代数 2 H 课程讲义

Instructor: 余成龙
Notes Taker: 刘博文

Qiuzhen College, Tsinghua University

2023 Spring

课程信息:

- 授课人: 余成龙.
- 办公室: 近春园西楼 260.
- 邮箱: yuchenglong@mail.tsinghua.edu.cn.
- 成绩分布: 作业 (20%) + 期中 (30%) + 期末 (50%).
- 参考书: M.Atiyah *Communicative algebra*, David Eisenbud *Commutative Algebra: with a View Toward Algebraic Geometry*, S.Lang *Algebra*.

内容大纲:

- Galois 理论.
- 同调代数.
- 交换代数.

目录

第一部分

Galois 理论

第一章　域论回顾

1.1　域扩张

在本课程中, 如不加特殊说明, 环 R 总是指含有单位元的交换环, 并且环同态是保持单位元的.

定义 1.1.1. 对于环 R, 总有环同态 $\rho\colon \mathbb{Z} \to R$, 如果记 $\ker\rho = (n)$, 那么 R 的**特征** (characteristic)定义为 n, 记作 $\operatorname{char} R$.

定义 1.1.2. 如果环 R 中任何非零元素都可逆, 那么环 R 被称为一个**域** (field).

命题 1.1.3. *域的特征是素数.*

我们在学习环论时, 环的理想是一个非常重要的概念, 但是对域来说, 其只有平凡理想, 即只有零理想及自身. 这很大程度上限制了域之间的同态. 假设有非平凡的域同态 $\tau\colon E \to F$, 那么 τ 一定是单射, 从而我们可以将 E 视作包含在 F 中, 这引出了下面的概念.

定义 1.1.4. 给定域 E, F, 如果存在 (单) 同态 $\tau\colon F \to E$, 那么称 E 是域 F 的**扩张** (extension), 记作 E/F.

注记. 当我们用 (单) 同态 τ 表示域扩张 E/F 时, 我们不仅强调可以将 F 视作 E 的子域, 也强调映射 τ, 因为可能存在多种方式将 F 视作 E 的子域, 例如:

$$\begin{aligned}\tau\colon \mathbb{R}[x]/(x^2+1) &\to \mathbb{C} \\ x &\mapsto \sqrt{-1}\end{aligned} \qquad\qquad \begin{aligned}\tau'\colon \mathbb{R}[x]/(x^2+1) &\to \mathbb{C} \\ x &\mapsto -\sqrt{-1}\end{aligned}$$

都给出了这样的映射.

定义 1.1.5. 给定域扩张 $\tau\colon F \to E, \tau'\colon F \to E'$, **域扩张之间的态射** (morphism between field extension)是指域之间的同态 $\varphi\colon E \to E'$, 使得如下的图交换

$$\begin{tikzcd} & E \arrow[d, "\varphi"] \\ F \arrow[ur, "\tau"] \arrow[r, "\tau'"'] & E' \end{tikzcd}$$

记号 1.1.6. 给定域扩张 $E/F, E'/F$, 用 $\operatorname{Hom}_F(E, E')$ 记域扩张之间的态射的全体.

定义 1.1.7. 给定域扩张 $E/F, E'/F$, 其被称为**同构的** (isomorphism), 如果两者间存在是同构的域扩张之间的态射.

定义 1.1.8. 给定域扩张 E/F, 扩张的**次数** (degree)定义为 $[E:F]=\dim_F E$.

命题 1.1.9. *对于域扩张 $F\subseteq E\subseteq K$, 则 $[K:F]=[K:E][E:F]$.*

定义 1.1.10. 一个域扩张被称为**有限的** (finite extension), 如果其扩张次数有限, 否则被称为**无限的** (infinite extension).

例子. *$\mathbb{C}/\mathbb{R}$ 是二次扩张, $\mathbb{R}/\mathbb{Q}$ 是无穷扩张.*

例子. *$\mathbb{Q}(i)=\{a+b\sqrt{-1}\mid a,b\in\mathbb{Q}\}/\mathbb{Q}$ 是二次扩张.*

定义 1.1.11. E/F 是域扩张, $S\subseteq K$ 是一个子集, 则 $F(S)$ 是 E 中包含 F,S 最小的子域. 特别地, 如果 $S=\{u\}$, $F(u)$ 叫做域 F 的一个**单扩张** (simple extension).

例子. *给定域 F, $F(u)$ 有如下的具体构造*

$$F(u)=\{\frac{f(u)}{g(u)}\mid f(x),g(x)\in F[x]\}$$

命题 1.1.12. *假设域 $\mathbb{F}$ 的特征不为 2, 如果 E/F 是二次扩张, 那么 $E=F(\alpha)$, 其中 $\alpha^2\in F$.*

证明: 假设 $\{1,\beta\}$ 是 E 的一组 F-基, 那么 $\beta^2=a+b\beta$, 其中 $a,b\in F$, 注意到

$$(\beta-\frac{1}{2}b)^2=a+\frac{1}{4}b^2\in F$$

那么 $\alpha=\beta-\frac{1}{2}$ 即可. □

注记. 域的特征不为 2 用在了配方上, 这是一个不可缺少的条件.

问题 1.1.13. *特征 2 域上的二次扩张是什么样的?*

研究域扩张的一个重要的好处就是可以帮助我们求解方程, 例如 $x^2+1=0$ 在 $\mathbb{R}$ 上没有根, 但是我们可以在 $\mathbb{R}$ 的域扩张 $\mathbb{C}$ 中找到它的一个根, 实际上, 我们总可以通过域扩张的办法去寻找根.

命题 1.1.14. *给定域 F 以及多项式 $f(x)\in F[x]$, 存在域扩张 E/F 使得 $f(x)$ 在 E 中有根.*

证明: 将 $f(x)$ 在 $F[x]$ 中写作不可约因子 $p_1(x)\dots p_k(x)$ 的乘积, 如果有一次因子, 那么 $f(x)$ 在 F 中就有根, 否则取某个不可约多项式 $p_1(x)$, 考虑

$$E=F[x]/(p_1(x))$$

那么 E/F 是一个域扩张, 并且 $f(x)$ 在 E 中有根 $x+(p_1(x))$. □

定义 1.1.15. 给定域扩张 $F\subseteq E\subseteq K$ 以及 $F\subseteq E'\subseteq K$, **域扩张的复合** (composition of field extension)定义为 K 中包含 E,E' 的所有子域的交, 记作 EE'.

1.2 代数扩张

定义 1.2.1. 给定域扩张 E/F, $\alpha \in E$ 称为在 F 上**代数** (algebraic), 如果存在非零多项式 $p(x) \in F[x]$, 使得 $p(\alpha) = 0$, 否则则称 α 在 F 上**超越** (transcendental).

例子. $\sqrt{2}$ 在 $\mathbb{Q}$ 上是代数元, e, π 在 $\mathbb{R}$ 上是超越元.

定义 1.2.2. 给定域扩张 E/F, $\alpha \in E$ 在 F 上代数, $F[x]$ 中零化 α 的最低次数首一多项式被称为 α 的在 F 上的**极小多项式** (minimal polynomial), 记作 $P_{\alpha,F}$.

注记. 我们还可以如下刻画 α 是否在 F 上代数: 考虑赋值映射 $\theta_\alpha \colon F[x] \twoheadrightarrow F[\alpha]$, 则

1. α 在 F 上代数当且仅当 $\ker \theta_\alpha \neq 0$.
2. α 在 F 上超越当且仅当 $\ker \theta_\alpha = 0$, 即 θ_α 是一个同构.

命题 1.2.3. 给定域扩张 E/F, $\alpha \in E$ 在 F 上代数, 那么 $[F(\alpha) : F] = \deg P_{\alpha,F}(x)$.

证明: 注意到 $F(\alpha) \cong F[x]/(P_{\alpha,F}(x))$, 并且 $[F[x]/(P_{\alpha,F}(x)) : F] = \deg P_{\alpha,F}$. □

引理 1.2.4. 给定单扩张 $F(\alpha)/F$, 其中 α 在 F 上代数. 对于域扩张 E/F, 存在 F-嵌入 $\tau \colon F(\alpha) \hookrightarrow E$ 当且仅当 $P_{\alpha,F}$ 在 E 中有根, 并且嵌入的个数与根的个数相同.

证明: 假设 $P_{\alpha,F}(x)$ 在 E 中有根 β, 那么考虑 F-映射

$$\begin{aligned} \varphi \colon F[x] &\to E \\ x &\mapsto \beta \end{aligned}$$

并且由于 $P_{\alpha,F}(\beta) = 0$, 从而 φ 给出了 $F[x]/(P_{\alpha,F}(x)) \cong F(\alpha)$ 到 E 的 $\mathbb{F}$-嵌入, 并且可以看出不同的根给出不同的嵌入. 另一方面, 如果存在 F-嵌入 $\tau \colon F(\alpha) \hookrightarrow E$, 显然 $\tau(\alpha)$ 是 $P_{\alpha,F}$ 在 E 中的根, 并且不同的嵌入给出的根是不同的. □

命题 1.2.5. 给定单扩张 $F(\alpha)/F$, 其中 α 在 F 上代数. 考虑映射 $\varphi \colon F \to F'$ 以及域扩张 E/F', 存在 $\tau \colon F(\alpha) \to E$ 使得如下的交换图当且仅当 $\varphi(P_{\alpha,F}(x))$ 在 E 中有根, 并且 τ 的个数等于 $\varphi(P_{\alpha,F}(x))$ 在 E 中根的个数.

$$\begin{tikzcd} F(\alpha) \arrow[r, "\tau"] & E \\ F \arrow[u] \arrow[r, "\varphi"] & F' \arrow[u] \end{tikzcd}$$

定义 1.2.6. 域扩张 E/F 称为**代数扩张** (algebraic extension), 如果 E 中任何一个元素都在 F 上代数, 否则称为**超越扩张** (transcendental extension).

例子. $\mathbb{C}/\mathbb{R}$ 是代数扩张, $\mathbb{R}/\mathbb{Q}$ 不是代数扩张.

命题 1.2.7. 有限扩张是代数扩张.

证明: 假设 E/F 是有限扩张, 任取 $\alpha \in E$, 考虑 $1, \alpha, \alpha^2, \ldots$, 由于 E/F 是有限扩张, 则存在足够大的 n 使得

$$\alpha^{n+1} = a_n\alpha^n + \cdots + a_1\alpha + a_0$$

从而 $\alpha \in E$ 在 F 上代数, 即 E/F 是代数扩张. □

注记. 反之并不成立, 即代数扩张不一定是有限扩张.

推论 1.2.8. 给定域扩张 E/F, E 中所有在 F 上代数的元素组成了 E 的一个子域.

证明: 即证明, 如果 $\alpha, \beta \in E$ 都在 F 上代数, 则 $\alpha \pm \beta, \alpha\beta, \alpha/\beta(\beta \neq 0)$ 都在 F 上代数. 由于 $\alpha, \beta \in E$ 都是代数的, 那么 $F(\alpha), F(\beta)$ 都是有限扩张, 从而 $F(\alpha, \beta)$ 也是有限扩张, 从而是代数扩张, 即 $\alpha \pm \beta, \alpha\beta, \alpha/\beta(\beta \neq 0)$ 都是代数的. □

命题 1.2.9. 给定代数扩张 $E/F, K/E$, 那么 K/F 也是代数扩张.

命题 1.2.10. 给定代数扩张 E/F, 则 $\mathrm{Hom}_F(E, E) = \mathrm{Aut}_F(E)$.

证明: 任取 $\varphi\colon E \to E$ 是域扩张之间的态射, 我们现在只需要说明其一定是满射即可. 任取 $\alpha \in E$, 我们用 S 记 $P_{\alpha,F}(x)$ 在 E 中的根的全体, 由于 φ 固定 F, 从而 φ 给出了 S 到自身的一个映射, 并且由于 φ 是单的, 以及 S 是有限集, 从而 φ 在 S 上是满射, 从而一定存在 E 中的元素被 φ 映射成 α, 即 φ 是满射. □

第二章 分裂域及其应用

2.1 分裂域

定义 2.1.1. 给定域扩张 E/F, 多项式 $f(x) \in F[x]$ 在 E 中**分裂** (split), 如果 $f(x)$ 在 E 中可以写成

$$f(x) = c\prod_{i=1}^{n}(x-\alpha_i)$$

其中 $\alpha_i \in E$.

定义 2.1.2. 给定域扩张 E/F, E 被称作是 $f(x) \in F[x]$ 的**分裂域** (splitting field), 如果 E 是包含 F 使得 $f(x)$ 分裂的最小的域.

注记. 如果 E 是 $f(x) \in F[x]$ 的分裂域, 那么 E/F 是代数扩张.

定理 2.1.3. *给定域 F, 多项式 $f(x) \in F[x]$ 的分裂域 E 存在且在同构意义下唯一, 并且 $[E:F] \le n!$, 其中 $n = \deg f(x)$.*

证明: 我们通过对 $p(x)$ 次数的归纳来证明存在唯一性, 当 $n=1$ 的时候是显然的.

1. 存在性: 根据命题1.1.14, 总可以找到域扩张 F'/F 使得 $p(x)$ 在 F' 中有根, 因此 $p(x)$ 在 $F'[x]$ 中可以写成:
$$f(x) = (x-u)f_1(x), \quad \deg f_1(x) = n-1$$
因此利用归纳假设, 存在 $f_1(x)$ 在 F' 上的唯一的分裂域 E, 并且 $[E:F'] \le (n-1)!$, 根据分裂域的定义自然有 E 也是 $p(x)$ 在 F 上的分裂域, 并且 $[E:F] = [E:F'][F':F] \le (n-1)! \cdot n = n!$.
2. 唯一性: 如果 E' 是 $f(x)$ 在 F 上的另一个分裂域, 根据引理1.2.4, 存在嵌入 $F' \hookrightarrow E'$, 那么 E' 也应是 $p_1(x)$ 在 F' 上的分裂域, 因此 $E' \cong E$.

□

上述证明分裂域存在的方法虽然简洁, 但是我们实际上可以做的更精细一些, 计算出分裂域之间的同构的个数有多少个, 这主要依赖于命题1.2.5.

定理 2.1.4. *给定域 F, E 是 $f(x) \in F[x]$ 的分裂域. 如果 $f(x)$ 在域扩张 L/F 中分裂, 那么存在 $\varphi \in \mathrm{Hom}_F(E, L)$. 这样 φ 的个数小于等于 $[E:F]$, 并且等号取得当且仅当 $f(x)$ 没有重根.*

证明: 假设 $\{\alpha_1, \ldots, \alpha_n\}$ 是 $f(x)$ 的所有根, 我们归纳地考虑: 由于 $f(x)$ 在 L 中分裂, 那么根据引理1.2.4有如下的延拓:

$$\begin{tikzcd} F(\alpha_1) \arrow[r, dashed, "\varphi_1"] & L \\ F \arrow[u] \arrow[r, "\mathrm{id}"] & F \arrow[u] \end{tikzcd}$$

此时延拓可以选择的个数小于等于 $[F(\alpha_1):F]$. 利用命题1.2.5我们可以做如下的延拓:

$$\begin{tikzcd} F(\alpha_1,\alpha_2) \arrow[r, dashed, "\varphi_2"] & L \\ F(\alpha_1) \arrow[u] \arrow[ur, "\varphi_1"] & \\ F \arrow[u] \arrow[r, "\mathrm{id}"] & F \arrow[uu] \end{tikzcd}$$

这是因为 α_2 在 $F(\alpha_2)$ 上的极小多项式 $P_{\alpha_2,F(\alpha_2)}$ 是 f 的因子, 从而 $\varphi_1(P_{\alpha_2,F(\alpha_2)})$ 依然在 L 中分裂, 此时延拓的可以选择的个数小于等于 $[F(\alpha_1,\alpha_2):F(\alpha_1)]$, 不断归纳即可得到 $\varphi\in\mathrm{Hom}_F(E,L)$, 并且这样的 φ 的个数小于等于

$$[F(\alpha_1):F][F(\alpha_1,\alpha_2):F(\alpha_1)]\ldots[F(\alpha_1,\ldots,\alpha_n):F(\alpha_1,\ldots,\alpha_{n-1})]=[E:F]$$

并且等号取得当且仅当 $f(x)$ 没有重根. □

注记. 特别地, 如果取 L 就是 $f(x)$ 的分裂域 E, 那么 $\varphi\in\mathrm{Hom}_F(E,E)=\mathrm{Aut}_F(E)$ 的个数小于等于 $[E:F]$, 并且等号取得当且仅当 $f(x)$ 没有重根.

2.2 有限域

定义 2.2.1. 域 F 被称为**有限域** (finite field), 如果其元素个数 $|F|<\infty$.

记号 2.2.2. 有 q 个元素的有限域通常记作 $\mathbb{F}_q$.

注记. 根据定义, 显然有限域 $\mathbb{F}_q$ 的特征一定是素数 p, 并且如果 $\mathbb{F}_q$ 是 $\mathbb{F}_p$ 的 n 次扩张, 则 $q=p^n$.

定理 2.2.3. *对任意 $n\in\mathbb{Z}_{\geq 0}$, 元素个数为 $q=p^n$ 的有限域存在且唯一, 其中 p 是素数.*

证明: 存在性: 考虑 $P(x)=x^q-x\in\mathbb{F}_p[x]$, 通过直接验证, 即验证加减乘除的封闭性, 可以发现 $P(x)$ 的所有根恰好组成了一个域 E. 并且根据引理3.2.4计算可知 $P(x)$ 没有重根, 因此 $|E|=q$, 即给出了一个元素个数为 $q=p^n$ 的有限域.

唯一性: 假设 $\mathbb{F}_q$ 是元素个数为 q 的有限域, 那么 $|F^\times|=q-1$, 即任取 $\alpha\in F^\times$, 有 $\alpha^{q-1}=1$, 从而任取 $\alpha\in F$, 其满足

$$\alpha^q-\alpha=0$$

并且由于上述方程至多有 q 个解, 从而 F 是 $x^q-x\in\mathbb{F}_p[x]$ 的分裂域, 因此是唯一的. □

引理 2.2.4. *给定域 F, 以及 $F^\times$ 的有限子群 G, 那么 G 是循环群.*

证明: 由于 G 是有限阿贝尔群, 如果记其最大的不变因子为 d_n, 那么任取 $\alpha\in G$, 有 $\alpha^{d_n}=1$. 考虑 $x^{d_n}-1\in F[x]$, 其最多只有 d_n 个根, 那么 $d_n\geq|G|$. 而另一方面, $|G|\leq d_n$, 从而 $|G|=d_n$, 即 $G\cong\mathbb{Z}/d_n\mathbb{Z}$. □

推论 2.2.5. $\mathbb{F}_q^\times$ 是 $q-1$ 阶循环群.

证明: 当 F 是有限域时, $F^\times$ 自身就是 $F^\times$ 的有限子群, 从而是循环群. □

例子. 考虑 $x^3-x-1\in\mathbb{F}_3[x]$, 其为 $\mathbb{F}_3[x]$ 上的不可约多项式, 那么

$$\mathbb{F}_3[x]/(x^3-x-1)$$

给出了一个 27 元域.

命题 2.2.6. 对任意的 $n\in\mathbb{Z}_{\geq 0}$, 都存在 $\mathbb{F}_q[x]$ 中的 n 次不可约多项式.

证明: 由于 $\mathbb{F}_{q^n}^\times$ 是循环群, 取其生成元为 α, 那么 $\mathbb{F}_q[\alpha]=F_{q^n}$, 从而 α 对应的极小多项式就是 $\mathbb{F}_q[x]$ 中的 n 次不可约多项式. □

问题 2.2.7. 对任意的 $n\in\mathbb{Z}_{\geq 0}$, $\mathbb{F}_q[x]$ 中的首一 n 次不可约多项式有多少个呢?

定义 2.2.8. 给定有限域 $\mathbb{F}_{p^n}$, 如下映射

$$\begin{aligned}\mathrm{Frob}\colon \mathbb{F}_{p^n}&\to\mathbb{F}_{p^n}\\ x&\mapsto x^p\end{aligned}$$

被称作**弗罗贝尼乌斯映射** (Frobenius map).

注记. 根据命题1.2.10, 我们有 $\mathrm{Frob}\in\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q)$, 并且直接计算可知 $\mathrm{Frob}^n=\mathrm{id}$.

命题 2.2.9. 给定有限域 $\mathbb{F}_{p^n}$, $\mathbb{F}_{p^m}$ 是 $\mathbb{F}_{p^n}$ 的子域当且仅当 $m\mid n$.

证明: 如果 $\mathbb{F}_{p^m}$ 是 $\mathbb{F}_{p^n}$ 的子域, 那么 $\mathbb{F}_{p^n}$ 可以视作 $\mathbb{F}_{p^m}$ 上的有限维线性空间, 不妨假设为 k 维, 那么 $p^n=(p^m)^k$, 即 $n=mk$. 另一方面, 如果 $m\mid n$, 那么考虑 $x^{n/m}-x\in\mathbb{F}_{p^m}[x]$, 其分裂域就是 $\mathbb{F}_{p^n}$. □

注记. 由于 $\mathrm{Frob}^n=\mathrm{id}$, 因此 Frob 生成了一个 n 阶循环群 G, 并且注意到 G 的任何一个子群都是由 Frob^m 生成的, 其中 $m\mid n$. 注意到 $\{\alpha\in\mathbb{F}_{p^n}\mid\mathrm{Frob}^m(\alpha)=\alpha\}=\mathbb{F}_{p^{n/m}}$, 这实际上给出了一个 G 的所有子群与 $\mathbb{F}_{p^n}$ 的所有子域之间的一一对应. 上述的结果实际上已经展示了 Galois 理论的雏形.

2.3 代数闭域与代数闭包

定义 2.3.1. 域 F 被称为**代数闭域** (algebraic closed field), 如果其不存在真的代数扩张.

