\alpha) + \zeta\sigma^2(\alpha) + \zeta^2\sigma^3(\alpha) + \cdots + \zeta^{k-1}\sigma^k(\alpha) = \zeta^{-1}(\alpha, \zeta)$。

对于每个 $0 < j < k$，都有 $\sigma^j(\alpha, \zeta) = \zeta^{-j}(\alpha, \zeta)$。因此，$(\alpha, \zeta)$ 不能被 $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ 中除单位元以外的任何元素固定。因此，$\mathrm{Gal}(\mathbb{K}/\mathbb{F}((\alpha, \zeta))) = \{1\}$，这意味着 $\mathbb{K} = \mathbb{F}((\alpha, \zeta))$。由 $\sigma(\alpha, \zeta) = \zeta^{-1}(\alpha, \zeta)$，我们知道$\sigma((\alpha, \zeta)^k) = \zeta^{-k}(\alpha, \zeta)^k = (\alpha, \zeta)^k$。也就是说，$(\alpha, \zeta)^k$ 属于 $\mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{F})} = \mathbb{F}$。

□

Definition 4.3.1. 若扩张 $\mathbb{K}/\mathbb{F}$ 是伽罗瓦扩张，且其伽罗瓦群为循环群，则称其为**循环**扩张。

(4) $\mathbb{F}_{p^n}/\mathbb{F}_p$的伽罗瓦群:

我们知道，$\mathbb{F}_{p^n}$ 是$\mathbb{F}_p$上可分多项式 $x^{p^n} - x$ 的分裂域，因此是 $\mathbb{F}_p$的伽罗瓦扩张。此外，$[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$。

Theorem 4.3.3. $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}_n$。

Proof. 我们将证明，弗罗贝尼乌斯同构 $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$由 $\sigma(a) = a^p$ 定义，对 $\mathbb{F}_{p^n}$ 中的每个 a 都成立，其阶为 n。因此，$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle\sigma\rangle \cong \mathbb{Z}_n$。

首先，σ 是 $\mathbb{F}_{p^n}$ 上的一个自同构，并固定 $\mathbb{F}_p$，因为对 $\mathbb{F}_p$中的每个 a，都有 $a^p = a$。其次，对于所有 $0 \leq j < n$，$\sigma^j \neq 1$；否则，$\mathbb{F}_{p^n}$ 的所有元素都是$x^{p^j} - x = 0$的根。这会导致矛盾，因为 $x^{p^j} - x = 0$ 至多有 p^j 个根，而$\mathbb{F}_{p^n}$ 有 p^n 个元素。

□

根据伽罗瓦理论基本定理，我们可以通过分类 $\mathbb{Z}_n$的子群来分类 $\mathbb{F}_{p^n}$的子域。

Corollary 4.3.1. $\mathbb{F}_{p^n}$ 的一个子域是某个 $d|n$的 $\mathbb{F}_{p^d}$。

Proof. 根据伽罗瓦理论基本定理，$\mathbb{F}_{p^n}$的每个子域 $\mathbb{E}$都具有如下形式：某个 $\mathbb{Z}_n$ 的子群 H 对应的 $\mathbb{F}_{p^n}^H$，其中 $m = |H|$ 整除 n。因此

$$[\mathbb{E} : \mathbb{F}_p] = [\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) : \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{E})] = d = \frac{n}{m}.$$

也就是说，$\mathbb{E} \cong \mathbb{F}_{p^d}$。 □

4.4. 伽罗瓦大定理与根式可解多项式

我们通过具体例子说明，如何用域扩张来描述多项式的根式可解性。

考虑有理数域中的二次多项式 $f(x) = x^2 + bx + c$。令 $\mathbb{F} = \mathbb{Q}(b, c)$。那么，$f(x)$ 的分裂域是 $\mathbb{F}(\sqrt{b^2 - 4c})$，并且 $\sqrt{b^2 - 4c}$ 是 $\mathbb{F}[x]$中 $x^2 - (b^2 - 4c)$的一个根。换句话说，$f(x)$ 的分裂域嵌入到域塔$\mathbb{F} \subseteq \mathbb{F}(\sqrt{b^2 - 4c})$ 中，其中 $\sqrt{b^2 - 4c}$ 是 $\mathbb{F}[x]$中 $x^2 - (b^2 - 4c)$ 的一个根。