命题 2.3.2. 给定代数扩张 E/F, 如果任取 $f(x)\in F[x]$, 其在 E 上都分裂, 那么 E 是代数闭域.

证明: 任取 $\alpha\in E$, 使得其在 E 上代数, 即存在 $f(x)=a_nx^n+\cdots+a_1x+a_0\in E[x]$, 使得 $f(\alpha)=0$, 特别地, 我们有 α 在 $F(a_n,\dots,a_0)$ 上代数, 并且由于 E/F 上代数, 那么 $F(a_n,\dots,a_0)/F$ 也是代数扩张, 从而根据命题1.2.9可知 $F(\alpha)/F$ 是代数扩张, 因此存在多项式 $g(x)\in F[x]$ 使得 $g(\alpha)=0$, 而由于 $g(x)$ 在 E 中分裂, 从而 $\alpha\in E$, 即证明了 E 是代数闭域. □

定义 2.3.3. 域扩张 E/F 中 E 被称为 F 的**代数闭包** (algebraic closure), 如果 E/F 是代数扩张, E 是代数闭域.

例子 ($\overline{\mathbb{Q}}$ 的构造)**.** 注意到 $\mathbb{Q}[x]$ 是可数的, 不妨排序为 $f_1, f_2, \ldots$, 那么我们令 E_1 是 f_1 在 $\mathbb{Q}$ 上的分裂域, E_2 是 f_2 在 E_1 上的分裂域, 依次不断操作得到

$$\mathbb{Q} \subseteq E_1 \subseteq E_2 \subseteq \ldots$$

考虑 $E = \bigcup_{i=1}^{\infty} E_i$, 则 $E/\mathbb{Q}$ 是一个域扩张, 并且 $\mathbb{Q}$ 上所有的多项式在 E 上都分裂, 并且根据命题*1.2.9*可知 E 是代数扩张, 从而 E 就是 $\overline{\mathbb{Q}}$.

例子 ($\overline{\mathbb{F}_p}$ 的构造)**.** 对于素数 p, 我们有如下的包含关系

$$\begin{tikzcd}
\cdots & & \mathbb{F}_{p^6} & & \cdots \\
\cdots & \mathbb{F}_{p^2} \arrow[ul] \arrow[ur] & & \mathbb{F}_{p^3} \arrow[ul] \arrow[ur] & \cdots \\
& & \mathbb{F}_p \arrow[ull] \arrow[ul] \arrow[ur] \arrow[urr] & &
\end{tikzcd}$$

那么我们有 $\overline{\mathbb{F}_p} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$.

命题 2.3.4 (E. Artin)**.** 任何域 F 都存在一个代数闭域 E 作为其扩张.

证明: 我们首先构造一个 F 的一个域扩张 E_1 使得任意次数大于等于 1 的 $f \in F[x]$ 在 E_1 中都有根: 考虑集合 $\mathfrak{X} = \{x_f \mid f \in F[x], \deg(f) \geq 1\}$, 以及以集合 $\mathfrak{X}$ 为未定元的多项式环 $F[\mathfrak{X}]$. 令 $I = (f(x_f))$, 我们断言 I 是 $F[\mathfrak{X}]$ 的一个真理想. 假设 $I = F[\mathfrak{X}]$, 则有

$$\sum_{i=1}^{n} g_i f_i(x_{f_i}) = 1$$

由于只有有限多个 f_i, 那么根据分裂域存在性的证明过程不难构造 F 的一个域扩张 F' 使得每一个 f_i 在 F' 中都有根 u_i. 考虑 $F[\mathfrak{X}] \to F'$, 定义为 $x_{f_i} \mapsto u_i$, 其余的 x_f 被映成零, 则考虑上述等式在这个映射下的结果, 我们有 $0 = 1$, 矛盾. 因此 I 是真理想, 我们取 $\mathfrak{m}$ 是包含 I 的一个极大理想, 令 $E_1 = F[\mathfrak{X}]/\mathfrak{m}$, 则

$$F \hookrightarrow F[\mathfrak{X}] \to F[\mathfrak{X}]/\mathfrak{m} = E_1$$

我们用 $\overline{x}_f$ 记 x_f 在 E_1 中的像, 可以发现其为 $f(x)$ 的一个根. 不断进行如上操作则有

$$F = E_0 \subseteq E_1 \subseteq E_2 \subseteq \ldots$$

令 $E = \bigcup_{i=0}^{\infty} E_i$, 我们证明 E 是代数闭的. 任取多项式 $f \in E[x]$, 那么其系数总会落在某一个 E_n 中, 则它在 E_{n+1} 中有根, 即在 E_{n+1} 中有分解

$$f = (x - u_1) f_1$$

其中 $f_1 \in E_{n+1}[x]$, 继续对 f_1 使用如上操作即可. $\square$

命题 2.3.5. *F 是域, E 是代数闭域, 并且有嵌入 $\tau\colon F \hookrightarrow E$. 如果 K/F 是代数扩张, 则 τ 可以延拓成 $\tau' : K \to E$. 特别地, 如果 K 是代数闭域, 那么 $\tau' : K \to E$ 是同构.*

证明: 任取 $u \in K$, α 在 F 上的极小多项式记作 $P_{\alpha,F}$, 由于 E 是代数闭域, 那么 $\tau(P_{\alpha,F})$ 在 E 中存在根 β, 那么根据引理1.2.4可知 σ 可以延拓到 $F(\alpha) \to E$. 用 M 记所有的 (K', τ'), 其中 K' 是 K 的包含 F 的子域, τ' 是 τ 的延拓. 并且定义偏序关系 $(K_1', \tau_1') \leq (K_2', \tau_2')$ 为 $K_1' \subseteq K_2'$ 并且 $\tau_2'|_{K_1'} = \tau_1'$. 我们已经知道 M 非空, 从而根据祖恩引理存在极大元 K', 并且再次利用引理1.2.4可知 K' 就是 K. □

定理 2.3.6. *域 F 的代数闭包 $\overline{F}$ 存在且唯一 (在同构意义下).*

证明: 存在性: 根据命题2.3.4, 存在代数闭域 E 使得其是 F 的扩张, 定义

$$\overline{F} := \{\alpha \in E \mid \alpha \text{ 在 } F \text{ 上代数}\}$$

那么有 $\overline{F}$ 是 F 的代数扩张. 并且 $\overline{F}$ 是代数闭域, 因为任取 $f(x) = a_n x^n + \cdots + a_0 \in \overline{F}[x]$, 根据韦达定理可知其根在 $F(a_0, \ldots, a_n)$ 上面代数, 从而在 F 上代数, 进而属于 $\overline{F}$.

唯一性: 根据命题2.3.5即可. □

注记 (Artin-Schreier). 如果 $[\overline{F} : F] < \infty$, 并且大于 1, 则 $[\overline{F} : F] = 2$, 且 -1 不是 F 中的平方根, $\overline{F} = F(\sqrt{-1})$.

第三章　正规扩张与可分扩张

3.1　正规扩张

定义 3.1.1. 代数扩张 E/F 被称为**正规扩张** (normal extension), 如果任取不可约多项式 $P(x) \in F[x]$, 如果其在 E 中有一个根, 则其全部的根都在 E 中.

例子. 二次扩张是正规扩张.

定理 3.1.2. 下列叙述等价:

(1) E/F 是正规扩张.

(2) 任何 F-嵌入 $\tau\colon E \to \overline{F}$ 满足 $\tau(E) \subseteq E$.

(3) $\mathrm{Hom}_F(E, \overline{F}) = \mathrm{Hom}_F(E, E)$.

如果 E/F 是有限扩张, 则上述三条还与下面等价:

(4) E 是某个多项式 $P(x) \in F[x]$ 的分裂域.

证明: 显然 (3) 和 (2) 等价, 下面我们只证明 (1) 和 (2) 的等价性:

(1) 推 (2): 假设 E/F 是正规扩张, 任取 $\alpha \in E$, 考虑 α 在 F 上的极小多项式 $P_{\alpha,F}$, 那么 $P_{\alpha,F}$ 的所有根都落在 E 中. 对于任意的 F-嵌入 $\tau\colon E \to \overline{F}$, $\tau(u)$ 一定是 $P_{\alpha,F}$ 的一个根, 因为 $P_{\alpha,F}(\tau(u)) = \tau(P_{\alpha,F}(u)) = 0$, 因此 $\tau(u) \in E$, 即 $\tau(E) \subseteq E$.

(2) 推 (1): 任取 $\alpha \in E$, 考虑其在 F 上的极小多项式 $P_{\alpha,F}$, 任取其另一个根 $\beta \in \overline{F}$, 则存在态射 $F(\alpha) \to \overline{F}, \alpha \mapsto \beta$, 因此根据引理1.2.4可以延拓成 $\tau\colon K \to \overline{F}$, 因此 $\tau(\alpha) = \beta \in E$, 即 E/F 是正规扩张.

现在假设扩张次数有限, 我们来证明 (4) 与上述命题的等价性:

(1) 推 (4): 假设 E/F 是正规扩张, 任取 $\alpha_1 \in E \setminus F$, 记其在 F 上的极小多项式为 $P_{\alpha_1,F}$, 并且 $[E : F(u_1)] < [E : F]$. 再取 $\alpha_2 \in E \setminus F(\alpha_1)$, 由于扩张次数不断在减小, 因此有限次重复后一定有 $E = F(\alpha_1, \dots, \alpha_n)$, 令 $P = \prod_{i=1}^{n} P_{\alpha_i,F}$, 则 K 是 P 的分裂域.

(4) 推 (2): 如果 E 是 $P(x)$ 的分裂域, 其所有的根为 $\{\alpha_1, \dots, \alpha_n\}$, 则 $E = F(\alpha_1, \dots, \alpha_n)$, 考虑 F-嵌入 $\tau\colon F(\alpha_1, \dots, \alpha_n) \to \overline{F}$, 由于 $\tau(\alpha_i)$ 仍然是 $P(x)$ 的根, 因此 $\tau(\alpha_i) \in E$, 即 $\tau(E) \subseteq E$.

□

推论 3.1.3. 对于域扩张 $F \subseteq E \subseteq K$,

(1) 如果 K/F 是正规扩张, 那么 K/E 也是正规扩张.

(2) 如果 $E/F, E'/F$ 都是正规扩张, 那么 EE'/F 也是正规扩张.

证明: (1). 任取 $\alpha \in K$, 考虑其在 F, E 上的极小多项式, 分别为 $P_{\alpha,F}, P_{\alpha,E}$, 则 $P_{\alpha,E} \mid P_{\alpha,F}$. 由于 K/F 是正规扩张, 因此 $P_{\alpha,F}$ 的所有根都在 K 中, 因此 $P_{\alpha,E}$ 的所有根也在 K 中, 即 K/E 也是正规扩张.

(2). 给定嵌入 $\tau\colon EE' \to \overline{F}$, 由于 $E/F, E'/F$ 都是正规扩张, 因此 $\tau(E) \subseteq E, \tau(E') \subseteq E'$, 因此 $\tau(EE') \subseteq EE'$, 即 EE'/F 是正规扩张. □

注记. 对于域扩张 $F \subseteq E \subseteq K$, K/F 是正规扩张并不意味着 E/F 是正规扩张, 例如考虑下面的例子:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi\sqrt{-1}}{3}})$$

注记. 如果 K/E 是正规扩张, E/F 是正规扩张, 但 K/F 不一定是正规扩张, 考虑下面的例子:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$$

由于二次扩张都是正规扩张, 从而 $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ 以及 $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ 都是正规扩张, 但是 $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ 不是正规扩张: 考虑 $\mathbb{Q}$ 上的不可约多项式 $x^4 - 2$, 其中一个根 $\sqrt[4]{2}$ 在 $\mathbb{Q}(\sqrt[4]{2})$ 中, 但存在一个根 $i\sqrt[4]{2}$ 不在其中.

3.2 可分扩张

引理 3.2.1. *给定代数扩张 $E = F(\alpha_1, \dots, \alpha_n)/F$, 则*

$$|\operatorname{Hom}_F(E, \overline{F})| \leq [E : F]$$

等号取得当且仅当 α_i 在 F 上的极小多项式 $P_{\alpha_i,F}$ 没有重根.

证明: 根据命题1.2.5即得. □

因此我们关心在什么时候极小多项式没有重根, 如下定义的形式导数给出了判别法.

定义 3.2.2. 给定域 F 以及 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$, 其**形式导数** (formal derivative)定义为

$$f'(x) := n a_n x^{n-1} + \cdots + a_1$$

引理 3.2.3. *对于 $f(x), g(x) \in F[x]$, 有*

1. $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.
2. $(f(g(x)))' = f'(g(x))g'(x)$.

引理 3.2.4. *给定 $f(x) \in F[x]$, $f(x)$ 有重根当且仅当 $(f, f') \neq 1$.*

证明: 在 $f(x)$ 的分裂域中将 $f(x)$ 写做 $f(x) = c\prod_{i=1}^n (x - \alpha_i)$, 则

$$f'(x) = c\sum_{i=1}^n (x-\alpha_1)\dots(x-\alpha_{i-1})(x-\alpha_{i+1})\dots(x-\alpha_n)$$

如果 $f(x)$ 有重根, 不妨假设 $\alpha_1 = \alpha_2$, 则 $f'(\alpha_1) = 0$, 即 $(x - \alpha_1) \mid (f, f')$. 另一方面, 如果 $\alpha_i \neq \alpha_j$ 对任意 $i \neq j$ 成立, 则 $f'(\alpha_i) \neq 0$ 对任意 $1 \leq i \leq n$ 成立, 从而 $(f, f') = 1$. □

推论 3.2.5. *如果 f 是不可约多项式, f 有重根等价于 $f'=0$.*

证明: 如果 f 是不可约的, 从而 $(f,f')=1$ 或 $(f,f')=f$. 从而 f 有重根当且仅当 $(f,f')=f$, 但是 $\deg p' \le n-1$, 从而有 $f'=0$. □

定义 3.2.6. 给定域 F, $p(x)\in F[x]$ 被称为**可分多项式** (seperable polynomial), 如果其不存在重根.

定义 3.2.7. 给定域扩张 E/F, $\alpha\in E$ 被称为 F 上的**可分元** (seperable element), 如果其在 F 上的极小多项式 $P_{\alpha,F}$ 是可分多项式.

定义 3.2.8. 代数扩张 E/F 被称为**可分扩张** (seperable extension), 如果 E 中所有元素都在 F 上可分.

定理 3.2.9. *给定代数扩张 E/F, 如下叙述等价:*

(1) *E/F 是可分扩张.*

(2) *$E=F(\{\alpha_i\}_{i\in I})$, 其中 α_i 是 F 上的可分元.*

如果 E/F 是有限扩张, 则上述两条还与下面的等价:

(3) $|\mathrm{Hom}_F(E,\overline{F})|=[E:F]$.

证明: (1) 推 (2) 是显然的, (2) 推 (3) 成立依赖于引理3.2.1. 下面我们假设 E/F 是有限扩张来证明 (3) 推 (1): 由于 E/F 是有限扩张, 因此不妨假设 E 是 F 添加有限多个元素得到的, 即 $E=F(\alpha_1,\dots,\alpha_n)$, 任取 $\alpha\in E$, 我们不妨考虑 $E=F(\alpha,\alpha_1,\dots,\alpha_n)$, 因此根据引理3.2.1的取等条件可知 $\alpha,\alpha_1,\dots,\alpha_n$ 都是 F 上的可分元. 特别地, 有 α 是 F 上的可分元, 即 E/F 可分.

最后我们来证明 (2) 推 (1): 假设 $E=F(\{\alpha_i\}_{i\in I})$, 其中 α_i 是 F 上的可分元. 任取 $\alpha\in E$, 由于 E/F 代数, 从而存在 F 的某个有限扩张 $L=F(\alpha_1,\dots,\alpha_n)$ 使得 $\alpha\in L$, 因此利用有限扩张情形的 (2) 推 (3) 推 (1) 即可知 α 在 F 上可分. □

推论 3.2.10. *可分多项式的分裂域是可分扩张.*

证明: 可分多项式的分裂域可以视作是添加若干可分元得到的扩域. □

推论 3.2.11. *域扩张 $F\subseteq E\subseteq K$, 则 K/F 是可分扩张当且仅当 $K/E, E/F$ 都是可分扩张.*

证明: 假设 K/F 是可分扩张, 那么任取 $u\in K$, 其在 E 上的不可约多项式可以整除其在 F 上的不可约多项式, 即 K/E 是可分扩张; E/F 是可分的更是显然, 因为任取 $u\in E$ 考虑其在 F 上的不可约多项式和将其看成是 K 中的元素考虑其在 F 上的不可约多项式是一样的.

另一方面, 任取 $\alpha\in K$, 其在 E 上的极小多项式记作 $P_{\alpha,E}(x)=a_nx^n+\cdots+a_0$. 考虑 $F\subseteq F(a_0,\dots,a_n)\subseteq E\subseteq E(u)\subseteq K$, 由于 E/F 是可分的, 从而 $F(a_0,\dots,a_n)/F$ 是可分的. 而 α 在 $F(a_0,\dots,a_n)$ 上的极小多项式也是 $P_{\alpha,E}$, 是一个可分多项式, 即 α 在 $F(a_0,\dots,a_n)$ 上可分, 从而根据定理3.2.9有 $F(u,a_0,\dots,a_n)/F$ 是可分的. 特别地, α 在 F 上是可分的. □

推论 3.2.12. *$E/F, E'/F$ 都是可分扩张, 则 EE'/F 也是可分扩张.*

证明: 显然 EE' 中所有的元素都是 F 上的可分元, 从而根据定理3.2.9可知 EE'/F 是可分扩张. □

命题 3.2.13. 如果 $\mathrm{char}\, F = 0$, 则任何不可约多项式都是可分的.

证明: 当 $\mathrm{char}\, F = 0$ 时, 任何非常数的多项式都有非零导数, 从而根据引理3.2.4即可. □

例子. 当 $\mathrm{char}\, F = p$ 时, 并非所有不可约多项式都是可分的: 令 $F = \mathbb{F}_p(t)$, 取 $f(x) = x^p - t \in F[x]$, 则 $p(x)$ 是不可约多项式, 但不是可分的, 因为

$$(f, f') = (x^p - t, px^p) = (x^p - t, 0) = 0 \neq 1$$

这里面关键的原因在于特征不为零时, 一个高次多项式的形式导数可能会为零.

命题 3.2.14. 如果 $\mathrm{char}\, F = p$, 则任何不可约多项式都是可分的当且仅当 $F = F^p$.

证明: 假设不可约 $f(x) \in F[x]$ 不可分当且仅当 $f'(x) = 0$, 这也当且仅当 $f(x)$ 可以写作

$$f(x) = \sum_{k=0}^{n} a_k x^{kp}$$

假设 $F = F^p$, 那么对于任意 a_k, 总存在 b_k 使得 $b_k^p = a_k$, 从而

$$f(x) = \sum_{k=0}^{n} b_k^p x^{kp} = (\sum_{k=0}^{n} b_k x^k)^p$$

与 $f(x)$ 不可约相矛盾. 另一方面, 假设 $F \neq F^p$, 那么存在 $t \in F$ 使得 $\sqrt[p]{t} \notin F$, 考虑 $x^p - t$ 便得到了一个不可约的不可分多项式. □

定义 3.2.15. 域 F 被称为**完美域** (perfect field), 如果任何不可约多项式都是可分的.

命题 3.2.16.

1. 如果 $\mathrm{char}\, F = 0$, 则 F 是完美域.
2. 如果 $\mathrm{char}\, F = p$, 域 F 是完美域当且仅的 $F^p = F$.
3. 任何有限域都是完美域.

证明: (1) 和 (2) 根据命题3.2.13以及命题3.2.14即可. 对于 (3), 弗罗贝尼乌斯映射给出了 $F^p = F$. □

命题 3.2.17. 完美域的代数扩张都是可分扩张.

证明: 假设 F 是完美域, E/F 是代数扩张, 任取 $\alpha \in E$, 则其在 F 上的极小多项式是可分多项式, 从而 α 是 F 上的可分元, 即 E/F 是可分扩张. □

推论 3.2.18. 如果 $\mathrm{char}\, F = 0$, 则任何代数扩张 E/F 是可分扩张.

推论 3.2.19. $\mathbb{F}_{p^n}/\mathbb{F}_p$ 是可分扩张.

3.3 纯不可分扩张

在本节中, F 总是指特征为 p 的域. 给定一个不可约的不可分多项式 $P(x) \in F[x]$, 那么根据 $P'(x) = 0$ 可知存在 $P_1(x)$, 使得 $P(x) = P_1(x^p)$. 下面考虑 $P_1(x)$ 是否不可分, 如果仍不可分, 可以继续做下去, 直到 $P = P_e(x^{p^e})$, 其中 $P_e(x)$ 是可分多项式.

定义 3.3.1. 对于不可约的不可分多项式 $P(x) \in F[x]$, $n_s := \deg P_e$, 则 $n = n_s \cdot p^e$, 其中 n_s 称为 $P(x)$ 的**可分次数** (seperable degree), p^e 称作 $P(x)$ 的**不可分次数** (inseperable degree).

命题 3.3.2. *给定域扩张 E/F, F 上所有可分的元素组成的集合记作 E_s, 那么 E_s 是 E 的一个子域.*

证明: 任取 $\alpha, \beta \in E$ 是可分元, 那么根据定理3.2.9可知 $F(\alpha, \beta)/F$ 是可分扩张, 从而可分元的加减乘除都在其中, 即 E_s 是 E 的一个子域. □

定义 3.3.3. $u \in \overline{F}$ 被称为在 F 上**纯不可分** (purely inseperable), 如果 $u^{p^m} \in F$, 对某个正整数 m 成立.

定义 3.3.4. 代数扩张 E/F 被称为**纯不可分扩张** (purely inseperable extension), 如果 E 中的每个元素在 F 上都是纯不可分的.

命题 3.3.5. *给定域扩张 E/F, 则 E/E_s 是纯不可分扩张.*

证明: 任取 $\alpha \in E \setminus E_s$, 考虑其在 F 上的极小多项式 $P_{\alpha,F}$, 是一个不可分的不可约多项式. 假设其不可分次数为 p^e, 那么 $P_{\alpha,F} = P_e(x^{p^e})$, 其中 P_e 是一个可分多项式, 即 $\alpha^{p^e} \in E_s$, 即 E/E_s 是纯不可分扩张. □

注记. 即给定域扩张 E/F, 其可以分解为可分扩张 E_s/F 和纯不可分扩张 E/E_s.

定义 3.3.6. 给定域扩张 E/F, 其**可分次数** (seperable degree)定义为 $[E:F]_s := [E_s : F]$, 其**不可分次数** (inseperable degree)定义为 $[E:F]_i := [E:E_s]$.

命题 3.3.7.

(1) *如果 E/F 是有限纯不可分扩张, 则 $[E:F]$ 是 p 的幂次.*

(2) *如果 $K/E, E/F$ 都是纯不可分扩张, 则 K/F 也是纯不可分扩张.*

证明: (1). 由于 E/F 是纯不可分扩张, 从而 $\alpha \in E$ 满足某个多项式 $x^{p^m} - c \in F[x]$, 从而其极小多项式整除 $x^{p^m} - c$, 进而极小多项式的次数也是 p 幂次. 对于 E 的任何包含 F 的子域 K, $\alpha \in E$ 在 K 上的极小多项式一定整除其在 F 上的极小多项式, 从而次数也是 p 的幂次, 从而

$$[E:F] = [F(\alpha_1, \ldots, \alpha_n) : F(\alpha_1, \ldots, \alpha_{n-1})] \ldots [F(\alpha_1) : F]$$

是 p 的幂次.

(2). 任取 $\alpha \in K$, 由于 K/E 是纯不可分的, 因此存在正整数 m_1 使得 $\alpha^{p^{m_1}} \in E$, 再利用 E/F 是纯不可分的, 可以找到正整数 m_2 使得 $(\alpha^{p^{m_1}})^{p^{m_2}} \in F$, 从而 K/F 是纯不可分的. □

命题 3.3.8. 给定有限扩张 E/F, 则

$$|\operatorname{Hom}_F(E,\overline{F})| = [E:F]_s \leq [E:F]$$

特别地, 等号取得当且仅当 E/F 是可分扩张.

证明: 如果 E/F 是可分扩张, 则根据定理3.2.9可知

$$|\operatorname{Hom}_F(E,\overline{F})| = [E:F]$$

而当 E/F 不是可分扩张时, 我们断言有如下一一对应:

$$\operatorname{Hom}_F(E,\overline{F}) = \operatorname{Hom}_F(E_s,\overline{F})$$

通过 $\tau \mapsto \tau|_{K_s}$ 给出. 对应是满射可根据命题2.3.5; 为了证明对应是单射, 即证明 τ 被 $\tau|_{E_s}$ 所决定: 任取 $u \in E$, 则存在正整数 m 使得 $u^{p^m} \in E_s$, 则 $\tau(u^{p^m}) = \tau(u)^{p^m} = v \in \overline{F}$, 因此 $\tau(u)$ 满足方程 $x^{p^m} - v = (x-v')^{p^m} = 0$, 可知 $\tau(u)$ 被唯一确定. $\square$

第四章 Galois 理论

4.1 Galois 扩张

记号 4.1.1. 给定域扩张 E/F, 对于 $H < \mathrm{Aut}_F(E)$, 记 $E^H = \{u \in E \mid \tau(u) = u, \forall \tau \in H\}$.

定义 4.1.2. 代数扩张 E/F 被称为 **Galois 扩张** (Galois extension), 如果其是可分正规扩张.

注记. 根据正规性可知 $\mathrm{Hom}_F(E, \overline{F}) = \mathrm{Hom}_F(E, E) = \mathrm{Aut}_F(E)$. 对于 Galois 扩张 E/F, F-自同构全体 $\mathrm{Aut}_F(E)$ 通常也被记作 $\mathrm{Gal}(E/F)$, 并且

$$|\,\mathrm{Gal}(K/F)| = |\,\mathrm{Hom}_F(K, K)| \overset{(1)}{=} |\,\mathrm{Hom}_F(K, \overline{F})| \overset{(2)}{=} [K : F]$$

其中 (1) 成立是根据定理3.1.2, (2) 成立是根据定理3.2.9.

命题 4.1.3. *对于域扩张 $F \subseteq E \subseteq K$, 如果 K/F 是 Galois 扩张, 则 K/E 也是.*

证明: 根据推论3.1.3以及推论3.2.11即可. □

注记. 注意, 对于域扩张 $F \subseteq E \subseteq K$, 如果 K/F 是 Galois 扩张, E/F 不一定是 Galois 扩张, 在下一节 Galois 对应中我们将看到 E/F 是 Galois 扩张当且仅当 $\mathrm{Gal}(K/E)$ 是 $\mathrm{Gal}(K/F)$ 的正规子群.

定义 4.1.4. 给定可分扩张 E/F, 则在 $\overline{F}$ 中包含 E 的最小的 Galois 扩张被称为 E/F 的 **Galois 闭包** (Galois closure).

注记. 对于一个任意的代数扩张 E/F, 我们都可以在 $\overline{F}$ 中寻找 E/F 的正规闭包: 将 E 写成 $F(\{\alpha_i\}_{i\in I})$, 其中 α_i 都是代数元. 对于每一个 α_i, 用 $P_{\alpha_i,F}$ 去记其在 F 上的极小多项式, 那么将这些 $P_{\alpha_i,F}$ 在 $\overline{F}$ 中的所有根都添加到 F 中, 得到的域记作 N, 不难发现 N 就是 K/F 的正规闭包. 特别地, 如果 E/F 是可分扩张, 我们可以选取 α_i 都是可分元, 从而此时的 N/F 也是可分扩张, 从而是 E/F 的 Galois 闭包. 更特别地, 如果 E/F 是有限可分扩张, 那么其 Galois 闭包也是 F 的有限扩张.

命题 4.1.5. *对于有限扩张 E/F, 如下叙述等价:*

(1) *E/F 是 Galois 扩张.*
(2) *E 是可分多项式 $f \in F[x]$ 的分裂域.*
(3) *$F = E^{\mathrm{Gal}(E/F)}$.*
(4) *存在 $\mathrm{Aut}_F(E)$ 的有限子群 H 使得 $F = E^H$.*

证明: (1) 和 (2) 等价是根据定理3.1.2和推论3.2.10即可. (1) 推 (3): 首先显然 $F \subseteq E^{\mathrm{Gal}(E/F)}$; 另一方面, 任取 $\alpha \in E^{\mathrm{Gal}(E/F)}$, 考虑 α 在 F 上的极小多项式 $P_{\alpha,F}$, 任取 $P_{\alpha,F}$ 的一个根 β, 定义嵌入 $F(\alpha) \hookrightarrow \overline{F}$ 为 $\alpha \mapsto \beta$, 根据命题2.3.5可以将其延拓成 $\tau\colon E \to \overline{F}$, 而根据 E 是正规扩张, 可知 $\tau(E) = E$, 即 $\tau \in \mathrm{Gal}(E/F)$. 由于 $\alpha \in E^{\mathrm{Gal}(E/F)}$, 因此 $\beta = \tau(\alpha) = \alpha$, 即 $P_{\alpha,F}(x) = x - \alpha$, 即 $\alpha \in F$. (3) 推 (4) 是显然的, 取 $H = \mathrm{Aut}_F(K)$ 即可. (4) 推 (1) 是下面将要证明的引理4.1.8, 即阿廷引理. □

记号 4.1.6. 如果 Galois 扩张 E/F 是多项式 $f(x) \in F[x]$ 的分裂域, 那么此时记 Galois 群为 G_f.

引理 4.1.7 (Dedekind 无关引理)**.** *K 是域, $H = \{\tau_1, \ldots, \tau_n\}$ 是 $\mathrm{Aut}(K)$ 的有限子集 (不必要是子群). 如果存在 $c_i \in K$ 使得*

$$c_1\tau_1(x) + \cdots + c_n\tau_n(x) = 0$$

对任意的 $x \in K$ 成立, 那么 $c_i = 0, i = 1, \ldots, n$.

证明: 假设存在这样的 c_i, 我们不妨假设

$$c_1\tau_1(x) + \cdots + c_r\tau_r(x) = 0 \tag{4.1.1}$$

对任意的 $x \in K$ 成立, 并且 $c_i \neq 0, 1 \leq i \leq r$, 其中 r 是满足这样条件最小的数. 用 $ax, a \in K^\times$ 替代 x 则有

$$c_1\tau_1(a)\tau_1(x) + \cdots + c_r\tau_r(a)\tau_r(x) = 0 \tag{4.1.2}$$

(4.1.2) 减 (4.1.1) 乘 $\tau_r(a)$ 则有

$$c_1[\tau_1(a) - \tau_r(a)]\tau_1(x) + \cdots + c_{r-1}[\tau_{r-1}(a) - \tau_r(a)]\tau_{r-1}(x) = 0$$

根据我们对 r 的假设则有 $\tau_i(a) = \tau_r(a)$ 对任意的 $1 \leq i \leq r-1$ 以及 $a \in K^\times$ 成立, 从而有 $\tau_1 = \tau_r, r \geq 2$, 相矛盾. □

引理 4.1.8 (阿廷引理)**.** *K 是域, $H = \{\tau_1, \ldots, \tau_n\}, \tau_1 = \mathrm{id}$ 是 $\mathrm{Aut}(K)$ 的有限子群, 记 $E = K^H$, 则 K/E 是 Galois 扩张, 并且扩张次数 $[K:E] = |H|$.*

证明: 我们首先证明 K/E 是 Galois 扩张: 任取 $\alpha \in K$, 记 α 在 E 上的极小多项式为 p, 令 $\mathcal{O}$ 是 α 在 H 作用下的轨道, 考虑:

$$q(x) = \prod_{\alpha \in \mathcal{O}} (x - \alpha)$$

则任取 $\tau \in H$ 有 $\tau(q(x)) = q(x)$, 即 $q(x) \in E[x]$. 并且由于 H 是一个子群, 其中含有单位元, 从而 $\alpha \in \mathcal{O}$, 即 $q(\alpha) = 0$, 因此 $p(x) \mid q(x)$, 但是 q 没有重根, 并且所有的根都在 K 中, 因此 K/E 是 Galois 扩张.

现在来证明 $[K:E] \leq |H|$: 只需要证明任取 $\alpha_1, \ldots, \alpha_{n+1} \in K$, 它们是 E-线性相关即可: 考虑矩阵 $(\tau_i(\alpha_j)) \in M_{n\times(n+1)}(K)$, 则其 $n+1$ 列 K-线性相关, 即存在 $c_1, \ldots, c_{n+1} \in K$, 且不全为零使得:

$$c_1\begin{pmatrix} \tau_1(\alpha_1) \\ \tau_2(\alpha_1) \\ \vdots \\ \tau_n(\alpha_1) \end{pmatrix} + c_2\begin{pmatrix} \tau_1(\alpha_2) \\ \tau_2(\alpha_2) \\ \vdots \\ \tau_n(\alpha_2) \end{pmatrix} + \cdots + c_{n+1}\begin{pmatrix} \tau_1(\alpha_{n+1}) \\ \tau_2(\alpha_{n+1}) \\ \vdots \\ \tau_n(\alpha_{n+1}) \end{pmatrix} = 0 \tag{4.1.3}$$

不妨假设 $c_1, \dots, c_r \neq 0$, $c_{r+1} = \cdots = c_{n+1} = 0$, 且这样的 r 是最小的. 那么 $r \geq 2$, 并且不妨假设 $c_1 = 1$, 考虑第一行:

$$\alpha_1 + c_2\alpha_2 + \cdots + c_r\alpha_r = 0 \tag{4.1.4}$$

我们断言 $c_2, \dots, c_n \in E$, 不然如果存在 $2 \leq i \leq r$, 使得对任意的 $1 \leq j \leq n$ 有 $\tau_j(c_i) \neq c_i$, 用 τ_j 作用 (4.1.4) 可得

$$\tau_j(\alpha_1) + \tau_j(c_2)\tau_j(\alpha_2) + \cdots + \tau_j(c_r)\tau_j(\alpha_r) = 0 \tag{4.1.5}$$

用 (4.1.5) 分别与 (4.1.3) 的每一行相减, 可以得到一个新的更小的 r', 这与 r 的选取相矛盾.

最后来证明 $[K : E] \geq |H|$: 假设 $[K : E] = r < n$, 令 $\{x_1, \dots, x_r\}$ 是 K 在 E 上的一组基, 那么任取 $y \in K$, 将其写成

$$y = c_1x_1 + \cdots + c_rx_r$$

考虑 $r \times n$ 矩阵 $(\tau_j(x_i))$, 其秩一定 $\leq r < n$, 因此存在非平凡的 ξ_i 满足

$$\begin{cases} \xi_1\tau_1(x_1) + \ldots + \xi_n\tau_n(x_1) = 0 \\ \vdots \\ \xi_1\tau_1(x_r) + \ldots + \xi_n\tau_n(x_r) = 0 \end{cases}$$

将上面第 i 个方程乘以 c_i, 由于 $E = K^H$, 因此 $\tau_j(c_i) = c_i$, 从而

$$\begin{cases} \xi_1\tau_1(c_1x_1) + \ldots + \xi_n\tau_n(c_1x_1) = 0 \\ \vdots \\ \xi_1\tau_1(c_rx_r) + \ldots + \xi_n\tau_n(c_rx_r) = 0 \end{cases}$$

因此 $\xi_1\tau_1(y) + \cdots + \xi_n\tau_n(y) = 0$ 对任意的 $y \in K$ 成立, 根据引理4.1.7可知 $\xi_i = 0$, 相矛盾! □

4.2 Galois 对应

定理 4.2.1 (Galois 主定理). *给定有限 Galois 扩张 K/F, 则*

(1) *存在如下的一一对应:*

$$\{\mathrm{Gal}(K/F)\text{的子群}\} \xleftrightarrow{1-1} \{K/F\text{的中间域}\}$$

对应法则为 $H \mapsto K^H$ 与 $E \mapsto \mathrm{Gal}(K/E)$.

(2) *E/F 是 Galois 扩张当且仅当 $\mathrm{Gal}(K/E)$ 是 $\mathrm{Gal}(K/F)$ 的正规子群, 并且:*

$$\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$$

证明: (1). 根据命题4.2.4的 (3) 可知

$$E \to \mathrm{Gal}(K/E) \to K^{\mathrm{Gal}(K/E)} = E$$

现在只需要证明下面的对应成立:

$$H \to K^H \to \mathrm{Gal}(K/K^H) = H$$

一方面 $H \subseteq \mathrm{Gal}(K/K^H)$ 是显然的, 而根据引理4.1.8:

$$|\mathrm{Gal}(K/K^H)| \le |H|$$

即两者相同.

(2). 根据推论3.2.11可知 E/F 是可分扩张, 从而 E/F 是 Galois 扩张当且仅当 E/F 是正规扩张, 即 $\tau(E) = E$. 任取 $\tau \in \mathrm{Gal}(K/F)$, 可以直接验证:

$$\mathrm{Gal}(K/\tau(E)) = \tau^{-1}\mathrm{Gal}(K/E)\tau$$

因此 E/F 是 Galois 扩张当且仅当 $\tau(E) = E$ 当且仅当 $\mathrm{Gal}(K/E)$ 是正规子群. □

推论 4.2.2. *E/F 是有限可分扩张, 则 E/F 中只存在有限多个中间域.*

证明: 考虑其 Galois 闭包 K/F, 由注记4.1可知其 Galois 闭包 K/F 也是有限扩张, 从而根据 Galois 对应 K/F 中只有有限多个中间域, 从而 E/F 中只有有限多个中间域. □

推论 4.2.3 (本原元定理)**.** *如果 E/F 是有限可分扩张, 则 $E = F(\alpha), \alpha \in E$.*

证明: 如果 F 是有限域, 则不妨假设 $F = \mathbb{F}_p, E = \mathbb{F}_q, q = p^m$, 根据推论2.2.5可知 $\mathbb{F}_q^\times$ 是循环群, 不妨记其生成元为 ξ, 则 $\mathbb{F}_q = \mathbb{F}_p(\xi)$; 如果 F 是无限域, 不妨假设 $E = F(\alpha_1, \alpha_2)$, 一般情况归纳即可: 任取 $r \in F$, 考虑 $F \subseteq F(\alpha_1 + r\alpha_2) \subseteq E$, 由于其中只有有限多个中间域, 并且 F 是无限域, 因此存在不同的 $r_1, r_2 \in F$ 使得:

$$F(\alpha_1 + r_1\alpha_2) = F(\alpha_1 + r_2\alpha_2)$$

考虑 $\alpha = \alpha_1 + r_1\alpha_2$, 我们断言 $F(\alpha) = F(\alpha_1, \alpha_2)$: 显然 $F(\alpha) \subseteq F(\alpha_1, \alpha_2)$; 另一方面, 由于 $\alpha = \alpha_1 + r_1\alpha_2 = \alpha_1 + r_2\alpha_2$, 并且 $r_1 \ne r_2$, 从而 $(r_1 - r_2)\alpha_2 \in F(\alpha)$, 即 $\alpha_2 \in F(\alpha)$, 从而 $\alpha_1 \in F(\alpha)$, 即 $F(\alpha) = F(\alpha_1, \alpha_2)$. □

命题 4.2.4. *如果 $E/F, K/F$ 都是有限 Galois 扩张, 则 EK/F 也是 Galois 扩张, 并且*

(1)

$$\varphi\colon \mathrm{Gal}(EK/K) \to \mathrm{Gal}(E/E \cap K)$$
$$\tau \mapsto \tau|_E$$

是同构.

(2)

$$\psi\colon \mathrm{Gal}(EK/F) \to \mathrm{Gal}(E/F) \times \mathrm{Gal}(K/F)$$
$$\tau \mapsto (\tau|_E, \tau|_K)$$

是单射. 如果 $E \cap K = F$, 那么上述映射还是满射, 从而使同构.

证明: 根据推论3.1.3可知 EK/F 是正规扩张. 根据推论3.2.12可知 EK/F 是可分扩张, 从而 EK/F 是 Galois 扩张, 并且由于 $E/F, K/F$ 都是有限的, 从而 EK/F 也是有限 Galois 扩张, 因此 EK/E 也是有限 Galois 扩张.

(1). 任取 $\tau \in \mathrm{Gal}(EK/K)$, 考虑 $\tau|_E : E \to EK \hookrightarrow \overline{F}$, 由于 E/F 是正规的, 从而根据定理3.1.2有 $\tau(E) \subseteq E$, 即 $\tau|_E \in \mathrm{Gal}(E/E \cap K)$. 如果 $\tau|_E = \mathrm{id}_E$, 那么由于 $\tau|_F = \mathrm{id}_F$ 有 $\tau = \mathrm{id}_{EK}$,

即 φ 是单射. 另一方面, $\operatorname{im}\varphi$ 是 $\mathrm{Gal}(E/E\cap K)$ 的子群, 并且 $E^{\operatorname{im}\varphi}=(EK)^{\mathrm{Gal}(EK/K)}\cap E=K\cap E$, 从而 $\operatorname{im}\varphi=\mathrm{Gal}(E/E\cap K)$.

(2). ψ 是单射与 φ 是单射的证明同理. 如果 $E\cap K=F$, 那么任取 $(\sigma_1,\sigma_2)\in \mathrm{Gal}(E/F)\times \mathrm{Gal}(K/F)$, 根据 (1) 有 σ_1,σ_2 可以被延拓成 $\sigma_1'\in \mathrm{Gal}(EK/K)$ 和 $\sigma_2'\in \mathrm{Gal}(EK/E)$. 令 $\tau=\sigma_2'\circ\sigma_1'\in \mathrm{Gal}(EK/F)$, 那么 $\tau|_K=\sigma_2'\circ\sigma_1'|_K=\sigma_2'|_K=\sigma_2$, 同理有 $\tau|_E=\sigma_1$, 从而是满射. □

定义 4.2.5. Galois 扩张被称为**阿贝尔扩张** (abelian extension), 如果其 Galois 群是阿贝尔群.

定义 4.2.6. Galois 扩张被称为**循环扩张** (cyclic extension), 如果其 Galois 群是循环群.

推论 4.2.7. *阿贝尔扩张的复合也是阿贝尔扩张, 循环扩张的复合也是循环扩张.*

证明: 注意到阿贝尔群 (循环群) 的子群还是阿贝尔群 (循环群). □

4.3 Galois 群的计算

4.3.1 简单多项式的分裂域

通过 Galois 对应, 我们可以计算一些常见的扩张的 Galois 群.

例子. *考虑 Galois 扩张 $\mathbb{Q}(\sqrt2,\sqrt3)/\mathbb{Q}$, 我们有如下的中间域:*

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt2,\sqrt3) \arrow[dl, no head] \arrow[dr, no head] & \\
\mathbb{Q}(\sqrt2) \arrow[dr, no head] & & \mathbb{Q}(\sqrt3) \arrow[dl, no head] \\
 & \mathbb{Q} &
\end{tikzcd}$$

其对应到子群

$$\begin{tikzcd}[column sep=small]
 & \{\mathrm{id}\} \arrow[dl, no head] \arrow[dr, no head] & \\
\langle\sigma\rangle \arrow[dr, no head] & & \langle\tau\rangle \arrow[dl, no head] \\
 & \mathrm{Gal}(\mathbb{Q}(\sqrt2,\sqrt3)/\mathbb{Q}) &
\end{tikzcd}$$

其中

$$\sigma:\begin{cases}\sqrt2\mapsto-\sqrt2\\ \sqrt3\mapsto\sqrt3\end{cases}\qquad \tau:\begin{cases}\sqrt2\mapsto\sqrt2\\ \sqrt3\mapsto-\sqrt3\end{cases}$$

由于 $\mathrm{Gal}(\mathbb{Q}(\sqrt2,\sqrt3)/\mathbb{Q})$ 是一个四阶群, 而我们已经找到了两个二阶子群 $\langle\sigma\rangle,\langle\tau\rangle$, 并且 $\sigma\tau=\tau\sigma$, 从而可知 $\mathrm{Gal}(\mathbb{Q}(\sqrt2,\sqrt3)/\mathbb{Q})=\mathbb{Z}_2\times\mathbb{Z}_2$.