[3]元素（α，ζ）称为拉格朗日预解式。

令 $f(x) = x^3 + qx + r$ 为有理数域中的一个三次多项式。[4]定义 $\mathbb{F} = \mathbb{Q}(q,\ r)$。$f(x)$ 的根的形式为 $y + z$、$\omega y + \omega^2 z$ 和 $\omega^2 y + \omega z$，其中 $y^3 = \frac{1}{2}(-r + \sqrt{r^2 + \frac{4q^3}{27}})$、$z = \frac{-q}{3y}$ 和 $\omega = e^{\frac{2\pi i}{3}}$。因此，$f(x)$ 的分裂域嵌入到域塔中的 $\mathbb{B}_3$

$$\mathbb{F} = \mathbb{B}_0 \subseteq \mathbb{B}_1 = \mathbb{B}_0(\omega) \subseteq \mathbb{B}_2 = \mathbb{B}_1(\sqrt{r^2 + \frac{4q^3}{27}}) \subseteq \mathbb{B}_3 = \mathbb{B}_2(\sqrt[3]{\frac{1}{2}(-r + \sqrt{r^2 + \frac{4q^3}{27}})}).$$

以上内容引出了以下定义。

Definition 4.4.1. 若存在一个域塔（称为**根式塔**）$\mathbb{F} = \mathbb{B}_0 \subseteq \mathbb{B}_1 \subseteq \cdots \subseteq \mathbb{B}_s = \mathbb{E}$，使得对某个正整数 m_i，其中每个 $\mathbb{B}_{i+1} = \mathbb{B}_i(\sqrt[m_i]{a_i})$ 都满足 a_i 在 $\mathbb{B}_i$ 中，则称扩张 $\mathbb{E}$ of $\mathbb{F}$ 为**根式扩张**。若多项式 $f(x)$ 在 $\mathbb{F}[x]$ 中满足 $f(x)$ 在 $\mathbb{F}$ 的某个根式扩张上分裂，则称其**根式可解**。

Proposition 4.4.1.
设 $\mathbb{F}$ 是一个特征为零的域。
如果 $f(x)$ 在 $\mathbb{F}[x]$ 中根式可解，那么它的分裂域包含于一个根式扩张 $\mathbb{F} = \mathbb{B}_0 \subseteq \mathbb{B}_1 \subseteq \cdots \subseteq \mathbb{B}_s = \mathbb{E}$ 中，使得 $\mathbb{E}/\mathbb{F}$ 是伽罗瓦扩张，并且对每个 i，$\mathbb{B}_{i+1}$ 都是 $\mathbb{B}_i$ 的循环扩张。[5]

Proof. 假设 $f(x)$ 在 $\mathbb{F}[x]$ 中根式可解，那么 $f(x)$ 的分裂域 $\mathbb{K}$嵌入到一个根式塔 $\mathbb{F} = \mathbb{B}_0 \subseteq \mathbb{B}_1 \subseteq \cdots \subseteq \mathbb{B}_s$ 中，其中 $\mathbb{B}_{i+1} = \mathbb{B}_i(\sqrt[m_i]{a_i})$，且对所有 $1 \leq i \leq s-1$，a_i 属于 $\mathbb{B}_i$。设 $x^n - 1$的分裂域为 $\mathbb{F}'$，其中 n 是 $m_i's$的最小公倍数。

可以假设上述所有域都包含在一个更大的域中，这样这些域的合成才有意义。

于是我们得到一个根式塔:

$$\mathbb{F} \subseteq \mathbb{F}\mathbb{F}' \subseteq \mathbb{B}_1\mathbb{F}' \subseteq \mathbb{B}_2\mathbb{F}' \subseteq \cdots \subseteq \mathbb{B}_s\mathbb{F}' = \mathbb{E}.$$

s首先可以验证，$\mathbb{E}$是 $\prod_i$的分裂域 $(x^{m_i} - a_i)$。[1]

其次，根据定理 4.3.2，域塔 $\mathbb{F}\mathbb{F}' \subseteq \mathbb{B}_1\mathbb{F}' \subseteq \mathbb{B}_2\mathbb{F}' \subseteq \cdots \subseteq \mathbb{B}_s\mathbb{F}'$ 已经是我们所需要的。