注记. 注意到 $\mathbb{Z}_2\times\mathbb{Z}_2$ 还有一个二阶子群 $\langle\tau\sigma\rangle$, 其对应到的不变子域为 $\mathbb{Q}(\sqrt6)$.

例子. 考虑 $f(x)=x^3-2\in\mathbb{Q}[x]$ 的分裂域 $\mathbb{Q}(\sqrt[3]{2},\xi_3)/\mathbb{Q}$, 其中 $\xi_3=e^{\frac{2\pi\sqrt{-1}}{3}}$, 我们有如下的中间域:

$$\begin{tikzcd}[column sep=small]
& \mathbb{Q}(\sqrt[3]{2},\xi_3) \arrow[dl, dash, "2"'] \arrow[dr, dash, "3"] & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash, "3"'] & & \mathbb{Q}(\xi_3) \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}$$

对应到子群

$$\begin{tikzcd}[column sep=small]
& \{\mathrm{id}\} \arrow[dl, dash] \arrow[dr, dash] & \\
\langle\sigma\rangle \arrow[dr, dash] & & \langle\tau\rangle \arrow[dl, dash] \\
& G_f &
\end{tikzcd}$$

其中

$$\sigma\colon\begin{cases}\xi_3\mapsto\xi_3^2\\ \sqrt[3]{2}\mapsto\sqrt[3]{2}\end{cases}\qquad \tau\colon\begin{cases}\xi_3\mapsto\xi_3\\ \sqrt[3]{2}\mapsto\sqrt[3]{2}\xi_3\\ \sqrt[3]{2}\xi_3\mapsto\sqrt[3]{2}\xi_3^2\end{cases}$$

并且直接计算可知

$$\sigma\tau\neq\tau\sigma$$
$$\sigma\tau\sigma^{-1}=\tau^2$$

从而可知 $G_f=S_3$.

练习. 写出 S_3 的其他子群, 与其对应的不变子域.

命题 4.3.1. 令 E 是不可约多项式 $f(x)\in F[x]$ 的分裂域, $\alpha_1,\dots,\alpha_n$ 是 $f(x)$ 的根, 那么 $\mathrm{Gal}(K/F)$ 在 $\{\alpha_1,\dots,\alpha_n\}$ 上忠实地[1] *(faithfully)*, 可递地 *(transitively)* 作用, 并且 n 整除 $|\mathrm{Gal}(E/F)|$.

证明: 任取 $\sigma\in\mathrm{Gal}(E/F)$, 其完全被 $\sigma(\alpha_i)$ 所决定, 因此 $G_f\hookrightarrow S_n$. 并且是可递的, 因为可以定义

$$\sigma'\colon\alpha_i\to\alpha_j$$

再将其延拓成 $\mathrm{Gal}(E/F)$ 中的元素. 注意到 $\mathbb{Q}\subseteq\mathbb{Q}(\alpha_1)\subseteq E$, 由于 $[\mathbb{Q}(\alpha_1):\mathbb{Q}]$ 的扩张次数是 n, 因此 n 整除 $|\mathrm{Gal}(E/F)|$. □

注记. 根据上述命题, 不难直接看出 x^3-2 的 Galois 群就是 S_3.

4.3.2 有限域上的 Galois 扩张

定理 4.3.2. $q=p^m, m>0$, 则 $\mathbb{F}_{q^d}/\mathbb{F}_q$ 是 *Galois* 扩张, 并且 $\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)=\mathbb{Z}/d\mathbb{Z}$, 由弗罗贝尼乌斯同构 $\sigma\colon x\mapsto x^q$ 生成.

[1]即有单嵌入 $\mathrm{Gal}(E/F)\to S_n$.

4.3.3 模 p 方法

给定 n 次首一多项式 $f(x)\in\mathbb{Z}[x]$, 其判别式定义为 $D(f)=\prod_{i<j}(\alpha_i-\alpha_j)^2\in\mathbb{Z}$, 其中 α_i 是 $f(x)$ 的根. 如果记 $f_p(x)\equiv f(x)\pmod p$, 那么 $D(f_p)\neq 0$ 当且仅当素数 p 不整除 $D(f)$.

定理 4.3.3 (Dedekind)**.** $f(x)\in\mathbb{Z}[x]$ 是 n 次首一多项式, p 是使得 $f_p(x)$ 可分的素数, 假设 $f_p(x)$ 在 $(\mathbb{Z}/p\mathbb{Z})[x]$ 中分解成次数分别是 $n_1,\dots,n_r$ 的不可约多项式的乘积, 那么 G_f 中包含一个类型为 $(n_1,\dots,n_r)$ 的置换.

证明: 假设 K 是 f 的分裂域, $f(x)$ 在 K 中分裂为 $(x-\alpha_1)\dots(x-\alpha_n)$. 考虑 $R=\mathbb{Z}[\alpha_1,\dots,\alpha_n]\subseteq K$, 由于 $\alpha_1,\dots,\alpha_n$ 都是代数整数, 从而 R 中所有的元素都是代数整数. 由 p 生成的主理想 $pR\neq R$, 否则 $1/p\in R$ 导致 $1/p\in R\cap\mathbb{Q}=\mathbb{Z}$, 相矛盾. 取包含 pR 的一个极大理想 P, 因为 $\mathbb{Z}$ 可以自然的嵌入到 R 中, 我们有映射 $\mathbb{Z}\to R/P$, 并且 $p\mathbb{Z}$ 包含在映射的核里, 再由于 $p\mathbb{Z}$ 是 $\mathbb{Z}$ 的极大理想可知映射的核就是 $p\mathbb{Z}$, 即 R/P 是 $\mathbb{F}_p$ 的一个域扩张. 假设

$$f(x)\equiv(x-\overline{\alpha}_1)\dots(x-\overline{\alpha}_n)\pmod P$$

从而 $f(x)$ 在 R/P 中分裂, 并且 R/P 由 $\overline{\alpha}_1,\dots,\overline{\alpha}_n$ 生成, 因此 R/P 是 $f_p(x)$ 的分裂域.

因为 $\mathrm{Gal}(K/\mathbb{Q})$ 可以作用在 $\{\alpha_1,\dots,\alpha_n\}$ 上, 从而 $\mathrm{Gal}(K/\mathbb{Q})$ 可以作用在 R 上. 令 $D_P=\{\sigma\in\mathrm{Gal}(K/\mathbb{Q})\mid\sigma P=P\}$, 从而有映射

$$\begin{aligned}\varphi\colon D_P&\mapsto\mathrm{Aut}(R/P)\\ \sigma&\mapsto\sigma|_R\end{aligned}$$

□

引理 4.3.4. $G<S_n$ 是 S_n 可递子群, 假设 G 包含一个 2-轮换 σ 和 $(n-1)$-轮换 τ, 那么 $G=S_n$.

证明: 我们不妨取 $(n-1)$-轮换 $\tau=(23\dots n)$, 因为任何 $(n-1)$-轮换都可以生成它. 并且我们可以取 $\sigma=(1a)$, 因为任取 $\sigma'\in S_n$, 我们有:

$$\sigma'(ij)\sigma'^{-1}=(\sigma'(i)\sigma'(j))$$

因此只需根据 G 的可递性取 σ' 满足 $\sigma'(i)=1$ 即可. 考虑如下 τ^k 在 $(1a)$ 上的作用

$$\tau^k(1a)\tau^{-k}=(1\tau^k(a))$$

可以得到 $(12),(13),\dots,(1n)$, 即 $G=S_n$. □

引理 4.3.5. p 是素数, $G<S_p$, 并且 G 包含一个对换和 p-轮换, 则 $G=S_p$.

例子. 考虑 $f(x)=x^5-x-1$, 首先模 5 可知 $f_5(x)=x^5-x-1$ 是不可约的, 从而 G_f 中包含一个 5-轮换. 模 2 可知 $f_2(x)=(x^2+x+1)(x^3+x^2+1)$, 从而 G_f 包含一个对换, 从而可知 $G_f=S_5$.

例子. 考虑 $f(x)=x^6+22x^5+21x^4+12x^3-36x^2-29x-15$, 首先模 2 可知 $f_2(x)=x^6+x^4+x^2+x+1$, 分析其不可约性可知其不可约, 从而 G_f 中包含一个 6-轮换, 即 G_f 是 S_6 的可递子群. 模 3 可知 $f_3(x)=x(x^5+x^4-x+1)$, 从而 G_f 包含一个 5-轮换. 最后考虑模 5 得到 $f_5(x)=x(x-1)(x+1)(x+2)(x^2+2)$, 从而 G_f 包含 2-轮换, 从而根据引理4.3.4可知 $G_f=S_6$.

4.3.4 分圆扩张

定义 4.3.6. ξ_n 被称为 n **次本原单位根** (n-th primitive root of unity), 如果 $\xi_n^n = 1$ 且对任意 $k < n$ 有 $\xi_n^k \neq 1$.

注记.

(1) n 次单位根的全体可以表示为 $\{\xi_n^k \mid 0 \leq k \leq n-1\}$.

(2) ξ_n^k 也是 n 次本原单位根当且仅当 $(n,k) = 1$.

定义 4.3.7. n **次分圆多项式** (n-th cyclotomic polynomial)被定义为:

$$\Phi_n(x) = \prod_{(n,k)=1} (x - \xi_n^k)$$

定理 4.3.8. *$\mathbb{Q}(\xi_n)/\mathbb{Q}$ 是 Galois 扩张, 并且 $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$.*

证明: $\mathbb{Q}(\xi_n)/\mathbb{Q}$ 是 Galois 扩张, 因为是特征零域上的 $x^n - 1$ 的分裂域. 任取 $\tau \in \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$, 其一定形如 $\tau(\xi_n) = \xi_n^k$, 并且如果假设其逆映射为 $\tau^{-1}(\xi_n) = \xi_n^l$, 则

$$\xi_n = \tau^{-1}(\tau(\xi_n)) = \tau^{-1}(\xi_n^k) = \xi_n^{kl}$$

即 $kl \equiv 1 \pmod n$, 即 $k \in (\mathbb{Z}/n\mathbb{Z})^\times$, 因此有单射 $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$. 为了证明满射, 只需要证明任取素数 $p \nmid n$, 存在 $\tau \in \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$ 使得 $\tau(\xi_n) = \xi_n^p$. 令 $R = \mathbb{Z}[\xi_n]$ 以及 P 是包含 pR 的极大理想, 那么根据模 p 方法的证明过程可知 R/P 是 $\Phi_n(x) \mod p$ 的分裂域. 假设 $\sigma \in D_P$ 使得 $\sigma|_R$ 上给出了 $\mathrm{Gal}((R/P)/\mathbb{F}_p)$ 的弗罗贝尼乌斯映射, 即

$$\sigma(\overline{\xi_n}) = \overline{\xi_n}^p = \overline{\xi_n^p}$$

假设 $\sigma(\xi_n) = \xi_n^i$, 那么 $\overline{\xi_n^i} = \overline{\xi_n^p}$. 由于 $\Phi_n(x) \mid x^n - 1$, 以及 $x^n - 1 \mod p$ 无重根, 从而 $\Phi_n(x) \mod p$ 无重根, 因此 $\xi_n^i = \xi_n^p$, 证毕. □

推论 4.3.9. *$\Phi_n(x)$ 是不可约多项式.*

推论 4.3.10.

$$\Phi_n(x) \in \mathbb{Z}[x]$$

证明: 任取 $\tau \in \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$, 有

$$\begin{aligned}\tau(\Phi_n(x)) &= \tau(\prod_{(n,k)=1} (x - \xi_n^k)) \\ &= \prod_{(n,k)=1} (x - \xi_n^k) \\ &= \Phi_n(x)\end{aligned}$$

从而 $\Phi_n(x) \in \mathbb{Q}[x]$. 并且注意到 $\Phi_n(x)$ 的系数都是本原单位根的组合, 从而是代数整数, 因此 $\Phi_n(x) \in \mathbb{Z}[x]$. □

推论 4.3.11. *对于 $\mathbb{Q} \subseteq E \subseteq \mathbb{Q}(\xi_n)$, $E/\mathbb{Q}$ 是阿贝尔扩张.*

定理 4.3.12 (Kronecker-Weber). *如果 $E/\mathbb{Q}$ 是有限阿贝尔扩张, 则存在 n 使得 $\mathbb{Q} \subseteq E \subseteq \mathbb{Q}(\xi_n)$.*

下面列出一些有关 $(\mathbb{Z}/n\mathbb{Z})^\times$ 的结果:

命题 4.3.13. *如果 $n = p_1^{k_1} \dots p_r^{k_r}$, 则我们有:*

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{k_r}\mathbb{Z})^\times$$

命题 4.3.14. *当 $p \geq 3$ 时, 我们有:*

$$(\mathbb{Z}/p^k\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{k-1}\mathbb{Z}$$

是循环群.

命题 4.3.15. *当 $p = 2, k \geq 4$ 时, 我们有:*

$$(\mathbb{Z}/2^k\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$$

不是循环群.

例子. *多项式 $f(x) = x^5 - 2$ 的 Galois 群 G_f 为 $\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$.*

证明: 考虑下图

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt[5]{2}, \xi_5) \arrow[dl, dash, "4"'] \arrow[dr, dash, "5"] & \\
\mathbb{Q}(\sqrt[5]{2}) \arrow[dr, dash, "5"'] & & \mathbb{Q}(\xi_5) \arrow[dl, dash, "4"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

首先根据分圆扩张可知 $\mathrm{Gal}(\mathbb{Q}(\sqrt[5]{2}, \xi_5)/\mathbb{Q}(\sqrt[5]{2})) = (\mathbb{Z}/5\mathbb{Z})^\times = \mathbb{Z}/4\mathbb{Z}$, 由如下的映射生成:

$$\sigma : \begin{cases} \xi_5 \mapsto \xi_5^2 \\ \sqrt[5]{2} \mapsto \sqrt[5]{2} \end{cases}$$

另一方面 $\mathrm{Gal}(\mathbb{Q}(\sqrt[5]{2}, \xi_5)/\mathbb{Q}(\xi + 5)) = \mathbb{Z}/5\mathbb{Z}$, 由如下的映射生成

$$\tau : \begin{cases} \xi_5 \mapsto \xi_5 \\ \sqrt[5]{2}\xi_5^i \mapsto \sqrt[5]{2}\xi_5^{i+1} \quad i = 0, 1, 2, 3, 4 \end{cases}$$

因此找到了 G_f 的两个子群 $\mathrm{Gal}(\mathbb{Q}(\sqrt[5]{2}, \xi_5)/\mathbb{Q}(\xi_5)) = \mathbb{Z}/5\mathbb{Z}$ 以及 $\mathrm{Gal}(\mathbb{Q}(\sqrt[5]{2}, \xi_5)/\mathbb{Q}(\sqrt[5]{2})) = \mathbb{Z}/4\mathbb{Z}$, 其中前者还是正规子群. 由于 $\mathbb{Q}(\sqrt[5]{2}) \cap \mathbb{Q}(\xi_5) = \mathbb{Q}$ 意味着这两个子群的交平凡. $\mathbb{Q}(\sqrt[5]{2}) \cap \mathbb{Q}(\xi_5) = \mathbb{Q}$ 意味着 G_f 可以写成这两个子群的并, 从而

$$G_f \cong \mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$$

□

例子. *对于素数 p, 我们有 $f(x) = x^p - 2$ 的 Galois 群 $G_f \cong \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/(p-1)\mathbb{Z}$.*

练习. *对于素数 p, 证明 $f(x) = x^p - 2$ 的 Galois 群 G_f 同构于*

$$\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in (\mathbb{Z}/p\mathbb{Z})^\times, b \in \mathbb{Z}/p\mathbb{Z}\} \subseteq \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$$

第五章　Galois 理论的应用

5.1　尺规作图问题

对于一个没有刻度的直尺和圆规, 我们只可以通过以下的方式得到新的点:

(1) 两条直线的交点.

(2) 一条直线与一个圆的交点.

(3) 两个圆的交点.

定义 5.1.1. $(a,b)\in\mathbb{R}^2$ 被称为**可构造的** (constructable), 如果我们可以从 $(0,0),(1,0)$ 以及尺规作图得到 (a,b).

注记 (标准构造). 利用尺规, 我们有下面两种基本的做法:

(1) 给定线段 AB, 作出以 AB 为直径的圆.

(2) 给定直线 l 以及直线外一点 p, 可以作出过 p 与 l 垂直或平行的直线.

推论 5.1.2. *(a,b) 可构造当且仅当 $(a,0),(b,0)$ 可构造.*

定义 5.1.3. $c\in\mathbb{R}$ 称为**可构造的** (constructable), 如果 $(c,0)$ 可构造. 我们用 $\mathfrak{C}$ 记 $\mathbb{R}$ 中所有可构造的点.

命题 5.1.4.

(1) *$\mathfrak{C}$ 是 $\mathbb{R}$ 包含 $\mathbb{Q}$ 的子域.*

(2) *如果 $c\in\mathfrak{C},c>0$, 则 $\sqrt{c}\in\mathfrak{C}$*

证明: (1). 由于任何特征零的域都包含 $\mathbb{Q}$ 作为子域, 所以只需要证明 $\mathfrak{C}$ 是一个域即可. 如果 $c\in\mathfrak{C}$, 那么以 $(0,0)$ 为圆心 c 为半径画圆, 则有 $-c\in\mathfrak{C}$. 如果 $ab\in\mathfrak{C}$, 我们可以通过以下方式得到 a^{-1}.

(2). 如果 $c\in\mathfrak{C}$, 那么可以用如下的方式构造 $\sqrt{c}$. □

定义 5.1.5. $K\subseteq\mathbb{R}$ 是子域, **K 中的平面** (plane of K)定义为 $K\times K\subseteq\mathbb{R}\times\mathbb{R}$; **$K$ 中的直线** (line of K)定义为连接 K 平面中两点的直线; **K 中的圆** (circle of K)定义为圆心在 K 平面中, 半径在 K 中的圆.

引理 5.1.6. *我们有如下结果:*

(1) *两条 K 中直线的交点要么是空集, 要么是 K 中的点.*

(2) *一条 K 中的直线与一个 K 中的圆的交点要么是空集, 要么是 $K(\sqrt{\alpha}),\alpha\in K$ 中的点.*

(3) *两个 K 中的圆的交点要么是空集, 要么是 $K(\sqrt{\alpha}),\alpha\in K$ 中的点.*

证明: 只需要注意到 K 中的直线由下面方程定义:

$$ax + by + c = 0, \quad a, b, c \in K$$

K 中的圆由下面方程定义:

$$x^2 + y^2 + ax + by + c = 0, \quad a, b, c \in K$$

$\square$

定理 5.1.7. *$c \in \mathfrak{C}$ 当且仅当存在下面的域扩张链:*

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$$

(1) $c \in K_n$.
(2) $[K_n : K_{n-1}] = 2$, 即 $K_{i+1} = K_i(\sqrt{\alpha_i})$, 其中 $0 < \alpha_i \in K_i$.
特别地, 如果 c 可构造, 则 c 在 $\mathbb{Q}$ 上代数, 并且 $[\mathbb{Q}(c) : \mathbb{Q}]$ 是 2 的幂次.

证明: 假设 $c \in \mathfrak{C}$, 即 $(c, 0)$ 在 $\mathbb{R}^2$ 上可构造, 即 $(c, 0)$ 可以通过有限步画圆或化直线的操作得到. 在每一步中, 新的点由两条线的交点, 线与圆的交点以及圆与圆的交点得到, 从而根据引理5.1.6有期待的域扩张链.

另一方面, 如果我们假设这样域扩张链存在, 那么 c 在 K_{n-1} 上的极小多项式为 $x^2+ax+b \in K_{n-1}[x]$, 那么 $(c, 0)$ 可以通过圆 $(x + \frac{a}{2})^2 + y^2 = \frac{a^2}{4} - b$ 与 x 轴的交点的到. 根据命题5.1.4, 如果 α, β 可构造, 那么 $\alpha \pm \beta, \alpha\beta$ 都可构造. 由于 a, b 是 1 和 $\sqrt{\alpha_{n-2}}$ 在 K_{n-2} 上线性组合得到的, 而 K_{n-2} 可由在 K_{n-3} 上构造 $\sqrt{\alpha_{n-3}}$ 的到. 因此问题归结于在 K_{n-2} 上构造 $\sqrt{\alpha_{n-2}}$. 由于 $(\sqrt{\alpha_{n-2}}, 0)$ 是 $x^2 + y^2 = \alpha_{n-2}$ 与 x 轴的交点, 即经过有限步操作后 c 可构造. 特别地, 如果 c 可构造, 那么 $\mathbb{Q} \subseteq \mathbb{Q}(c) \subseteq K_n$, 从而 $[K_n : \mathbb{Q}(c)][\mathbb{Q}(c) : \mathbb{Q}] = 2^n$, 从而 $[\mathbb{Q}(c) : \mathbb{Q}]$ 也是 2 的幂次. $\square$

5.1.1 化圆为方

构造一个正方形, 使得其面积为给定的圆的面积: 这等价于 $\sqrt{\pi}$ 是否可构造? 显然是不可以的, 因为 π 在 $\mathbb{Q}$ 上超越.

5.1.2 倍立方体

构造一个立方体, 使得其体积为给定立方体的二倍, 这等价于 $\sqrt[3]{2}$ 是否可构造? 也是不可以的, 因为 $[\mathbb{Q}\sqrt[3]{2} : \mathbb{Q}] = 3$, 不是 2^n.

5.1.3 三等分角

给定角 θ, 三等分角即等价于构造 $\cos\theta/3$, 我们有如下的三角公式:

$$\cos\theta = 4\cos^3\theta/3 - 3\cos\theta/3$$

即等价于构造 $4x^3 - 3x - a = 0$ 的根, 我们给出下面的一些例子, 来说明这并非总是可以构造的:

例子. 如果 $a=\cos\frac{\pi}{3}=\frac{1}{2}$, 则此时是不可构造的, 因为等价于构造 $8x^3-6x-1=0$ 这个不可约多项式的根, 这是三次扩张.

例子. 如果 $a=\cos\frac{\pi}{4}$, 此时是可以构造的, 此时下述多项式:

$$4x^3-6x-\frac{\sqrt{2}}{2}\in\mathbb{Q}(\sqrt{2})[x]$$

是可约的, $-\frac{\sqrt{2}}{2}$ 是其一个根, 因此实际上此时是二次扩张.

5.1.4 尺规作正 n 边形状问题

正 n 边形是否尺规可作等价于 $\theta_n=2\pi/n$ 是否可构造, 我们有下述引理:

引理 5.1.8. 正 n 边形尺规可作等价于 $[\mathbb{Q}(\xi_n):\mathbb{Q}]=2^n$.

证明: 令 $\xi_n=\cos\theta_n+\sqrt{-1}\sin\theta_n$, 只需要注意到:

$$[\mathbb{Q}(\xi_n):\mathbb{Q}(\theta_n)]\leq 2$$

即可. □

定理 5.1.9. 正 n 边形尺规可作等价于 n 有如下分解:

$$n=2^kp_1\dots p_k$$

其中 p_k 是不同的 *Fermat* 素数.

证明: 由于 $[\mathbb{Q}(\xi_n):\mathbb{Q}]=\phi(n)$, 令 $n=2^kp_1^{r_1}\dots p_s^{r_s}$, 则

$$\phi(n)=2^{k-1}(p_1-1)p^{r_1-1}\dots(p_s-1)p^{r_s-1}$$

若为 2 的幂次, 应该有 $r_i\leq 1$, p_i 形如 2^m+1, 但是形如 2^m+1 的素数一定是 $2^{2^n}+1$ 的形式, 即为 Fermat 素数. □

注记. 有关 Fermat 素数, 是形如 $2^{2^n}+1$ 的素数, 实际上, 现在对 Fermat 素数的所知仍然很少, 已知的五个 Fermat 素数为 $n=0,1,2,3,4$ 的情况, 对于 $n>4$ 的情况, 所能验证的都不是素数, 但是否仅仅只有这五个 Fermat 素数, 还是一个猜想.

5.2 代数基本定理的证明

命题 5.2.1. 对于任何 p-群 G, 都存在 G_i 使得

$$G\supseteq G_1\supseteq G_2\supseteq\cdots\supseteq G_n=\{e\}$$

满足 $|G_i/G_{i+1}|=p$.

定理 5.2.2. 任何 $f(x)\in\mathbb{C}[x]$ 在 $\mathbb{C}$ 中都有根.

证明: 考虑 $f(x)\overline{f(x)}\in\mathbb{R}[x]$, 如果 $f(x)\overline{f(x)}$ 有复根 α, 那么 α 或 $\overline{\alpha}$ 是 $f(x)$ 的一个复根, 从而我们不妨在一开始就假设 $f(x)\in\mathbb{R}[x]$. 记 $|G_f|=n$, 考虑 G_f 的西罗 2-子群 H, 那么 $[G_f:H]$ 是奇数, 从而根据 Galois 主定理对应到 $\mathbb{R}$ 的一个奇数次扩域 L, 然而任何奇数次多项式 $f(x)\in\mathbb{R}[x]$ 在 $\mathbb{R}$ 中都有根, 从而 $L=\mathbb{R}$, 再根据 Galois 主定理有 $G_f=H$, 即 $|G_f|=2^n$.

根据命题5.2.1可知存在 G_i 使得

$$G_f\supseteq G_1\supseteq G_2\supseteq\cdots\supseteq G_n=\{e\}$$

使得 $|G_i/G_{i+1}|=2$. 注意到 $\mathbb{R}$ 的任何二次扩张都同构于 $\mathbb{C}$, 从而 G_1 对应的 $\mathbb{R}$ 的扩域就是 $\mathbb{C}$, 但是 $\mathbb{C}$ 没有非平凡的二次扩域, 从而 $K_2=\cdots=K_n=\mathbb{C}$, 从而 $f(x)$ 的分裂域就是 $\mathbb{C}$, 即 $f(x)$ 有复根. □

5.3 根式可解问题

在本节中, 所有的域的特征都是 0.

5.3.1 根式扩张与根式可解

定义 5.3.1. 有限扩张 E/F 被称为**根式扩张** (radical extension), 如果存在 $\alpha_1,\dots,\alpha_n\in E, m_1,\dots,m_n\in\mathbb{N}$, 使得:

(1) $E=F(\alpha_1,\dots,\alpha_n)$

(2) $\alpha_1^{m_1}\in F$, 并且对 $2\le i\le n$ 有 $\alpha_i^{m_i}\in F(\alpha_1,\dots,\alpha_{i-1})$.

即:

$$F\subseteq F(\alpha_1)\subseteq\cdots\subseteq F(\alpha_1,\dots,\alpha_n)$$

其中每一步被称为**单根式扩张** (simple radical extension).

注记. 根式扩张不一定是 Galois 扩张, 例如 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

定义 5.3.2. $f(x)\in F[x]$ 被称为**根式可解** (solvable by radical), 如果其分裂域包含在 F 的某个根式扩张中.

命题 5.3.3.

(1) *如果 $F\subseteq E\subseteq K$, 其中 K/F 是根式扩张, 则 K/E 也是根式扩张, 但 E/F 不一定是根式扩张*[1].

(2) *如果 $K/E, E/F$ 都是根式扩张, 则 K/F 也是根式扩张.*

(3) *如果 $E/F, E'/F$ 都是根式扩张, 则 EE'/F 也是根式扩张.*

(4) *如果 E/F 是根式扩张, 则其 Galois 闭包 K/F 也是根式扩张.*

证明: (1). 如果 K/F 是根式扩张, 那么有 $K=F(\alpha_1,\dots,\alpha_n)$, 其中 $\alpha_1,\dots,\alpha_n$ 满足定义里的要求, 那么自然有 $K=E(\alpha_1,\dots,\alpha_n)$, 即 K/E 也是根式扩张.

(2). 如果 $E=F(\alpha_1,\dots,\alpha_n), K=E(\alpha_{n+1},\dots,\alpha_m)$, 那么 $K=F(\alpha_1,\dots,\alpha_m)$, 即 K/F 是根式扩张.

[1]这条性质与正规扩张类似.

(3). 假设 $E=F(\alpha_1,\dots,\alpha_n)$, 那么 $EE'=E'(\alpha_1,\dots,\alpha_n)$, 并且 $\alpha_i^{m_i}\in F(\alpha_1,\dots,\alpha_{i-1})\subseteq E'(\alpha_1,\dots,\alpha_{i-1})$, 从而 EE'/E' 是根式扩张, 从而根据 (2) 可知 EE'/F 也是根式扩张.

(4). 假设 $E=F(\alpha_1,\dots,\alpha_n)$, 其中 $\alpha_i^{m_i}\in F(\alpha_1,\dots,\alpha_{i-1})$, 那么 Galois 闭包 K 由所有 $P_{\alpha_i,F}$ 的根生成. 令 $G=\mathrm{Gal}(K/F)$, 任取 $\tau\in G$, 那么 $\tau(E)=F(\tau(\alpha_1),\dots,\tau(\alpha_n))$ 在 F 上也是根式扩张, 因为 $\tau(\alpha_i)^{m_i}=\tau(\alpha_i^{m_i})\in\tau(F(\alpha_1,\dots,\alpha_{i-1}))=F(\tau(\alpha_1),\dots,\tau(\alpha_{i-1}))$. 从而根据 (3) 有 $K=\prod_\tau\tau(E)$ 是根式扩张. □

5.3.2 可解群及其性质

本节中的群 G 都是有限群.

定义 5.3.4. 群 G 的**换位子群** (commutator group), 定义为由形如 $ghg^{-1}h^{-1}$, 其中 $g,h\in G$ 生成的子群, 记作 $[G,G]$.

记号 5.3.5. 给定群 G, 记 $G^{(1)}=[G,G]$, 以及 $G^{(i)}:=[G^{(i-1)},G^{(i-1)}],i\geq 2$.

命题 5.3.6. *给定群 G, 有*

(1) *$[G,G]$ 是 G 的正规子群.*

(2) *$G/[G,G]$ 是阿贝尔群.*

(3) *对于群同态 $\varphi\colon G\to H$, 如果 H 是阿贝尔群, 那么 $[G,G]\subseteq\ker\varphi$.*

定义 5.3.7. 群 G 被称为**可解群** (solvable group), 如果 $G^{(n)}=\{e\}$ 对某个 $n\in\mathbb{Z}_{>0}$ 成立.

命题 5.3.8. *如果 G 是非交换的单群, 则 G 不是可解群.*

证明: 注意到 $G=G^{(1)}=\cdots=G^{(n)}$ 对任意 $n\in\mathbb{Z}_{>0}$ 成立, 从而 G 不是可解群. □

推论 5.3.9. *$A_n,n\geq 5$ 时不是可解群.*

命题 5.3.10. *如下叙述等价:*

(1) *群 G 可解.*

(2) *如果 G 存在一个子群链 $G=G_0\supseteq G_1\supseteq\cdots\supseteq G_n=\{e\}$, 满足 $G_{i+1}\lhd G_i$, 并且 G_i/G_{i+1} 是阿贝尔群.*

(3) *如果 G 存在一个子群链 $G=G_0\supseteq G_1\supseteq\cdots\supseteq G_n=\{e\}$, 满足 $G_{i+1}\lhd G_i$, 并且 G_i/G_{i+1} 是素数阶循环群.*

推论 5.3.11. *p-群是可解群.*

证明: 根据命题5.2.1即可. □

命题 5.3.12.

(1) *如果 G 是可解群, $H<G$, 则 H 也是可解群.*

(2) *如果 G 是可解群, $H\lhd G$, 那么 G/H 也是可解群.*

(3) *如果 $H\lhd G$, 且 $H,G/H$ 都是可解群, 则 G 也是可解群.*

(4) *如果 G 是可解群, 则 G 有个极大正规子群, 其指数为素数 p.*

5.3.3 根式可解与可解群

命题 5.3.13. *如果 E/F 是有限 Galois 根式扩张, 则 $\operatorname{Gal}(E/F)$ 是可解群.*

证明: 假设 $E=F(\alpha_1,\dots,\alpha_n)$, 其中 $\alpha_i^{m_i}\in F(\alpha_1,\dots,\alpha_{i-1})$, 我们对 n 做归纳法. 当 $n=1$ 时, $E=F(\alpha_1)$, 并且 $\alpha_1^{m_1}\in F$, 注意到 $E\subseteq F(\alpha_1,\xi_{m_1})$, 从而根据命题5.3.12的 (2) 可知只需要证明 $\operatorname{Gal}(F(\alpha_1,\xi_{m_1})/F)$ 是可解群即可. 考虑下图

$$\begin{tikzcd}
F(\alpha_1,\xi_{m_1}) \arrow[d, dash] \\
F(\xi_{m_1}) \arrow[d, dash] \\
F
\end{tikzcd}$$

由于 $F(\xi_{m_1})$ 是 m_1 次本元多项式的分裂域, 从而 $F(\xi_{m_1})/F$ 是 Galois 扩张. 根据 Galois 对应, $\operatorname{Gal}(F(\alpha_1,\xi_{m_1})/F(\xi_{m_1}))$ 是 $\operatorname{Gal}(F(\alpha_1,\xi_{m_1})/F)$ 的正规子群, 并且

$$\operatorname{Gal}(F(\xi_{m_1})/F)\cong\operatorname{Gal}(F(\alpha_1,\xi_{m_1})/F)/\operatorname{Gal}(F(\alpha_1,\xi_{m_1})/F(\xi_{m_1}))$$

那么根据命题5.3.12的 (3), 我们只需要证明 $\operatorname{Gal}(F(\xi_{m_1})/F)$ 和 $\operatorname{Gal}(F(\alpha_1,\xi_{m_1})/F(\xi_{m_1}))$ 是可解群即可. 考虑如下图

$$\begin{tikzcd}
 & F(\xi_{m_1}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\xi_{m_1}) \arrow[dr, dash] & & F \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

我们有嵌入 $\operatorname{Gal}(F(\xi_{m_1})/F)\hookrightarrow\operatorname{Gal}(\mathbb{Q}(\xi_{m_1})/\mathbb{Q})\cong(\mathbb{Z}/m_1\mathbb{Z})^\times$, 从而 $\operatorname{Gal}(F(\xi_{m_1})/F)$ 是阿贝尔群, 从而是可解群. 另一方面, 任取 $\tau\in\operatorname{Gal}(F(\alpha_1,\xi_{m_1})/F(\xi_{m_1}))$, τ 完全由其在 α_1 上的值决定, 由于 $x^{m_1}-\alpha_1^{m_1}$ 的所有根是 $\alpha_1\xi_{m_1}^k$, 其中 $0\le k\le m_1-1$, 因此 $\tau(\alpha_1)=\alpha_1\xi_{m_1}^k$, 并且由于 $\tau(\xi_{m_1})=\xi_{m_1}$, 从而可知 $\operatorname{Gal}(F(\alpha_1,\xi_{m_1})/F(\xi_{m_1}))$ 是一个阿贝尔群, 从而是个可解群, 至此我们解决了 $n=1$ 的情况. 对于一般情况, 我们考虑下图

$$\begin{tikzcd}
E=F(\alpha_1)(u_2,\dots,\alpha_n) \arrow[r, dash] \arrow[d, dash] & E(\xi_{m_1}) \arrow[d, dash] \\
F(\alpha_1) \arrow[r, dash] \arrow[d, dash] & F(\alpha_1,\xi_{m_1}) \\
F \arrow[ur, dash] &
\end{tikzcd}$$

首先我们有 $\operatorname{Gal}(F(\alpha_1,\xi_{m_1})/F)$ 是可解群, 并且根据归纳假设 $\operatorname{Gal}(E(\xi_{m_1})/F(\alpha_1,\xi_{m_1}))$ 是可解群, 根据命题5.3.12的 (3) 有 $\operatorname{Gal}(E(\xi_{m_1})/F)$ 是可解群, 再根据命题5.3.12的 (1) 有 $\operatorname{Gal}(E/F)$ 是可解群. □

引理 5.3.14 (Kummer)**.** *假设域 F 包含 p 次单位根 ξ_p, 其中 p 是素数. 域扩张 E/F 是 p 次 Galois 扩张当且仅当 $E=F(\alpha)$, 其中 $\alpha\notin F,\alpha^p\in F$.*

证明: 假设 E/F 是 p 次 Galois 扩张, 即 $\mathrm{Gal}(E/F)=\langle\sigma\rangle$ 是一个 p 阶循环群. 将 E 视作 p 维 F-线性空间, $\sigma\colon E\to E$ 是 F-线性变换, 满足 $\sigma^p=1$. 由于 F 含有 ξ_p, 从而 σ 可对角化, 并且特征值为 $\{1,\xi_p,\dots,\xi_p^{p-1}\}$, 考虑 ξ_p 对应的特征向量 α, 那么

$$\sigma(\alpha^i)=\sigma(\alpha)^i=(\xi_p\alpha)^i=\xi_p^i\alpha^i$$

对任意 $0\le i\le p-1$ 成立, 从而 $\{1,\alpha,\dots,\alpha^{p-1}\}$ 构成了一组 E/F 的基, 并且 $\alpha^p\in F$, 从而 α 对应的极小多项式为 $x^p-\alpha^p$, 从而 $E=F(\alpha)$. 另一方面, 假设 $E=F(\alpha),\alpha\notin F,\alpha^p\in F$, 那么 E 是 $x^p-\alpha^p$ 的分裂域, 下面只需证明 $[E:F]=p$ 即可: 考虑 $\sigma\in\mathrm{Gal}(E/F)$, 其中 $\sigma(\alpha)=\xi_p\alpha$, 可知 $\mathrm{Gal}(E/F)$ 在 $\{\alpha,\xi_p\alpha,\dots,\xi_p^{p-1}\alpha\}$ 上的作用是可递的, 从而 $x^p-\alpha^p$ 是 α 的极小多项式, 从而 $[E:F]=p$. □

定理 5.3.15. *K/F 是有限 Galois 扩张, 并且 $\mathrm{Gal}(K/F)$ 是可解群, 那么 K 包含在 F 的某个根式扩张中.*

证明: 我们对 $[K:F]=n$ 进行归纳. 假设 $n=2$, 由于任何二次方程 $x^2+ax+b=0$ 有求根公式, 从而 E/F 本身就是根式扩张. 假设命题对 $[K:F]\le n-1,n\ge 2$ 时成立, 考虑如下图

$$\begin{tikzcd}
K \arrow[r, dash] \arrow[d, dash] & K(\xi_p) \arrow[r, dash] \arrow[d] & L \arrow[dl, dash] \\
F \arrow[r, dash] & F(\xi_p) &
\end{tikzcd}$$

由于 $\mathrm{Gal}(K/F)$ 是可解群, 根据命题5.3.12的 (4) 可知其存在一个指数是素数 p 的正规子群, 我们将 p 次本原单位根 ξ_p 添加到 E 中, 那么由于 $F\subseteq K$, 则 $[K(\xi_p):E]\le[F(\xi_p):F]$, 因此 $[K(\xi_p):K]\le n$. 我们分以下两种情况考虑:

1. 如果 $[K(\xi_p):F(\xi_p)]<n$, 那么根据归纳假设 $K(\xi_p)$ 包含在某个 F 的根式扩张 L 中, 进而 L/F 是根式扩张, 并且包含 K.
2. 如果 $[K(\xi_p):K(\xi_p)]=n$. 我们令 $E=K(\xi_p)^H$, 其中 H 是 $\mathrm{Gal}(K/F)$ 指数为 p 的正规子群. 考虑下图

$$\begin{tikzcd}
K(\xi_p) \arrow[r, dash] \arrow[d, dash] & L \arrow[dl, dash] \\
E \arrow[d, dash] & \\
F(\xi_p) &
\end{tikzcd}$$

   由于 H 是正规子群, 从而 $E/F(\xi_p)$ 是次数为 p 的 Galois 扩张, 那么根据引理5.3.14可知其为单根式扩张, 再根据归纳假设有 $K(\xi_p)/E$ 包含在某个根式扩张 L/E 中, 因此 $L/F(\xi_p)$ 也是根式扩张.

□

定理 5.3.16. *$f(x)\in F[x]$ 根式可解当且仅当 G_f 是可解群.*

证明: 如果 $f(x)$ 根式可解, 因此分裂域 E 包含在 F 的某个根式扩张 K 中, 并且不妨假设 K/F 是 Galois 的, 因为根据命题5.3.3的 (4) 根式扩张的 Galois 闭包依然是根式扩张. 根据命

题5.3.13有 $\mathrm{Gal}(K/F)$ 是可解群, 则 $G_f = \mathrm{Gal}(E/F) \hookrightarrow \mathrm{Gal}(K/F)$, 也是一个可解群. 另一方面, 根据定理5.3.15即可. $\square$

5.4 求根公式

5.4.1 五次及以上方程无求根公式

给定环 R, S_n 在 $R[x_1, \ldots, x_n]$ 上有如下的作用

$$\sigma \cdot f(x_1, \ldots, x_n) := f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

定义 5.4.1. S_n 作用下不变的子环 $R[x_1, \ldots, x_n]^{S_n}$ 中的元素称为 R 系数的**对称多项式** (symmetric polynomial).

例子 (初等对称多项式)**.**

$$\begin{aligned} s_1 &= \sum_{i=1}^{n} x_i \\ s_2 &= \sum_{1\le i<j\le n} x_i x_j \\ &\vdots \\ s_n &= x_1 \ldots x_n \end{aligned}$$

定理 5.4.2 (对称多项式基本定理)**.**

$$\begin{aligned} \varphi\colon R[y_1, \ldots, y_n] &\to R[x_1, \ldots, x_n]^{S_n} \\ g(y_1, \ldots, y_n) &\mapsto g(s_1, \ldots, s_n) \end{aligned}$$

则 φ 是环同构.

证明: φ 是满射: 任取 $f \in R[x_1, \ldots, x_n]^{S_n}$, 那么 $f(x_1, \ldots, x_{n-1}, 0) \in \mathbb{R}[x_1, \ldots, x_{n-1}]^{S_{n-1}}$, 根据归纳假设存在 $n-1$ 元多项式 g 使得

$$f(x_1, \ldots, x_{n-1}, 0) = g(x_1, \ldots, x_{n-1})$$

令 $h(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) - g(s_1, \ldots, s_{n-1})$, 如果 $h \equiv 0$, 那么证明结束. 如果 $h \neq 0$, 根据构造有 $h(x_1, \ldots, x_{n-1}, 0) = 0$, 即 x_n 整除 $h(x_1, \ldots, x_n$, 并且注意到 $h(x_1, \ldots, x_n)$ 是 S_n 不变的, 从而任取 $1 \le i \le n$, 都有 $x_i \mid h(x_1, \ldots, x_n)$, 因此不妨假设

$$h(x_1, \ldots, x_n) = x_1 \ldots x_n H(x_1, \ldots, x_n)$$

此时 $\deg H < \deg h$, 再对次数做归纳则可知 $H(x_1, \ldots, x_n)$ 是初等对称多项式的组合, 从而 $h(x_1, \ldots, x_n)$ 也是.