最后，根据伽罗瓦理论基本定理，可以在 $\mathbb{F}$ 和 $\mathbb{F}\mathbb{F}'$ 之间插入中间域，从而得到一个循环塔。□

现在我们要讲伽罗瓦理论中的一个核心定理。

Theorem 4.4.1. （伽罗瓦大定理）
设 $\mathbb{F}$ 是一个特征为零的域。
那么，$f(x)$ 是 $\mathbb{F}[x]$ 上的根式可解多项式，当且仅当其分裂域 $\mathbb{K}$的伽罗瓦群$\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ 是可解群。

Proof. 假设 $f(x)$是根式可解的。
根据命题 4.4.1，存在一个根式塔 $\mathbb{F} = \mathbb{B}_0 \subseteq \mathbb{B}_1 \subseteq \cdots \subseteq \mathbb{B}_s = \mathbb{E}$，使得 $\mathbb{E}$ 是 $\mathbb{F}$ 的伽罗瓦扩张，并且每个 $\mathbb{B}_{i+1}$ 都是 $\mathbb{B}_i$ 的伽罗瓦扩张，且 $\mathrm{Gal}(\mathbb{B}_{i+1}/\mathbb{B}_i)$ 是循环群。

[4]解三次方程 $y^3 + ay^2 + by + c = 0$ 相当于令 $y = x - \frac{a}{3}$ 来解三次方程$x^3 + qx + r = 0$。[5]我们称这样的域塔为**循环的**。

根据伽罗瓦理论基本定理，有 Gal($\mathbb{E}/\mathbb{B}_0$) $\geq$ Gal($\mathbb{E}/\mathbb{B}_1$) $\geq \cdots \geq$ Gal($\mathbb{E}/\mathbb{E}$) $= \{1\}$。此外，每个 $\mathbb{B}_{i+1}$ 都是 $\mathbb{B}_i$的伽罗瓦扩张，因此 Gal($\mathbb{E}/\mathbb{B}_{i+1}$) 是 Gal($\mathbb{E}/\mathbb{B}_i$) 的正规子群，并且 Gal($\mathbb{E}/\mathbb{B}_i$)/Gal($\mathbb{E}/\mathbb{B}_{i+1}$) $\cong$Gal($\mathbb{B}_{i+1}/\mathbb{B}_i$) 是循环群。所以 Gal($\mathbb{E}/\mathbb{F}$) 是一个可解群。 $f(x)$ 的伽罗瓦群 Gal($\mathbb{K}/\mathbb{F}$) $\cong$Gal($\mathbb{E}/\mathbb{F}$)/Gal($\mathbb{E}/\mathbb{K}$) 也是可解的。

现在假设 $G =$Gal($\mathbb{K}/\mathbb{F}$) 是可解的。根据练习 1.32，存在 $G_0 = G \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_s = \{1\}$，使得 G_i/G_{i+1}是循环群。根据伽罗瓦理论基本定理，我们有 $\mathbb{F} = \mathbb{K}^{G_0} \subseteq \mathbb{K}^{G_1} \subseteq \mathbb{K}^{G_2} \subseteq \cdots \subseteq \mathbb{K}^{G_s} = \mathbb{K}$。令 $\mathbb{B}_i = \mathbb{K}^{G_i}$，并注意到 Gal($\mathbb{B}_s/\mathbb{B}_i$) =Gal($\mathbb{K}/\mathbb{K}^{G_i}$) $= G_i$。对于每个 i，由于 Gal($\mathbb{K}/\mathbb{B}_{i+1}$) $= G_{i+1}$ 是 Gal($\mathbb{K}/\mathbb{B}_i$) $= G_i$的正规子群，因此 $\mathbb{B}_{i+1}$是 $\mathbb{B}_i$ 的伽罗瓦扩张，且 Gal($\mathbb{B}_{i+1}/\mathbb{B}_i$) 是循环群。根据定理 4.3.2，$\mathbb{F} = \mathbb{B}_0 \subseteq \mathbb{B}_1 \subseteq \cdots \subseteq \mathbb{B}_s = \mathbb{K}$ 是一个根式塔。因此， $f(x)$ 根式可解。□