φ 是单射: 假设 $\varphi(g) = 0$, 即 $g(s_1, \ldots, s_n) = 0$, 特别地有 $g(s_1, \ldots, s_{n-1}, 0) = 0$. 根据归纳假设有 $g(y_1, \ldots, y_{n-1}, 0) = 0$, 从而 $y_n \mid g(y_1, \ldots, y_n)$, 不妨假设

$$g(y_1, \ldots, y_n) = y_n h(y_1, \ldots, y_n)$$

利用 $\varphi(g)=0$ 有

$$x_1\dots x_n\varphi(h)=0$$

即 $\varphi(h)=0$, 并且 $\deg h<\deg g$, 再对次数做归纳即可. □

推论 5.4.3.

$$F(y_1,\dots,y_n)\cong F(x_1,\dots,x_n)^{S_n}$$

是域同构.

证明: 首先 $\varphi\colon F[x_1,\dots,x_n]\to F[x_1,\dots,x_n]^{S_n}$ 给出了分式域之间的同态

$$\begin{aligned}\varphi\colon F(y_1,\dots,y_n)&\to F(x_1,\dots,x_n)^{S_n}\\ \frac{f(y_1,\dots,y_n)}{g(y_1,\dots,y_n)}&\mapsto\frac{f(s_1,\dots,s_n)}{g(s_1,\dots,s_n)}\end{aligned}$$

下面只需要证明是满射: 任取 $\tau=\dfrac{f(x_1,\dots,x_n)}{g(x_1,\dots,x_n)}\in F(x_1,\dots,x_n)^{S_n}$, 考虑

$$r=\frac{f(x_1,\dots,x_n)\prod_{\sigma\in S_n\setminus\{\mathrm{id}\}}\sigma g}{\prod_{\sigma\in S_n}\sigma g}$$

由于 $\prod_{\sigma\in S_n}\sigma g$ 以及 r 都在 $F(x_1,\dots,x_n)^{S_n}$ 中, 从而

$$r\prod_{\sigma\in S_n}\sigma g\in F[x_1,\dots,x_n]\cap F(x_1,\dots,x_n)^{S_n}=F[x_1,\dots,x_n]^{S_n}$$

□

令 $K=F(x_1,\dots,x_n)$ 以及 $S_n\subseteq\mathrm{Aut}_F(K)$, 那么 $K^{S_n}=F(s_1,\dots,s_n)$ 并且 K/K^{S_n} 是 Galois 扩张, 并且实际上 K 是

$$x^n-s_1x^{n-1}+\cdots+(-1)^ns_n=0$$

的分裂域. 即我们找到了一个多项式 $f(x)$, 使得其 Galois 群 $G_f=S_n$. 由于我们知道 A_n 在 $n\geq 5$ 的时候不可解, 从而 S_n 在 $n\geq 5$ 的时候不可解, 即不存在五次及以上的多项式的求根公式.

注记. 对于素数 p, Galois 群为 S_p 的多项式的存在性更容易一些.

定理 5.4.4. *p 是素数, f 是 $\mathbb{Q}$ 上恰有两个虚根的不可约 p 次多项式, 则 $G_f\cong S_p$.*

证明: 首先复共扼 $c\colon a+b\sqrt{-1}\mapsto a-b\sqrt{-1}$ 属于 G_f, 对应于一个对换. 并且根据柯西定理, 对于一个有限群, 如果素数 p 整除群的阶数, 则其中包含一个 p 阶的元素, 这对应于 S_p 中的一个 p 轮换. 根据引理4.3.5可知 $G_f\cong S_p$. □

5.4.2 低次方程求根公式

给定三次多项式 $x^3-s_1x^2+s_2x-s_3$, 有 Galois 对应如下

$$\begin{array}{ccc} K=F(x_1,x_2,x_3) & \quad & \{\mathrm{id}\} \\ \Big| & & \Big| \\ L & & A_3 \\ \Big| & & \Big| \\ E=F(s_1,s_2,s_3) & & S_3 \end{array}$$

即 L 是 K 的 A_3 不变子域. 令

$$D=(x_1-x_2)(x_1-x_3)(x_2-x_3)$$

注意到 D 在 A_3 下不变, 并且 $[E(\sqrt{D}):E]=[L:E]=2$, 从而有 $L=E(\sqrt{D})$. 取 $\sigma\in A_3=\mathrm{Gal}(K/L)$, 其中

$$\sigma(x_1)=x_2$$
$$\sigma(x_2)=x_3$$
$$\sigma(x_3)=x_1$$

假设 F 中有三次单位根 ξ_3, 考虑

$$t_1=x_1+\xi_3x_2+\xi_3^2x_3$$
$$t_2=x_2+\xi_3x_3+\xi_3^2x_1$$

直接验证则有 $t_1^3,t_2^3\in E(\sqrt{D})$, 如果我们将 t_1^3,t_2^3 用 $\sqrt{D}$ 以及 s_1,s_2,s_3 表示出来, 并注意到 $\sqrt{D}$ 可以写成 s_1,s_2,s_3 的组合, 因此我们可以给出三次方程的求根公式.

注记. 四次方程的求根公式也可由上述步骤给出.

5.5 Kummer 理论

在本节中[2], 域 F 总是满足如下两条假设:

(1) F 包含 n 次本原单位根 ξ_n, 并用 μ_n 表示全体单位根组成的群.

(2) x^n-1 在 F 中有 n 个不同的根.

引理 5.5.1. *令 $a\in F^\times$, m 是 a 在 $F^\times/(F^\times)^n$ 中的阶数, 那么 x^n-a 的每个不可约因子都是 $x^m-b, b\in F$ 的形式.*

证明: 即证明如果 α 是 $P(x)=x^n-a$ 在 $\overline{F}$ 中的根, 则 $P_{\alpha,F}=x^m-b, b\in F$ 的形式. 首先, 由于 $a^m\in(F^\times)^n$, 因此存在 $b\in F^\times$, 使得 $a^m=b^n$. 而 $\alpha^n=a$, 因此 $\alpha^{nm}=b^n$, 即 $a^m/b\in\mu_n\subseteq F$. 由于 $b\in F^\times$ 我们有 $\alpha^m\in F^\times$, 因此 $P_{\alpha,F}\mid x^m-b$, 下面只需要证明 $\deg P_{\alpha,F}=m$ 即可. 不妨记 $\deg P_{\alpha,F}=d$, 由于 $P(x)=\prod_{i=0}^{n-1}(x-\alpha\xi_n^i)$, 因此 $P_{\alpha,F}=\prod_{i\in S}(x-\alpha\xi_n^i)$, 其中 $|S|=d$. 将 $P_{\alpha,F}$ 展开, 考虑其常数项则有 $\alpha^d\xi_n^i\in F\implies\alpha^d\in F$. 因此:

$$a^d=(\alpha^n)^d=(\alpha^d)^n\in(F^\times)^n$$

[2]对于一般的域也有 Kummer 理论, 但为了方便起见, 我们在这种域上考虑.

因此 $m \mid d$, 再加上 $d \leq m$, 从而有 $m = d$. $\square$

命题 5.5.2. *$E = F(\alpha)$, 其中 $\alpha^n = a \in F^\times$, 则 E/F 是 m 次循环扩张, 其中 m 是 a 在 $F^\times/(F^\times)^n$ 中的阶数.*

证明: 首先引理5.5.1可知 E/F 的扩张次数就是 m. 由于 $x^n - a$ 的所有根是 $\{\alpha\xi_n^i \mid 0 \leq i \leq n-1\}$ 是不同的, 进而 α 的极小多项式也没有重根, 从而 α 是 F 上的可分元, 根据定理3.2.9可知 E/F 是可分扩张; 并且由于 E 是 $x^n - a$ 的分裂域, 从而根据定理3.1.2可知 E 是正规扩张, 从而 E/F 是 Galois 扩张. 最后我们来证明其为循环扩张: 考虑映射

$$\begin{aligned} \varphi\colon \operatorname{Gal}(E/F) &\to \mu_n \\ \sigma &\mapsto \frac{\sigma(\alpha)}{\alpha} \end{aligned}$$

这定义了一个群同态, 因为:

$$\varphi(\sigma\tau) = \frac{\sigma\tau(\alpha)}{\alpha} = \frac{\sigma\varphi(\tau)}{\alpha} = \varphi(\tau)\frac{\sigma(\alpha)}{\alpha} = \varphi(\sigma)\varphi(\tau)$$

并且是单射, 因为如果 $\varphi(\sigma) = 1$, 即 $\sigma(\alpha) = \alpha$, 这意味着 σ 固定 E, 从而根据定理4.2.1, 即 Galois 对应可知 $\sigma = \mathrm{id}$. 因此 $\operatorname{Gal}(E/F)$ 嵌入到循环群 μ_n 中, 也是一个循环群. $\square$

定理 5.5.3 (Kummer)**.** *给定有限 Galois 扩张 E/F, 其 Galois 群为 n 阶循环群 $\langle\sigma\rangle$, 则 $E = F(\alpha), \alpha^n \in F^\times$.*

证明: 根据引理4.1.7存在 $\gamma \in F^\times$ 使得

$$\alpha := \sum_{i=0}^{n-1} \xi_n^i \sigma^i(\gamma) \neq 0$$

从而 $\sigma(\alpha) = \xi_n^{-1}\alpha$, 进而 $\sigma(\alpha^n) = (\sigma(\alpha))^n = \alpha^n$. 下面说明 $E = F(\alpha)$, 只需要证明 $\operatorname{Gal}(E/F(\alpha)) = \{\mathrm{id}\}$. 如果存在 $\tau = \sigma^k \in \operatorname{Gal}(E/F(\alpha))$, 则 $\tau(\alpha) = \sigma^k(\alpha) = \xi_n^k\alpha$, 那么 $\xi_n^k = 1$, 而 ξ_n 是本原单位根, 因此 $k = n$, 即 $\tau = \mathrm{id}$. $\square$

推论 5.5.4.

$$\{F \text{ 的 } \mathbb{Z}/n\mathbb{Z} \text{ 扩张}\} \xleftrightarrow{1-1} \{a \in F^\times/(F^\times)^n, \text{其中 } a \text{ 的阶数为 } n\}$$

证明: 命题5.5.2给出了从左往右的对应, 定理 5.5.3 说明这个对应是满射, 现在只需证明对应是单射: 假设 $F(\alpha) = F(\beta)$ 是 F 的两个 $\mathbb{Z}/n\mathbb{Z}$ 扩张, 其中 $\alpha^n = a \in F^\times, \beta^n = b \in F^\times$, 我们要证明 a, b 在 $F^\times/(F^\times)^n$ 中的阶数相同. 根据命题5.5.2的证明过程, 我们可以定义映射:

$$\varphi_\alpha(\sigma) = \frac{\sigma(\alpha)}{\alpha}$$
$$\varphi_\beta(\sigma) = \frac{\sigma(\beta)}{\beta}$$

并且由构造可知 $\dfrac{\sigma(\alpha)}{\alpha}, \dfrac{\sigma(\beta)}{\beta}$ 都是 n 次本原单位根, 因此存在整数 k 满足 $(k, n) = 1$ 使得

$$\frac{\sigma(\alpha)}{\alpha} = (\frac{\sigma(\beta)}{\beta})^k$$

即 $\sigma(\alpha\beta^{-k}) = \alpha\beta^{-k}$, 这意味着 $\alpha\beta^{-k} \in F^\times$, 并且注意到 $ab^{-k} = (ab^{-k})^n \in (F^\times)^n$, 从而在 $F^\times/(F^\times)^n$ 中 $a = b^k$, 由于 $(k, n) = 1$ 可知 a, b 的阶数相同. $\square$

定义 5.5.5. n 次扩张 E/F 被称为 **Kummer 扩张** (Kummer extension), 如果其为一个阿贝尔扩张, 并且其 Galois 群 $\mathrm{Gal}(E/F)$ 的指数[3]整除 n.

定理 5.5.6. *E/F 是 Kummer 扩张, 当且仅当 $E = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r}), a_i \in F^\times$.*

证明: 一方面, $F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r})$ 是 $F(\sqrt[n]{a_i})$ 的复合, 因此:

$$\mathrm{Gal}(K/F) \hookrightarrow \prod_i \mathrm{Gal}(F(\sqrt[n]{a_i})/F)$$

是一个指数整除 n 的阿贝尔群. 另一方面, 考虑阿贝尔群的分解:

$$\mathrm{Gal}(E/F) \cong C_1 \times \cdots \times C_r$$

其中 C_r 是阶数整除 n 的循环群, 令 $H_i = \prod_{j \neq i} H_j \times \{1\}$, 令 $K_j = K^{H_j}$, 那么 $\mathrm{Gal}(K_j/F) \cong C_i$, 因此 $K_j = F(\sqrt[n]{a_i})$, 下面只需要说明 $K = K_1 \ldots K_r$ 即可, 下面以一个引理的形式证明, 因为这对一般情况来说也是正确的. □

引理 5.5.7. *K/F 是有限 Galois 扩张, 其 Galois 群为 $G = G_1 \times \cdots \times G_r$, 则 $K = K_1 \ldots K_r$, 其中 $K_j = K^{H_j}, H_j = \prod_{i \neq j} G_i \times \{1\}$*

证明: 根据归纳法, 只需要证明 $r = 2$ 的情况即可: 如果 $K_1/F, K_2/F$ 都是 Galois 扩张, 则 $[K_1K_2 : K_2] = [K_1 : K_1 \cap K_2]$, 而这里 $K_1 \cap K_2 = F$, 因此 $[K_1K_2 : F] = [K_1 : F][K_2 : F] = |H_1||H_2| = |G|$, 因此 $K = F_1F_2$. □

5.6 正规基定理

定理 5.6.1 (正规基定理). *给定有限 Galois 扩张 E/F, 则存在 E/F 的一族正规基, 即存在 $\alpha \in E^\times$, 使得 $\{\sigma(\alpha) \mid \alpha \in \mathrm{Gal}(E/F)\}$ 构成了 E/F 的一族基.*

[3] exponent, 指群中所有元素阶的最小公倍数.

第六章　Galois 上同调与 Hilbert 90

6.1　范与迹

定义 6.1.1. E/F 是有限扩张, 对于 $\alpha \in E$, 其**范数** (norm)定义为 F-线性映射 $m_\alpha(x) = \alpha x$ 的行列式, 即

$$\mathrm{N}_{E/F}(\alpha) = \det(m_\alpha)$$

其**迹** (trace)定义为

$$\mathrm{Tr}_{E/F}(\alpha) = \mathrm{trace}(m_\alpha)$$

命题 6.1.2.

(1) $\mathrm{N}_{E/F}$ 是可乘的.

(2) 如果 $a \in F$, 则 $\mathrm{N}_{E/F}(a\alpha) = a^{[E:F]}\,\mathrm{N}_{E/F}(\alpha)$.

(2) $\mathrm{Tr}_{E/F}$ 是可加的.

(4) 如果 $a \in F$, 则 $\mathrm{Tr}_{E/F}(a\alpha) = a\,\mathrm{Tr}_{E/F}(\alpha)$.

(5) 如果 $\alpha \in F$, 则

$$\mathrm{N}_{E/F}(\alpha) = \alpha^{[E:F]}$$
$$\mathrm{Tr}_{E/F}(\alpha) = [E:F]\alpha$$

证明: 线性代数. □

引理 6.1.3. 如果 $F \subseteq E \subseteq K, \alpha \in E$, 则

$$\mathrm{N}_{K/F}(\alpha) = \mathrm{N}_{E/F}(\alpha)^{[K:E]}$$
$$\mathrm{Tr}_{K/F}(\alpha) = [K:E]\,\mathrm{Tr}_{E/F}(\alpha)$$

证明: 假设 $\{x_1, \ldots, x_n\}$ 是 E/F 的一组基, $\{y_1, \ldots, y_n\}$ 是 K/E 的一组基, 那么根据线性代数的结果 $\{x_i y_j\}$ 是 K/F 的一组基. 如果 $A \in M_{n\times n}(F)$ 是 m_α 在 E/F 上对应的矩阵, 即

$$\alpha \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

那么则有

$$\alpha\begin{pmatrix} x_1y_1 \\ x_2y_1 \\ \vdots \\ x_ny_1 \\ x_1y_2 \\ \vdots \\ x_ny_2 \\ \vdots \\ x_ny_m \end{pmatrix} = \begin{pmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{pmatrix}\begin{pmatrix} x_1y_1 \\ x_2y_1 \\ \vdots \\ x_ny_1 \\ x_1y_2 \\ \vdots \\ x_ny_2 \\ \vdots \\ x_ny_m \end{pmatrix}$$

从而有 $\mathrm{N}_{K/F}(\alpha) = \det(A)^m = N_{E/F}(\alpha)^{[K:E]}$ 以及 $\mathrm{Tr}_{K/F}(\alpha) = m\,\mathrm{Tr}_{E/F}(\alpha) = [K:E]\,\mathrm{Tr}_{E/F}(\alpha)$. □

注记. 实际上, 上述引理是如下传递性的特殊情况.

$$\mathrm{N}_{K/F} = \mathrm{N}_{K/E} \circ \mathrm{N}_{E/F}$$
$$\mathrm{Tr}_{K/F} = \mathrm{Tr}_{K/E} \circ \mathrm{Tr}_{E/F}$$

引理 6.1.4. *给定 $E = F(\alpha)$, 如果 $P_{\alpha,F}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, 则*

$$\mathrm{N}_{E/F}(\alpha) = (-1)^n a_0$$
$$\mathrm{Tr}_{E/F}(\alpha) = -a_{n-1}$$

证明: 选取基 $\{1, \alpha, \ldots, \alpha^{n-1}\}$ 即可. □

命题 6.1.5. *如果 E/F 是有限扩张, 任取 $\alpha \in K$, 则*

$$\mathrm{N}_{E/F}(\alpha) = \prod_{\sigma\in\mathrm{Hom}_F(E,\bar{F})} \sigma(\alpha)^{[E:F]_i}$$
$$\mathrm{Tr}_{E/F}(\alpha) = [E:F]_i \sum_{\sigma\in\mathrm{Hom}_F(E,\bar{F})} \sigma(\alpha)$$

其中 $[K:F]_i$ 为扩张的纯不可分次数[1].

证明: 下面只对范数证明, 迹的证明是类似的: 任取 $\alpha \in E$, 考虑域扩张 $F \subseteq F(\alpha) \subseteq E$, 根据引理6.1.3有:

$$\mathrm{N}_{E/F}(\alpha) = \mathrm{N}_{F(\alpha)/F}(\alpha)^{[E:F(\alpha)]}$$

而考虑满射:

$$\mathrm{Hom}_F(E, \bar{F}) \twoheadrightarrow \mathrm{Hom}_F(F(\alpha), \bar{F})$$

其每个纤维都包含 $[E:F(\alpha)]$ 个元素: 这是因为 $\mathrm{Hom}_F(E,\bar{F}) = \mathrm{Hom}_F(E_s,\bar{F})$ 中恰有 $[E:F]_s$ 个元素, $\mathrm{Hom}_F(F(\alpha),\bar{F}) = \mathrm{Hom}_F(F(\alpha)_s,\bar{F})$ 中恰有 $[F(\alpha):F]_s$ 个元素. 因此:

$$\Big(\prod_{\sigma\in\mathrm{Hom}_F(K,\bar{F})} \sigma(\alpha)\Big)^{[K:F]_i} = \prod_{\mathrm{Hom}_F(F(\alpha),\bar{F})} \sigma(\alpha)^{[K:F(\alpha)]_s[K:F]_i}$$

[1] 见定义3.3.6.

由于 $[K:F(\alpha)]=[K:F(\alpha)]_i[K:F(\alpha)]_s$, 因此只需要证明:

$$N_{F(\alpha)/F}(\alpha)=\prod_{\mathrm{Hom}_F(F(\alpha),\bar{F})}\sigma(\alpha)^{[F(\alpha):F]_i}$$

即单扩张的情形, 而根据引理6.1.4直接可以得到想要的结果. □

推论 6.1.6. *E/F 是有限扩张, 则 E/F 可分当且仅当 $\mathrm{Tr}_{E/F}$ 是满射, 这也当且仅当 $\mathrm{Tr}_{E/F}$ 是非零映射.*

证明: 根据线性代数的知识, $\mathrm{Tr}_{E/F}$ 非零当且仅当其为满射是显然的. 如果 E/F 不可分, 假设 $\mathrm{char}\,F=p$, 则根据命题6.1.5可知 $\mathrm{Tr}_{E/F}(\alpha)$ 中含有 $[K:F]_i$ 作为因子, 然而其为 p 的幂次, 因此 $\mathrm{Tr}_{E/F}(\alpha)$ 恒为零映射. 另一方面, 如果 E/F 是可分的, 需要证明 $Tr_{E/F}$ 不是零映射, 这只需要寻找 α 使得:

$$\sum_{\sigma\in\mathrm{Hom}_F(E,\bar{F})}\sigma(\alpha)\neq 0$$

□

命题 6.1.7. *E/F 是有限域上的有限扩张, 则 $\mathrm{N}_{E/F},\mathrm{Tr}_{E/F}$ 都是满射.*

证明: 不妨记 $E=\mathbb{F}_{q^d},F=\mathbb{F}_q$. 根据推论6.1.6可知 $\mathrm{Tr}_{E/F}$ 是满射, 因为有限域上的扩张都是可分的. 另一方面, 注意到 $\mathrm{N}_{E/F}$ 是可乘的, 并且 $E^\times$ 是循环群, 因此我们只需要考虑 $\mathrm{N}_{E/F}$ 在 x 上的取值即可:

$$\mathrm{N}_{E/F}(x)=\prod_{\sigma\in\mathrm{Gal}(E/F)}\sigma(x)=x\cdot x^q\cdot\dots\cdot x^{q^{d-1}}=x^{\frac{q^d-1}{q-1}}:=a\in\mathbb{F}_q^\times$$

并且 a 的阶为 $q-1$, 而注意到 $\mathbb{F}_q^\times$ 是一个 $q-1$ 阶循环群, 因此 a 是其一个生成元, 因此 $\mathrm{N}_{K/F}$ 也是满射. □

注记. Hilbert90 问题断言: 如果 $\mathrm{Gal}(E/F)=\langle\sigma\rangle$ 是一个循环群, $\alpha\in E$ 满足其范数为 1, 则 $\alpha=\dfrac{\sigma(\beta)}{\beta}$, 对于某个 $\beta\in E^\times$ 成立. 对于有限域来说, 这个命题的答案可以显式的构造出来: 不妨沿用命题6.1.7中的记号, 如果 $\alpha=x^k$ 满足范数为 1, 则由于可乘性:

$$\mathrm{N}_{E/F}(\alpha)=\mathrm{N}_{E/F}(x)^k=a^k=1$$

因此 $q-1\mid k$, 不妨记作 $k=(q-1)r$, 则

$$\alpha=x^{(q-1)r}=\frac{x^{qr}}{x^r}=\frac{\sigma(x^r)}{x^r}$$

6.2 Galois 上同调

定义 6.2.1. G 是一个有限群, 一个 G-**模** (module)是指一个阿贝尔群 A 以及一个 G 作用 $\mu\colon G\times A\to A$ 满足:

(1) $1\cdot a=a$

(2) $gg'\cdot a=g\cdot(g'\cdot a)$

(3) $g\cdot(a+a')=g\cdot a+g\cdot a'$

并且 G-模之间的**态射** (morphism)为是满足 $f(ga)=gf(a), g\in G, a\in A$ 的群同态.