Remark 4.4.1. 在定理 4.4.1 中，我们假设 $\mathbb{F}$ 的特征为零，以保证对每个 i，$\mathbb{F}$ 的特征都不整除 m_i。因此，在证明中可以应用定理 4.3.2。

Corollary 4.4.1. 在特征零的域上，所有次数小于 5 的多项式都是根式可解的。

Proof. 设 f 属于 $\mathbb{F}[x]$，且 deg$f \leq 4$。 f 的伽罗瓦群是 S_4的一个子群，因此是可解群。□

Theorem 4.4.2（阿贝尔–鲁菲尼）。

存在一个 $\mathbb{Q}[x]$ 上的五次多项式，它不是根式可解的。

Proof. 考虑 $\mathbb{Q}[x]$中的 $f(x) = x^5 - 80x + 5$。令 $\mathbb{K}$ 为f 的分裂域，并且 $G =$ Gal($\mathbb{K}/\mathbb{Q}$)。

根据艾森斯坦判别法， $f(x)$不可约。设 α是 $f(x) = 0$的一个根。那么[$\mathbb{Q}(\alpha)$: $\mathbb{Q}$] $= 5$。因此，5整除 $|G| = [\mathbb{K}:\ \mathbb{Q}]$。

由于 $f'(x) = 5x^4 - 80$， $f(x)$在 $[-2, 2]$上递减，在（$-\infty$， -2]和 $[2, \infty)$上递增。注意， $f(-2) > 0$且 $f(2) < 0$，所以 $f(x)$恰有3个实根。因此，复数的复共轭是 G中的一个元素。这个元素是一个对换，因为它交换了两个复根，并固定其余的根。

因此， G 在 S_5中包含一个5-循环和一个对换。由练习 1.18， $G = S_5$。由于 G 不可解，根据伽罗瓦大定理， $f(x)$不能根式可解。□

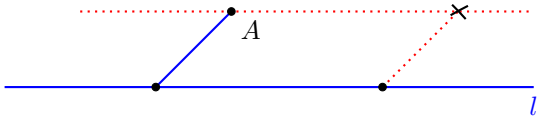
4.5. 尺规作图问题

Definition 4.5.1. 如果复数 $z = x + iy$ 或平面中的点（x， y）可以通过以下尺规作图操作得到，则称其为**可用尺规作图**的：

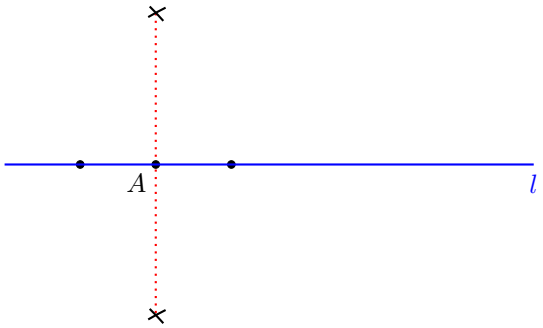
- 用直线连接两个给定点；
- 求两条直线的交点；
- 以给定的圆心和半径作圆；
- 求一条直线与一个圆的交点，或求两个圆的交点。

通过尺规作图操作，可以实现以下作图：

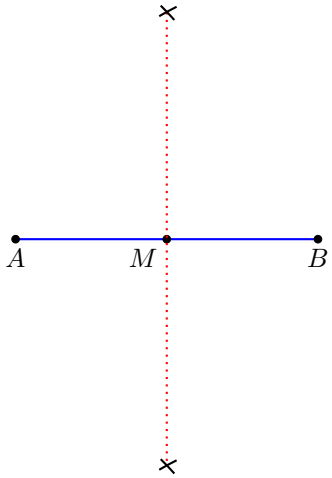
- 作一条经过给定点 A 且平行于给定直线 l的直线;



- 作一条经过给定点 A、位于直线 l 上且垂直于 l 的直线;



- 求线段 AB 的中点。

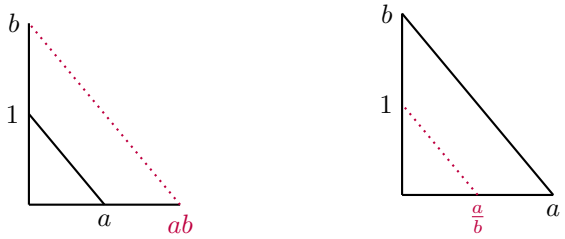


将半径设为固定值 1。
由上文可得以下结论。

Remarks 4.5.1. (1) 用尺规可以作出一个具有有理坐标的直角坐标系。(2) 点 $(x,\ y)$ 可作图，当且仅当 $(x,\ 0)$ 和 $(0,\ y)$ 可作图。