注记. 模论中的结果告诉我们阿贝尔群可以与 $\mathbb{Z}$ 模等同起来, 则上述定义的 G-模可以与 $\mathbb{Z}[G]$ 模等同起来, 其中 $\mathbb{Z}[G]=\{\sum_{g\in G}a_g g\mid a_g\in\mathbb{Z}\}$ 是 G 的群代数,

注记. 在上述定义中我们为了叙述方便假设 G 是乘法群, A 是加法群, 但这并不关键. 之后可能会根据情况需要而调整, 请读者留心.

例子. *给定有限 Galois 扩张 E/F, 令 $G=\mathrm{Gal}(E/F)$, 则 $G\curvearrowright(E,+), G\curvearrowright(E^\times,\times)$ 都是 G-模.*

定义 6.2.2. 给定有限群 G 和群 A, 定义

$$C^n(G,A)=\begin{cases}A & n=0\\ \{f\colon G^n\to A\} & n\geq 1\end{cases}$$

并且定义 $\mathrm{d}^n\colon C^n(G,A)\to C^{n+1}(G,A)$ 如下:

$$\begin{cases}\mathrm{d}^0a(g)=ga-a\\ \mathrm{d}^nf(g_1,\dots,g_{n+1})=g_1f(g_2,\dots,g_{n+1})+\sum_{i=1}^n(-1)^if(g_1,\dots,g_ig_{i+1},\dots,g_{n+1})+(-1)^{n+1}f(g_1,\dots,g_n)\end{cases}$$

可以验证, (C,d) 构成了一个链复形, 因此定义**群的上同调** (group cohomology)[2]为:

$$H^n(G,A)=\frac{\ker\mathrm{d}^n}{\mathrm{im}\,\mathrm{d}^{n-1}}$$

例子. *当 $n=0$ 时, $H^0(G,A)=\ker\mathrm{d}^0$. 若 $a\in\ker\mathrm{d}^0$, 当且仅当对任意的 $g\in G$, 有 $ga-a=0$, 当且仅当 $a\in A^G$, 即:*

$$H^0(G,A)=A^G$$

这实际上与一般的导出函子是一致的, 零阶导出函子就是其自身.

例子. *当 $n=1$ 时:*

$$\mathrm{d}^1f(g_1,g_2)=g_1f(g_2)-f(g_1g_2)+f(g_2)$$

因此:

$$\ker\mathrm{d}^1=\{f\colon G\to A\mid f(g_1g_2)=f(g_1)+g_1f(g_2)\}$$

*满足上述条件的函数也被称为***交错同态** *(crossed homomorphism). 特别地, 当 A 是一个平凡 G-模时, 一个交错同态就是群同态. 而*

$$\mathrm{im}\,\mathrm{d}^0=\{f\colon G\to A\mid \text{存在 } a\in A \text{ 使得} f(g)=ga-a\}$$

注记. 如果 $f\colon G\to A$ 是一个交错同态, 则有下面的观察:

(1)

$$f(1)=f(1)+1\cdot f(1)=2f(1)\implies f(1)=0$$

即 f 将 G 中的单位元映成 A 中的单位元.

[2]在同调代数中, 函子 $A\to A^G=\{a\in A\mid ga=a\}$ 是左正合函子, 则 $H^n(G,A)$ 被定义为这个函子的右导出函子.

(2)

$$f(g^2) = f(g) + g \cdot f(g) = (1+g) \cdot f(g)$$

归纳地可以得到:

$$f(g^n) = (1 + g + \cdots + g^{n-1}) f(g)$$

假设 G 是一个 n 阶循环群, 生成元为 g, 则

$$0 = f(1) = f(g^n) = (1 + g + \cdots + g^{n-1}) f(g)$$

反之, 如果 $x \in A$ 满足 $(1+g+\cdots+g^{n-1})x = 0$, 则 $f(g) := x$ 定义了交错同态 $f\colon G \to A$.

定理 6.2.3 (Hilbert 90). *给定有限 Galois 扩张 E/F, 则*

$$H^1(\mathrm{Gal}(E/F), E^\times) = 1$$
$$H^1(\mathrm{Gal}(E/F), E^+) = 0$$

前者称为乘法版本, 后者称为加法版本.

证明: 我们先来证明乘法版本: 令 $f\colon G \to E^\times$ 是交错同态, 那么任取 $\tau \in G, f(\tau) \neq 0$, 根据引理4.1.7可知 $\sum_{\tau \in G} f(\tau)\tau$ 是非零的, 即存在 $a \in E^\times$ 使得

$$\beta = \sum_{\tau \in G} f(\tau)\tau(a) \neq 0$$

因此

$$\begin{aligned} \sigma(\beta) &= \sum_{\tau \in G} \sigma f(\tau)(\sigma\tau)(\gamma) \\ &= \sum_{\tau \in G} f^{-1}(\sigma) f(\sigma\tau)(\sigma\tau)(\gamma) \\ &= f^{-1}(\sigma)\beta \end{aligned}$$

即 $f(\sigma) = \beta/\sigma(\beta)$. 令 $x = \beta^{=1}$, 则 $f(\sigma) = \sigma(x)/x$, 即任何交错同态都落在 $\mathrm{im}\,\mathrm{d}^0$ 中, 即上同调群平凡.

现在来证明加法版本: 令 $f\colon G \to E$ 是交错同态, 不妨假设 $f \not\equiv 0$, 那么任取 $\tau \in G, f(\tau)$ 不全为零, 同样根据 Dedekind 无关引理4.1.7有 $a \in E$ 使得

$$\beta = \sum_{\tau \in G} f(\tau)\tau(a) \neq 0$$

另外, 我们取 $b \in E^\times$ 满足 $\mathrm{Tr}_{E/F}(b) \neq 0$, 并且根据推论6.1.6, 这样的 b 是存在的. 令 $\mu = \sum_{\tau \in G} f(\tau)\tau$, 如果 $\mu(a+b) = 0$, 那么 $\mu(b) = -\mu(a) \neq 0$; 如果 $\mathrm{Tr}_{E/F}(a+b) = 0$, 那么 $\mathrm{Tr}_{E/F}(a) \neq 0$; 如果 $\mu(a+b) \neq 0$ 并且 $\mathrm{Tr}_{E/F}(a+b) \neq 0$, 那么我们用 $\mu(a+b)$ 代替 β. 如上分

析说明我们总可以找到 $a \in E^{\times}, \mu(a) \neq 0$ 并且 $\mathrm{Tr}_{E/F}(a) \neq 0$, 令 $\beta = \mu(a)$, 那么

$$\begin{aligned}\sigma(\beta) &= \sum_{\tau \in G} \sigma(f(\tau)\tau(a)) \\ &= \sum_{\tau \in G} \sigma(f(\tau))\sigma\tau(a) \\ &= \sum_{\tau \in G} (f(\sigma\tau) - f(\sigma))\sigma\tau(a) \\ &= \beta - f(\sigma) \sum_{\tau \in G} \sigma\tau(a) \\ &= \beta - f(\sigma)\,\mathrm{Tr}_{E/F}(a)\end{aligned}$$

则 $f(\sigma) = \mathrm{Tr}_{E/F}(a)^{-1}(\beta - \sigma(\beta))$, 取 $x = \dfrac{-\beta}{\mathrm{Tr}_{E/F}(a)}$, 则有 $f(\sigma) = \sigma(x) - x$. □

定理 6.2.4 (Hilbert 90)**.** *给定有限 Galois 扩张 E/F, 并且 $G = \mathrm{Gal}(E/F) = \langle \sigma \rangle$ 是 n 阶循环群, 则*

(1) *如果 $\alpha \in E^{\times}$ 满足范数为 1, 则 $\alpha = \dfrac{\sigma(\beta)}{\beta}, \beta \in E^{\times}$.*
(2) *如果 $\alpha \in E$ 满足迹为 0, 则 $\alpha = \sigma(\beta) - \beta, \beta \in E$.*

证明: 由于 (1) 和 (2) 的证明几乎完全一致, 在这里我们给出 (2) 的证明: 如果 $\alpha \in E$ 满足迹为零, 则

$$0 = \mathrm{Tr}_{K/F}(\alpha) = \sum_{\tau \in G} \tau\alpha = \sum_{i=0}^{n-1} \sigma^i \alpha$$

考虑 $f \colon G \to K$, 定义为 $\sigma^i \mapsto (1 + \sigma + \cdots + \sigma^{i-1})x$, 可以直接验证[3]其为一个是一个交错同态. 根据定理6.2.3可知存在 $\beta \in E$ 使得 $f(\sigma^k) = \sigma^k(\beta) - \beta$ 对任意的 $0 \leq k \leq n-1$ 成立. 特别地, $\alpha = f(\sigma) = \sigma(\beta) - \beta$. □

推论 6.2.5. *令 $a, b \in \mathbb{Q}$, 满足 $a^2 + b^2 = 1$, 则存在 $c, d \in \mathbb{Z}$ 使得*

$$a = \frac{c^2 - d^2}{c^2 - d^2}, \quad b = \frac{-2cd}{c^2 + d^2}$$

证明: 考虑 $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$, 取 $a + b\sqrt{-1} \in \mathbb{Q}(\sqrt{-1})$ 满足范数为 1, 则存在 $c + d\sqrt{-1}$ 使得:

$$a + b\sqrt{-1} = \frac{c - d\sqrt{-1}}{c + d\sqrt{-1}}$$

实部虚部对应即可. □

[3]这里用到了 α 的迹为零这个条件.

第二部分

交换代数

第七章　交换代数的若干背景

7.1　代数数论与交换代数

代数数论给出了一类相当重要的交换环, 即代数整数环, 这已经在之前的课程中被提及. 例如给定无平方因子的整数 d, 虚二次数域 $K=\mathbb{Q}(\sqrt{d})$ 的代数整数环 $\mathcal{O}_K$ 为

$$\mathcal{O}_K=\begin{cases}\mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d\equiv 1 \pmod 4\\ \mathbb{Z}[\sqrt{d}] & d\equiv 2,3 \pmod 4\end{cases}$$

并且我们通过引入理想类群来研究了虚二次数域代数整数环的唯一分解性. 实际上, 某些交换环是否具有唯一分解性是代数数论非常关心的问题, 这实际上源于 Fermat 大定理 (Fermat's last theorem).

Fermat 大定理的表述是: 对于任意大于 2 的自然数 n, 方程 $x^n+y^n=z^n$ 没有正整数解. 这个问题在 17 世纪由法国数学家 Fermat 提出, 因为没有给出完整证明而备受关注. Fermat 大定理的研究过程给代数数论的发展带来了蓬勃生机, 19 世纪的法国数学家 Gabriel Lamé 将 Fermat 大定理转化为研究方程 $x^n+y^n=z^n$ 的唯一分解性. Lamé 的研究表明, 如果对于一个奇素数 p, 方程 $x^n+y^n=z^n$ 满足 $x^n+y^n=z^n \pmod p$ 的整数解 (x,y,z) 只有有限个, 那么方程 $x^n+y^n=z^n$ 就不存在正整数解.

如果 $\mathbb{Z}[\xi_n]$ 是唯一分解整环, Lamé 便可以解决 Fermat 大定理. 但 Kummer 指出 $\mathbb{Z}[\xi_n]$ 在 $n=23$ 时就不是唯一分解整环, 这宣布了 Lamé 证明的失败. 但这给了 Kummer 很大的启发, 他提出了所谓理想数的概念以及考虑其对应的唯一分解, 并用此对证明了一些特殊情形的 Fermat 大定理.

7.2　代数几何与交换代数

代数几何主要关心的对象是一些代数闭域 k 上多项式 $f_1,\dots,f_r\in k[x_1,\dots,x_n]$ 的公共零点组成的集合, 而 Hilbert 的零点定理则是给出代数和几何之间的深刻联系.

定理 7.2.1 (Nullstellensatz)**.** $\mathbb{C}[x_1,\dots,x_n]$ 的极大理想与 $\mathbb{C}^n$ 中的点一一对应.

推论 7.2.2. 令 I 是 $\mathbb{C}[x_1,\dots,x_n]$ 中一些多项式 $f_1,\dots,f_r$ 生成的理想, $R=\mathbb{C}[x_1,\dots,x_n]/I$. 令 V 是 $f_1,\dots,f_r$ 公共零点组成的集合, 那么 R 的极大理想和 V 中的点有一一对应.

7.3 Hilbert 与不变量理论

7.3.1 不变量理论

在本节中 k 总是指特征零的代数闭域.

定义 7.3.1. 给定环 R, 一个 R-**代数** (algebra)是一个环 A 以及环同态 $\varphi\colon R \to A$.

定义 7.3.2. 给定环 R, R-代数 A 称为**有限生成** R-**代数** (finitely generated algebra), 如果存在满的环同态 $R[x_1,\dots,x_n] \to A$.

给定群 G 作用在环 R 上, 用 R^G 来表示在群作用下不变的元素, 不变量理论关心的则是 R^G 的性质, 即是否有限生成? 以及如果是有限生成, 那么生成元之间的关系如何?

例子. 根据对称多项式基本定理有 $k[x_1,\dots,x_n]^{S_n} \cong k[s_1,\dots,s_n]$, 其中 $s_1,\dots,s_n$ 是初等对称多项式. 特别地, $k[x_1,\dots,x_n]^{S_n}$ 是有限生成 k-代数.

例子. 令 $G = \mathbb{Z}/2\mathbb{Z}$, 考虑 G 通过 $(-1)\cdot(x_1,x_2) = (-x_1,-x_2)$ 作用在 k^2 上, 这给出了一个 G 在 $k[x_1,x_2]$ 上的作用, 并且 $k[x_1,x_2]^G \cong k[x,y,z]/(y^2-xz)$. 根据 *Hilbert* 零点定理可知 $k[x,y,z]/(y^2-xz)$ 的极大理想一一对应于 $V = \{(x,y,z)\in k^3 \mid y^2 = xz\}$ 中的点. 考虑如下映射

$$\begin{aligned}\varphi\colon k^2 &\to V\\ (x_1,x_2) &\mapsto (x_1^2, x_1x_2, x_2^2)\end{aligned}$$

不难发现 φ 是一个 $2:1$ 的映射, 并且有如下的交换图

$$\begin{tikzcd} k^2 \arrow[rr, "\varphi"] \arrow[dr] & & V \\ & k^2/G \arrow[ur] & \end{tikzcd}$$

其中 k^2/G 是 k^2 在群 G 作用下的轨道空间, 并且 $k^2 \to k^2/G$ 也是 $2:1$ 的, 从而 $k^2/G \cong V$.

注记. 这个例子实际上反映了不变量理论的重要性: k^2 在群 G 作用下的轨道空间可以由环 $k[x_1,x_2]^G$ 对应的代数簇给出, 即代数上的不变量给出了几何上的商结构[1].

定理 7.3.3 (Hilbert)**.** 如果 $G \subseteq \mathrm{GL}(n,k)$ 是有限群, 则 $S = k[x_1,\dots,x_n]^G$ 是有限生成 k-代数.

为了证明上述的结果, 我们先来探究一下 $S \subseteq R = k[x_1,\dots,x_n]$ 作为子环的性质.

定义 7.3.4. 环 R 被称为一个 $\mathbb{Z}$-**分次环** ($\mathbb{Z}$-graded ring), 如果 $R = \bigoplus_{i\in\mathbb{Z}} R_i$, 并且 $R_iR_j \subseteq R_{i+j}$, 其中 R_i 是 R 的阿贝尔子群.

定义 7.3.5. 给定 $\mathbb{Z}$-分次环 R, 理想 $I \subseteq R$ 被称为**齐次理想** (homogenous ideal), 如果其由一些齐次的元素生成.

命题 7.3.6. 给定 $\mathbb{Z}$-分次环 $R = \bigoplus_{i\in\mathbb{Z}} R_i$, 如下叙述等价.

1. $I \subseteq R$ 是齐次理想.

[1]感兴趣的读者可以阅读一些几何不变量理论.

2. $I = \bigoplus_{i\in\mathbb{Z}} I_i$, 其中 $I_i = I \cap R_i$.

命题 7.3.7. 如果 $G \subseteq \mathrm{GL}(n,k)$, 则 $S = k[x_1,\dots,x_n]^G$ 是分次环.

证明: 首先 $R = k[x_1,\dots,x_n]$ 是 $\mathbb{Z}$-分次环, 其分次由多项式次数给出, 即 $R = \bigoplus_{i\in\mathbb{Z}_{\geq 0}} R_i$. 假设 $f \in S$, 假设 $f = f_1 + \cdots + f_d$, 其中 f_i 是 f 的 i 次齐次部分, 则 $g \cdot f = f$ 意味着 $g \cdot f_i = f_i$, 从而

$$S = \bigoplus_{i\in\mathbb{Z}_{\geq 0}} S \cap R_i$$

即 S 是一个分次环. □

命题 7.3.8. 如下正合列分裂

$$0 \to S \xrightarrow{\iota} R$$

证明: 定义

$$\begin{aligned} p\colon R &\to S \\ f &\mapsto \frac{1}{|G|}\sum_{g\in G} g \cdot f \end{aligned}$$

显然 $p \circ \iota = \mathrm{id}$. □

推论 7.3.9. S 作为 S-模是 R 的直和项, 即有作为 S-模的分解 $R = S \oplus T$, 其中 $T \subseteq$ 是 S-模.

现在我们来证明定理7.3.3.

定理7.3.3的证明. 假设 I 是 R 中由 S 中次数大于等于 1 的齐次元生成的齐次理想. 根据 Hilbert 基定理可知 R 是诺特环, 从而 I 是有限生成的, 不妨假设其由齐次元 $f_1,\dots,f_m$ 生成. 下面我们断言 $S = k[f_1,\dots,f_m]$. 由于 S 上具有 $\mathbb{Z}$-分次环结构 $S = \bigoplus_{i\in\mathbb{Z}_{\geq 0}} S_i$, 因此只需要对任意的 $N \in \mathbb{Z}_{\geq 0}$ 证明 $f \in S_N$ 可以由 $f_1,\dots,f_m$ 生成即可. 我们对 N 做归纳: 当 $N = 0$ 时是显然的, 现在假设 $S_i \subseteq k[f_1,\dots,f_m]$ 对任意的 $i \leq N-1$ 都成立, 任取 $f \in S_N$, 根据 $f \in I$ 可知

$$f = \sum_{j=1}^m G_j f_j$$

其中 $G_j \in R$. 注意到 f 是齐次元, 从而 G_j 可以被写成若干个齐次元的求和, 因此上述等式可以重写为

$$f = \sum_{j=1}^m g_i f_j$$

其中 $g_i \in R$ 都是齐次元. 注意到

$$f = p(f) = \sum_{j=1}^m p(g_i)p(f_i) = \sum_{j=1}^m p(g_i) f_i$$

而 $p(g_i)$ 是次数严格小于 f 的 S 中的齐次元, 从而根据归纳假设即可. □

7.3.2 Hilbert 多项式与维数

定义 7.3.10. 给定 $\mathbb{Z}$-分次环 $R=\bigoplus_{i\in\mathbb{Z}}R_i$, R-模 M 被称为是**分次模** (graded module), 如果 M 作为阿贝尔群有分解 $M=\bigoplus_{i\in\mathbb{Z}}M_i$, 并且满足 $R_iM_j\subseteq M_{i+j}$.

注记. 给定 $\mathbb{Z}$-分次环 $R=\bigoplus_{i\in\mathbb{Z}}R_i$ 以及分次 R-模 $M=\bigoplus_{i\in\mathbb{Z}}M_i$, 任何 M_i 都可以视作是 R_0-模, 因为 $R_0M_i\subseteq M_i$.

例子. *给定 $\mathbb{Z}$-分次环 R 和齐次理想 $I\subseteq R$, 则 R/I 是分次 R-模.*

如无特殊说明, 在本节的余下内容中我们总假设 R 是多项式环 $k[x_1,\dots,x_r]$, 其中 k 是特征零的代数闭域.