Definition 4.5.2. 若实数 x 满足点 $(x,\ 0)$ 可作图，则称 x 为**可作图的**；等价地，用尺规可以作出点 $(0,\ x)$。

若 $a,\ b$ 属于 $\mathbb{R}$ 且可作图，则 $a \pm b$ 也可作图。
如果正数 a, b 是可作图的，那么如以下图形所示，ab 和 $\frac{a}{b}$ 也是可作图的:



因此，所有可作实数构成一个包含 $\mathbb{Q}$ 的域 $\mathbb{E}$ 。

假设在 $\mathbb{F}^2$ 中有两个可作点，它们属于由可作数构成的域 $\mathbb{F}$ 。连接这两个点，便得到 $\mathbb{R}^2$ 中的一条直线 $ax+by+c=0$，其满足 $a,b,c\in\mathbb{F}$。我们称它为 $\mathbb{F}$上的可作直线。

THEOREM 4.5.1.

设 $\mathbb{F}$ 是实数域的一个子域，且 $[\mathbb{F}:\ \mathbb{Q}]<\infty$。那么 $\mathbb{F}$ 是 $\mathbb{E}$ 的子域，当且仅当 $[\mathbb{F}:\ \mathbb{Q}]=2^m$ 对某个非负整数 m 成立。

PROOF. 设有限扩张 $\mathbb{F}$ 是 $\mathbb{Q}$ 的子域，且它是 $\mathbb{E}$ 的子域。

要证明 $[\mathbb{F}:\mathbb{Q}]=2^m$，只需证明对于 $\mathbb{F}$ 中的每个 α ， $[\mathbb{Q}(\alpha):\ \mathbb{Q}]$ 都是 2 的幂。注意， α 是经过有限次尺规作图操作从 $\mathbb{Q}$ 得到的。因此，只需证明：若实数 α 通过一次尺规作图操作从 $\mathbb{F}$ 的子域 $\mathbb{F}'$ 得到，那么 $[\mathbb{F}'(\alpha):\ \mathbb{F}']=1$ 或 2。

若 $(\alpha,\ \beta)$ 是两条关于 $\mathbb{F}'$ 可作直线的交点，那么 α 是 $\mathbb{F}'[x]$ 中一个次数为 1 的多项式的根，这意味着 $\mathbb{F}'(\alpha)=\mathbb{F}'$。

如果 (α,β) 是圆 $(x-x_0)^2+(y-y_0)^2=r^2$ 与直线 $ax+by+c=0$ 的交点，且 $x_0,y_0,r,a,b,c\in\mathbb{F}'$，那么 α 和 β 是 $\mathbb{F}'[x]$ 中一个次数至多为 2 的方程的根。因此 $[\mathbb{F}'(\alpha):\ \mathbb{F}']=1$ 或 2。

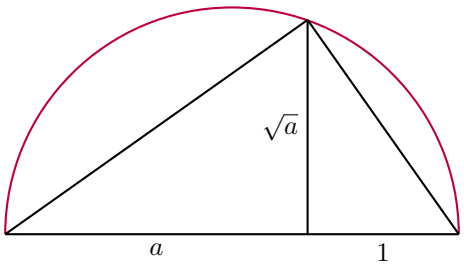
类似地，如果 (α,β) 是两个圆的交点，且它们的圆心坐标和半径都属于 $\mathbb{F}'$。将两个圆的方程结合起来，可知 (α,β) 是圆 $(x-x_0)^2+(y-y_0)^2=r^2$ 与直线 $ax+by+c=0$ 的交点，且 $x_0,y_0,r,a,b,c\in\mathbb{F}'$。再次有 $[\mathbb{F}'(\alpha):\ \mathbb{F}']=1$ 或 2。

反过来，我们证明以下命题：

如果 $\mathbb{F}'$ 是一个由可作数构成的域，且 $\mathbb{F}$是一个实数域，且它是 $\mathbb{Q}$ 的有限扩张，使得 $[\mathbb{F}:\ \mathbb{F}']=2^m$，那么 $\mathbb{F}$ 也由可作数构成。

我们对 m进行归纳法。

下图表明，若正数 a可作图，则$\sqrt{a}$ 可作图。因此，当 $m=1$时，该命题成立。



假设当 $m<n$时，该命题成立。

现在假设 $[\mathbb{F}:\ \mathbb{F}']=2^n$。取 α 于 $\mathbb{F}\setminus\mathbb{F}'$中。若 $[\mathbb{F}'(\alpha):\ \mathbb{F}']=2^n$，则 $\{1,\alpha,\cdots,\alpha^{2^n-1}\}$是 $\mathbb{F}'$上的 $\mathbb{F}$的一组基。由于 $\mathbb{F}'(\alpha):\ \mathbb{F}'(\alpha^2)]=2$，我们有$[\mathbb{F}'(\alpha^2):\ \mathbb{F}']=2^{n-1}$。总之，存在 β 属于 $\mathbb{F}$，使得 $[\mathbb{F}'(\beta):\ \mathbb{F}']=2^k<2^n$。根据假设，$\mathbb{F}'(\beta)$由可作数构成。此外，$[\mathbb{F}:\ \mathbb{F}'(\beta)]=2^{n-k}<2^n$。因此，$\mathbb{F}$ 由可作实数构成。□

Remark 4.5.1. 定理 4.5.1 表明，实数 α 是可作图的，当且仅当 $[\mathbb{Q}(\alpha):\ \mathbb{Q}]=2^m$。

因此，可作数域还包含许多有理数以外的数。不过，它毕竟是一个由代数数组成的域。此外，利用尺规不可能作出以下图形：

(1) 面积为 π 的正方形；(2) 体积为 2 的立方体；(3) 将 $\theta=\frac{\pi}{3}$ 三等分，

因为

(1) 数 π 是**超越数**（不是 $\mathbb{Q}$上的代数数）。[Bak90]。(2) 数$\sqrt[3]{2}$ 不可作图，因为 $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$。(3) 角 θ 可以三等分，当且仅当 $\cos\frac{\theta}{3}$ 可作图。但 $\cos\frac{\pi}{9}$的最小多项式是$8x^3-6x-1$ [6]，这意味着 $[\mathbb{Q}(\cos\frac{\pi}{9}):\ \mathbb{Q}]=3$。

整数 $F_k=2^{2^k}+1$ 称为第 k个**费马素数**。在费马数中，目前只发现了 5 个素数：F_0，$\cdots$，F_4，尽管人们猜测这样的素数有无穷多个。

Theorem 4.5.2. 正 n边形可作图，当且仅当 $n=2^m p_1\cdots p_k$，其中 $p_i's$是费马素数。

Proof. 正 n 边形可作图，当且仅当 x^n-1 的本原根 ζ_n 可作图。根据定理 4.5.1，数 ζ_n 可作图，当且仅当 $\varphi(n)=[\mathbb{Q}(\zeta_n):\mathbb{Q}]=2^l$，其中 l 是某个非负整数。而 $\varphi(n)=2^l$ 当且仅当 $n=2^m p_1\cdots p_k$ 是费马素数。□

习题

Exercise 4.1. 证明，当 $\mathbb{K}/\mathbb{F}$ 是有限域扩张时，$\mathrm{Aut}(\mathbb{K}/\mathbb{F})$ 是有限群。

Exercise 4.2. 设 $\mathbb{K}$ 是 $\mathbb{F}$ 的伽罗瓦扩张。定义

$$\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(\alpha)=\sum_{\sigma\in\mathrm{Gal}(\mathbb{K}/\mathbb{F})}\sigma(\alpha)$$

对每个 α，均有 $\mathbb{K}$。

(1) 证明对于所有 α，$\mathbb{K}/\mathbb{F}(\alpha)$ 属于 $\mathbb{F}$。*(2)* 证明 $\mathbb{K}/\mathbb{F}(\alpha+\beta)=\mathbb{K}/\mathbb{F}(\alpha)+\mathbb{K}/\mathbb{F}(\beta)$。*(3)* 设 $\mathbb{K}=\mathbb{F}(\sqrt{D})$ 是 $\mathbb{F}$ 的二次扩张。证明对于所有 $a,b\in\mathbb{F}$，$\mathbb{K}/\mathbb{F}(a+b\sqrt{D})=2a$。*(4)* 设 $m_{\alpha,\mathbb{F}}(x)=x^d+a_{d-1}x^{d-1}+\cdots+a_1x+a_0$ 是 $\mathbb{F}[x]$ 中 α 的最小多项式。证明 $\mathbb{K}/\mathbb{F}(\alpha)=-\frac{n}{d}a_{d-1}$。

[6]回忆一下，$\cos 3\theta=4\cos^3\theta-3\cos\theta$，并令 $\cos 3\theta=\frac{1}{2}$。

EXERCISE 4.3. 设 $\mathbb{K}$ 是 $\mathbb{F}$ 的伽罗瓦扩张。定义

$$\mathrm{N}_{\mathbb{K}/\mathbb{F}}(\alpha) = \prod_{\sigma\in\mathrm{Gal}(\mathbb{K}/\mathbb{F})} \sigma(\alpha).$$

(1) 证明 $N^{\mathbb{K}/\mathbb{F}}(\alpha)$ 属于 $\mathbb{F}$。*(2)* 证明 $N^{\mathbb{K}/\mathbb{F}}(\alpha\beta) = N^{\mathbb{K}/\mathbb{F}}(\alpha)N^{\mathbb{K}/\mathbb{F}}(\beta)$。*(3)* 设 $\mathbb{K} = \mathbb{F}(\sqrt{D})$ 是 $\mathbb{F}$ 的二次扩张。证明 $N^{\mathbb{K}/\mathbb{F}}(a+b\sqrt{D}) = a^2 - Db^2$。*(4)* 设 $m_{\alpha,\mathbb{F}}(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$ *in* $\mathbb{F}[x]$ 是 α 的最小多项式。证明 $N^{\mathbb{K}/\mathbb{F}}(\alpha) = (-1)^d a_0$。

EXERCISE 4.4. 设 $\mathbb{K}$ 是 $\mathbb{F}$ 的伽罗瓦扩张，且 σ 属于$\mathrm{Gal}(\mathbb{K}/\mathbb{F})$。

(1) 设 $\alpha = \frac{\beta}{\sigma(\beta)}$ 对某个非零的 β *in* $\mathbb{K}$ 成立。证明 $\mathrm{N}^{\mathbb{K}/\mathbb{F}}(\alpha) = 1$.

(2) 设 $\alpha = \beta - \sigma(\beta)$ 对某个 β *in* $\mathbb{K}$ 成立。证明 $\mathrm{Tr}^{\mathbb{K}/\mathbb{F}}(\alpha) = 0$。

EXERCISE 4.5. 设 $\mathbb{K}$ 是 $\mathbb{F}$ 的伽罗瓦扩张，且 $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ 是由 σ 生成的 n 阶循环群。假设 $\alpha \in \mathbb{K}$ 满足 $\mathrm{N}^{\mathbb{K}/\mathbb{F}}(\alpha) = 1$。证明，对于某个非零的 $\beta \in \mathbb{K}$，有 $\alpha = \frac{\beta}{\sigma(\beta)}$ 。

EXERCISE 4.6. 设 $\mathbb{K}$ 是 $\mathbb{E}$ 的伽罗瓦扩张，且 $\mathbb{E}$ 是$\mathbb{F}$的伽罗瓦扩张。 $\mathbb{K}$ 是否为 $\mathbb{F}$ 的伽罗瓦扩张?

EXERCISE 4.7. 设 $\mathbb{K}/\mathbb{F}$ 是伽罗瓦扩张，且 $\mathbb{E}$ 是 $\mathbb{F}$ 与 $\mathbb{K}$ 之间的中间域。证明， $\mathbb{E}/\mathbb{F}$ 是伽罗瓦扩张，当且仅当对所有 $\sigma\in\mathrm{Gal}(\mathbb{K}/\mathbb{F})$，都有 $\sigma(\mathbb{E}) = \mathbb{E}$ 。

EXERCISE 4.8. 设 ζ 是一个 p^{th} 次单位根，其中 p 是素数。证明，$\mathrm{Tr}^{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta)$ 是 -1 或 $p-1$，具体取决于 ζ 是否为本原 p^{th} 次单位根。

EXERCISE 4.9. 设 p、q、r 为素数，且 $q \neq r$。设 ζ为 $x^p - q$ 的任意一个根，η 为 $x^p - r$的任意一个根。证明 $\mathbb{Q}(\zeta) \neq \mathbb{Q}(\eta)$。

EXERCISE 4.10. 求 $\mathrm{Aut}(\mathbb{Q}(\sqrt{3+\sqrt{3}})/\mathbb{Q})$，并判断它是否为伽罗瓦扩张。

EXERCISE 4.11. 求 $x^4 + 2$的伽罗瓦群，并找出所有子群及其对应的不动域。

EXERCISE 4.12. 确定 $x^4 - 14x^2 + 9$的伽罗瓦群，并找出所有子群及其对应的不动域。

EXERCISE 4.13. 描述 $f(x) = x^4 + x + 1$ 在 $\mathbb{F}_2[x]$ 上关于$\mathbb{F}_2$的伽罗瓦群。求 f 在 $\mathbb{F}_2$上的分裂域的所有中间域。

EXERCISE 4.14. 为扩张 $\mathbb{Q}(\sqrt[6]{1+\sqrt[4]{3}}, \sqrt[4]{2})/\mathbb{Q}$求一个根式塔。

EXERCISE 4.15. 证明 $x^5 - 4x + 2$ 不可解。

EXERCISE 4.16. 证明 $\cos\theta$ 可作图，当且仅当 $\sin\theta$ 可作图。

EXERCISE 4.17. 证明正 n 边形可作图，当且仅当 $\cos\frac{2\pi}{n}$ 可作图。

EXERCISE 4.18. 判断下列正 n 边形是否可作图:

(1) $n = 9$。
(2) $n = 5$。
(3) $n = 7$。

参考文献

[Art44] Artin, Emil. *Galois Theory*。Arthur N. Milgram 编，并增补一章。1944 年第二版重印。Dover Publications, Inc., 纽约州米尼奥拉，1998 年。[Bak90] Baker, Alan. *Transcendental Number Theory*。剑桥大学出版社，1990 年。[DF04] Dummit, David S.; Foote, Richard M. *Abstract Algebra*。第三版。John Wiley & Sons, Inc., 新泽西州霍博肯，2004 年。[Edw84] Edwards, Harold M. *Galois Theory*。数学研究生教材第 101 卷。施普林格出版社，纽约，1984 年。[Eis] Eisenstein, Gotthold. ¨关于整条双纽线分割方程的不可约性及其若干其他性质”, 《数学年刊》¨, ¨ *Journal für* （）, –。[Fen98] Fenrick, Maureen H. *die reine und angewandte Mathematik* **39** 1850 160 179 *Introduction to the Galois Correspondence*。第二版。Birkhäuser Boston, Inc.，马萨诸塞州波士顿，1998 年。[Hun80] Hungerford, Thomas W. *Algebra*。1974 年原版重印。数学研究生教材第 73 卷。施普林格出版社，纽约—柏林，1980 年。[IR 90] Ireland, Kenneth; Rosen, Michael. *Theory. 2nd edition. GTM **84**. Springer* , *A Classical Introduction to Modern Number* ,

1990. ,

[Kle86] Kleiner

Israel. The Evolution of Group Theory: A Brief Survey. Mathematics , *Magazine **59** No. 4 (1986)*

195–215. ,

[Kle98] Kleiner

Israel. From Numbers to Rings:The Early History of Ring Theory. Elem. , *Math. **53** (1998) 18–35.*

[Lan02] Lang Serge. Algebra. Revised third edition. Graduate Texts in Mathematics

211. , *2002.* ,

Springer-Verlag New York *[Leo20] Leon*

Steven J. Linear Algebra with Applications. 10th Edition. China Machine , *2020.* ,

Press *[Rot98] Rotman*

Joseph. Galois Theory. Second edition. Universitext. Springer-Verlag,

New York , *1998.* ,

[Syl] Sylow

M. L. Théorèmes sur les groupes de substitutions. (French)《数学年刊》 ***5***

(1872) no. 4 , *584–594.* ,

[Wie59] Wielandt

Helmut. Zum Satz von Sylow. II. (German) ***71*** *(1959) 461–*《数学杂志》,

462.