定义 7.3.11. 有限生成 R-分次模 $M=\bigoplus_{d\in\mathbb{Z}_{\geq 0}}M_d$ 的 **Hilbert 函数** (Hilbert function)定义为

$$\begin{aligned} H_M\colon \mathbb{Z}&\to\mathbb{Z}\\ s&\mapsto \dim_k M_s\end{aligned}$$

并且 M 的 **Hilbert 级数** (Hilbert series)定义为

$$HS_M(t)=\sum_{s=0}^{\infty}H_M(s)t^s$$

定理 7.3.12 (Hilbert)**.** *对于有限生成分次 R-模 M, $H_M(s)$ 在 s 足够大的时候与一个次数不超过 $r-1$ 的多项式 $P_M(s)$ 相同, $P_M(s)$ 也被称为* ***Hilbert 多项式*** *(Hilbert polynomial)*

第八章　谱与 Zariski 拓扑

8.1　点集拓扑回顾

定义 8.1.1. 集合 X 上的一个**拓扑** (topology)是 X 的一个子集族 $\mathcal{T}$, 它满足下列条件:
(1) $\varnothing$ 和 X 在 $\mathcal{T}$ 中,
(2) $\mathcal{T}$ 的任意子族的元素的并在其中,
(3) $\mathcal{T}$ 的任意有限子族的元素的交在其中,
二元组 $(X, \mathcal{T})$ 被称为一个**拓扑空间** (topological space), $\mathcal{T}$ 中的元素称为**开集** (open set).

例子. 全体开区间 $\{(a,b) \mid a,b \in \mathbb{R}\}$ 给出了 $\mathbb{R}$ 上的一个拓扑.

例子. 对于集合 X, X 的所有子集的族是 X 的一个拓扑, 称为**离散拓扑** *(discrete topology)*.

例子. 仅由 X 和 $\varnothing$ 组成的族也是 X 的一个拓扑, 称为**平凡拓扑** *(trivial topology)*.

命题 8.1.2. 给定集合 X, $\mathcal{T}_f$ 是使得 $X - U$ 是有限集或者等于 X 的那些子集 U 组成的全体, 那么 $\mathcal{T}_f$ 是一个拓扑, 被称为**余有限拓扑** *(finite complement topology)*.

证明: 首先显然 X 和 $\varnothing$ 都在其中, 因为空集是一个有限集, 它的补集是 X. 而后两条性质的验证关键在于集合的运算: 考虑 $\{U_\alpha\}$ 是 $\mathcal{T}_f$ 中的一族元素, 验证他们的并也在其中, 考虑:

$$X - \bigcup U_\alpha = \bigcap (X - U_\alpha)$$

显然有限集的交集也是有限集. 而另一方面, 若验证有限交也在其中, 则考虑:

$$X - \bigcap_{i=1}^{n} U_i = \bigcup_{i=1}^{n} (X - U_i)$$

□

定义 8.1.3. 给定拓扑空间 $(X, \mathcal{T})$, 若 $Y \subseteq X$, 则族 $\mathcal{T}_Y = \{Y \cap U \mid U \in \mathcal{T}\}$ 是 Y 的一个拓扑, 称为**子空间拓扑** (subspace topology).

定义 8.1.4. 设 X 是一个拓扑空间, A 是一个集合, $p\colon X \to A$ 是满射, 则 p 可以如下给出 A 上一个拓扑 $\mathcal{T}$: U 是 A 的开集当且仅当 $p^{-1}(U)$ 是 X 的开集. $\mathcal{T}$ 称为由 p 导出的**商拓扑** (quotient topology), 当 A 带有商拓扑时, p 被称为**商映射** (quotient map).

定义 8.1.5. 拓扑空间 X 被称为**紧的** (compact), 如果 X 的任何开覆盖存在有限子覆盖.

定义 8.1.6. 拓扑空间 X 称为**豪斯多夫的** (Hausdorff)的, 如果任取 $x, y \in X$, 存在开集 U_x, U_y 使得 $x \in U_x, y \in U_y$ 以及 $U_x \cap U_y = \varnothing$.

引理 8.1.7 (Urysohn's lemma)**.** *假设 X 是紧, Hausdorff 拓扑空间, 则 X 的任何两个闭集都可以被连续函数分离. 特别地, 任何两个点都能被连续函数分离.*

定义 8.1.8. 拓扑空间之间的映射 $f \colon X \to Y$ 被称为**连续的** (continous), 如果 Y 中的开集在 f 下的原像是 X 中的开集.

定义 8.1.9. 两个拓扑空间 X, Y 被称为**同胚的** (homeomorphic), 如果两者间存在连续的双射, 使得其逆映射也连续.

定义 8.1.10. 拓扑空间之间的映射 $f \colon X \to Y$ 被称为**开映射** (open map), 如果对于 X 的每一个开集 U, $f(U)$ 都是 Y 的开集.

定义 8.1.11. 拓扑空间之间的映射 $f \colon X \to Y$ 被称为**闭映射** (closed map), 如果对于 X 的每一个闭集 V, $f(V)$ 都是 Y 的闭集.

8.2 环的素谱与极大谱

定义 8.2.1. 环 R 的极大理想的全体组成的集合称为 R 的**极大谱** (maximal spectral), 记做 $\operatorname{mSpec} R$.

定义 8.2.2. 环 R 的素理想的全体组成的集合称为 R 的**素谱** (prime spectral), 记做 $\operatorname{Spec} R$.

命题 8.2.3. *给定环 R, 任取理想 $I \subseteq R$, 定义 $V(I) = \{\mathfrak{p} \in \operatorname{Spec} R \mid I \subseteq \mathfrak{p}\}$. 所有形如 $V(I)$ 的集合全体给出了 $\operatorname{Spec} R$ 上的所有闭集, 称为* ***Zariski 拓扑*** *(Zariski topology).*

证明: 注意到

$$\begin{aligned} V((0)) &= \operatorname{Spec} R \\ V((1)) &= \varnothing \\ V(I) \cap V(J) &= V(IJ) \\ \bigcup_{k \in K} V(I_k) &= V(\sum_{k \in K} I_k) \end{aligned}$$

□

注记. 给定环 R, $\operatorname{mSpec} R$ 上的 Zariski 拓扑由 $\operatorname{mSpec} R \subseteq \operatorname{Spec} R$ 作为子空间的子空间拓扑给出.

推论 8.2.4. *给定环 R, 如下的集族*

$$\mathcal{T} = \{U_f = \{\mathfrak{p} \in \operatorname{Spec} R \mid f \notin \mathfrak{p}\}\}_{f \in R}$$

是 $\operatorname{Spec} R$ 上 Zariski 拓扑的拓扑基.

证明: 任取 $\operatorname{Spec} R$ 中的开集 $U = (V(I))^c$, 则

$$\bigcup_{f\in I} U_f = \bigcup_{f\in I} (V(f))^c = (\bigcap_{f\in I} V(f))^c = (V(I))^c$$

$\square$

推论 8.2.5. *给定环 R, 如下的集族*

$$\mathcal{T} = \{U_f = \{\mathfrak{m} \in \operatorname{mSpec} R \mid f \notin \mathfrak{m}\}\}_{f\in R}$$

是 $\operatorname{mSpec} R$ 上 Zariski 拓扑的拓扑基.

8.2.1 连续函数环的极大谱

给定拓扑空间 X, 用 $C(X)$ 表示 X 到 $\mathbb{R}$ 的连续函数全体, 其上存在一个环结构. 下面的定理反映了极大谱的一个重要特性.

定理 8.2.6. *给定紧, Hausdorff 拓扑空间 X, $\operatorname{mSpec} C(X)$ 与 X 之间存在集合上的一一对应.*

证明: 任取 $x \in X$, 考虑如下赋值映射

$$\begin{aligned} e_x\colon C(X) &\to \mathbb{R} \\ f &\mapsto f(x) \end{aligned}$$

从而 $\mathfrak{m}_x := \{f \in C(X) \mid f(x) = 0\}$ 是 $C(X)$ 的一个极大理想. 下面我们证明

$$\begin{aligned} \mu\colon X &\to \operatorname{mSpec} C(X) \\ x &\mapsto \mathfrak{m}_x \end{aligned}$$

是双射.

1. μ 是满射: 给定 $C(X)$ 的极大理想 $\mathfrak{m}$, 令

   $$V = \{x \in X \mid f(x) = 0, \forall f \in \mathfrak{m}\}$$

   我们断言 $V \neq \varnothing$, 否则对任意 $x \in X$, 存在 $f_x \in \mathfrak{m}$ 使得 $f_x(x) \neq 0$, 由于 f_x 是连续的, 从而存在 x 的一个开邻域 U_x 使得 f_x 在 U_x 恒不为零. 由于 X 是紧的, 从而有限多个 $U_{x_1}, \dots, U_{x_n}$ 覆盖 X, 令 $f = f_{x_1}^2 + \dots + f_{x_n}^2$, 从而 f 在 X 上恒不为零, 从而 f 是 $C(X)$ 中的单位, 而 $f \in \mathfrak{m}$ 与 $\mathfrak{m}$ 是极大理想矛盾, 从而 $V \neq \varnothing$. 任取 $x \in V$, 从而 $\mathfrak{m} \subseteq \mathfrak{m}_x$, 再利用 $\mathfrak{m}$ 是极大理想则有 $\mathfrak{m} = \mathfrak{m}_x$, 即 μ 是满射.
2. μ 是单射: 根据引理8.1.7, X 上的连续函数分离 X 上的点, 从而 $x \neq y$ 意味着 $\mathfrak{m}_x \neq \mathfrak{m}_y$, 从而 μ 是单射.

$\square$

定理 8.2.7. *给定紧, Hausdorff 拓扑空间 X, 则如下映射在 $\operatorname{mSpec} C(X)$ 带有 Zariski 拓扑时是同胚*

$$\begin{aligned} \mu\colon X &\to \operatorname{mSpec} C(X) \\ x &\mapsto \mathfrak{m}_x \end{aligned}$$

证明: 给定 $f\in C(X)$, 令 $\widetilde{U}_f=\{x\in X\mid f(x)\neq 0\}$, 注意到

$$f\in\widetilde{U}_f\iff f(x)\neq 0\iff f\notin\mathfrak{m}_x\iff\mathfrak{m}_x\in U_f$$

从而 $\mu(\widetilde{U}_f)=U_f$. 根据推论8.2.5, 只需证明 $\widetilde{U}_f$ 构成了 X 的一组拓扑基: 任取 $x\in X$ 以及 x 的一个开邻域 V, 根据引理8.1.7, 存在 $f\in C(X)$ 使得 $f(x)=1$ 以及 $f(V^c)=0$, 因此 $x\in\widetilde{U}_f$ □

给定拓扑空间之间的连续映射 $F\colon X\to Y$, 其可以诱导连续函数环之间的映射

$$\begin{aligned}F^*\colon C(Y)&\to C(X)\\ f&\mapsto f\circ F\end{aligned}$$

而极大谱的另一个好处在于, 通过连续函数环之间的映射可以通过极大谱来恢复出拓扑空间之间的映射: 因为任取 $C(X)$ 的极大理想 $\mathfrak{m}_x$, 有

$$\begin{aligned}(F^*)^{-1}(\mathfrak{m}_x)&=\{f\in C(Y)\mid (F^*)^{-1}(f)\in\mathfrak{m}_x\}\\ &=\{f\in C(Y)\mid f\circ F(x)=0\}\\ &=\mathfrak{m}_{F(x)}\end{aligned}$$

从而有

$$\begin{aligned}\operatorname{mSpec}C(X)&\to\operatorname{mSpec}C(Y)\\ \mathfrak{m}_x&\mapsto\mathfrak{m}_{F(x)}\end{aligned}$$

并且可以直接验证在带有 Zariski 拓扑时上述映射是连续的, 并且在将 $\operatorname{mSpec}C(X)$ 同胚地视为 X 之后, 该映射还原了 F. 但是一般来说, 环之间的同态, 并不能给出极大谱之间的映射, 这是极大谱最大的缺点, 但是在下一节我们将介绍素谱具有函子性.

例子. 考虑 $\varphi\colon\mathbb{Z}\to\mathbb{Q}$ 是嵌入给出的同态, 则 $\varphi^{-1}((0))$ 不是 $\mathbb{Z}$ 的极大理想.

8.2.2 素谱的函子性

命题 8.2.8. 给定环同态 $\varphi\colon A\to B$, 则

$$\begin{aligned}\varphi^*\colon\operatorname{Spec}B&\to\operatorname{Spec}A\\ \mathfrak{p}&\mapsto\varphi^{-1}(\mathfrak{p})\end{aligned}$$

在 *Zariski* 拓扑下是连续映射.

证明: 由于

$$\begin{aligned}U_f&=\{\mathfrak{p}\in\operatorname{Spec}A\mid f\notin\mathfrak{p}\}\\ \widetilde{U}_f&=\{\widetilde{\mathfrak{p}}\in\operatorname{Spec}B\mid f\notin\widetilde{\mathfrak{p}}\}\end{aligned}$$

分别给出了 $\operatorname{Spec}A$ 和 $\operatorname{Spec}B$ 的拓扑基, 如果我们能证明 $(\varphi^*)^{-1}(U_f)=\widetilde{U}_{\varphi(f)}$, 则 φ^* 是连续映射. 注意到

$$\mathfrak{q}\in\widetilde{U}_{\varphi(f)}\iff\varphi(f)\notin\mathfrak{q}\iff f\notin\varphi^*(\mathfrak{q})\iff\varphi^*(\mathfrak{q})\in U_f\iff\mathfrak{q}\in\varphi^{*-1}(U_f)$$

□

命题 8.2.9. 给定环 A 和理想 $\mathfrak{a} \subseteq A$, 并且 $\varphi\colon A \to A/\mathfrak{a}$ 是商映射, 则 $\varphi^*\colon \operatorname{Spec} A/\mathfrak{a} \to V(\mathfrak{a})$ 在 *Zariski* 拓扑意义下是同胚.

证明: 显然 φ^* 给出了 $\operatorname{Spec} A/\mathfrak{a}$ 和 $V(\mathfrak{a})$ 作为集合间的双射, 并且由于 $\varphi^*\colon \operatorname{Spec} A/\mathfrak{a} \to \operatorname{Spec} A$ 是连续的, 以及 $V(\mathfrak{a})$ 是闭集, 从而 $\varphi^*\colon \operatorname{Spec} A/\mathfrak{a} \to V(\mathfrak{a})$ 也是连续的. 因此我们只需要验证 φ^* 是闭映射: 任取 $\operatorname{Spec} A/\mathfrak{a}$ 中的闭集 $V(\mathfrak{b}/\mathfrak{a})$, 其中 $\mathfrak{b} \subseteq A$ 是理想, 则

$$\begin{aligned}\varphi^*(V(\mathfrak{b}/\mathfrak{a})) &= \varphi^*(\{\mathfrak{p}/\mathfrak{a} \mid \mathfrak{b} \subseteq \mathfrak{p}, \mathfrak{p} \in \operatorname{Spec} A\}) \\ &= \{\mathfrak{p} \mid \mathfrak{b} \subseteq \mathfrak{p}, \mathfrak{p} \in \operatorname{Spec} A\} \\ &= V(\mathfrak{b})\end{aligned}$$

□

例子. 给定域 k, $\operatorname{Spec} k$ 是单点集.

例子. $\operatorname{Spec} \mathbb{Z}$ 作为集合是由 (0) 和 (p) 构成的, 其中 p 是素数. 并且由于 (p) 也是 $\mathbb{Z}$ 的极大理想, 从而 $\{(p)\} = V((p))$, 即除去 $\{(0)\}$ 以外的单点集是 $\operatorname{Spec} \mathbb{Z}$ 的闭集. 任取 $\mathbb{Z}$ 的理想 (n), 假设 $n = \prod_{i=1}^s p_i^{\alpha_i}$, 其中 p_i 是素数, $\alpha_i \in \mathbb{Z}_{>0}$, 则 $V((n)) = \{(p_1), \dots, (p_s)\}$, 从而 $\operatorname{Spec} \mathbb{Z}$ 上的全体闭集是 $\varnothing, \operatorname{Spec} \mathbb{Z}$, 以及形如 $\{(p)\}$ 的单点集的有限并. 特别地, 任何非空的开集都会包含 (0), 即 $\overline{\{(0)\}} = \operatorname{Spec} \mathbb{Z}$, (0) 也被称为是一般点 *(generic point)*.

例子. $\operatorname{mSpec} \mathbb{Z}$ 作为集合是由 (p) 构成的, 其中 p 是素数, 并且其上的拓扑是余有限拓扑. 值得注意的是, $\operatorname{mSpec} \mathbb{Z}$ 和 $\operatorname{Spec} \mathbb{Z}$ 只相差了一般点.

例子. 由于 $\mathbb{C}[x]$ 是主理想整环, 因此所有的非零素理想都由不可约多项式给出, 即 $\operatorname{Spec} \mathbb{C}[x]$ 作为集合是由 (0) 和 $(x - \alpha)$ 组成, 其中 $\alpha \in \mathbb{C}$. 其拓扑的情况与 $\operatorname{Spec} \mathbb{Z}$ 类似.

例子. 由于 $\mathbb{R}[x]$ 是主理想整环, 因此所有的非零素理想都由不可约多项式给出. 注意到 $\mathbb{R}[x]$ 上的不可约多项式只有 $x - a, a \in \mathbb{R}$ 以及 $(x - \alpha)(x - \overline{\alpha}), \alpha \in \mathbb{C} \setminus \mathbb{R}$, 因此 $\operatorname{Spec} \mathbb{R}[x]$ 是 $\operatorname{Spec} \mathbb{C}[x]$ 在 $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ 作用下的轨道.

8.3 诺特拓扑空间

定义 8.3.1. 拓扑空间 X 被称为**诺特的** (noetherian), 如果其满足闭集的降链条件.

例子. 给定诺特环 R, $\operatorname{Spec} R$ 是诺特拓扑空间.

定义 8.3.2. 拓扑空间 X 被称为**不可约的** (irreducible), 如果其不能写成两个真闭子集的并, 即如果 X_1, X_2 是 X 的闭子集, 且满足 $X = X_1 \cup X_2$, 则 $X_1 = X$ 或 $X_2 = X$.

注记. 不可约拓扑空间的一个等价描述是任何两个开集都相交.

例子. $\operatorname{Spec} \mathbb{C}[x,y]/(xy)$ 不是不可约的, 因为 $\operatorname{Spec} \mathbb{C}[x,y]/(xy) = V((x)) \cup V((y))$.

命题 8.3.3. 令 X 是一个拓扑空间.

1. X 是诺特的当且仅当每一个闭集组成的族在包含关系下都有最小元.

2. X 是诺特的当且仅当 X 的每一个开集都是紧的.
3. 假设 X 是诺特的, 那么 X 的任何闭集都可以写成有限个不可约闭集的并.

证明: 留作习题. □

命题 8.3.4. 给定拓扑空间 X 以及 $x \in X$, $\overline{\{x\}}$ 带有子空间拓扑是不可约的.

证明: $\overline{\{x\}}$ 的任何两个开集都包含 x. □

命题 8.3.5. 给定环 R 以及 $\mathfrak{p} \in \operatorname{Spec} R$, 则 $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$.

证明: 根据定义可知 $\overline{\{\mathfrak{p}\}}$ 是所有包含 $\{\mathfrak{p}\}$ 的闭集的交, 即

$$\overline{\{\mathfrak{p}\}} = \bigcap_{i \in I} V(\mathfrak{a}_i)$$

其中 $\mathfrak{a}_i$ 取遍 R 所有使得 $\mathfrak{a}_i \subseteq \mathfrak{p}$ 的理想. 特别地存在某个 i 使得 $\mathfrak{a}_i = \mathfrak{p}$, 因此

$$\overline{\{\mathfrak{p}\}} = \bigcap_{i \in I} V(\mathfrak{a}_i) = V(\bigcup_{i \in I} \mathfrak{a}_i) = V(\mathfrak{p})$$

□

定理 8.3.6. 给定环 R, $\operatorname{Spec} R$ 中所有的不可约闭集都形如 $\overline{\{\mathfrak{p}\}}$, 其中 $\mathfrak{p} \in \operatorname{Spec} R$.

注记. 这个定理反映了素谱除了函子性以外的另一个特性, 即其上的拓扑可以由其本身的点所刻画.

证明: 任取 $\operatorname{Spec} R$ 的不可约闭集 $V(I)$, 不妨假设 I 是根式理想, 即 $r(I) = I$, 因为 $V(r(I)) = V(I)$, 现在我们证明 I 是素理想. 任取 $a, b \in R$ 满足 $ab \in I$, 则

$$(I + (a))(I + (b)) \subseteq I$$

从而 $V(I) \subseteq V(I + (a)) \cup V(I + (b))$. 并且 $I \subseteq I + (a)$ 意味着 $V(I) \subseteq V(I + (a))$, 同样有 $V(I) \subseteq V(I + (b))$, 因此 $V(I) \subseteq V(I + (a)) \cup V(I + (b))$. 根据不可约性我们不妨假设 $V(I) = V(I + (a))$, 下面我们证明 $a \in I$, 首先证明如下的引理.

引理 8.3.7. 给定环 R 以及理想 $I \subseteq R$, 如果 S 是乘法封闭集, 并且 $S \cap I = \varnothing$, 那么存在素理想 $\mathfrak{p} \supseteq I$ 使得 $\mathfrak{p} \cap S = \varnothing$.

引理的证明. 用 $\overline{S}$ 记 S 在 R/I 中的像, 根据假设 $\overline{0} \notin \overline{S}$, 用 $\mathcal{A}$ 记所有 R/I 与 $\overline{S}$ 不交的理想, 其上自然有包含关系给出的偏序关系, 并且每一个链都有一个极大元, 从而根据祖恩引理可知存在一个最大元 J, 现在我们只需要证明 J 是一个素理想即可. 任取 $\overline{a}_1, \overline{a}_2 \in R/I$ 使得 $\overline{a}_1\overline{a}_2 \in J$, 并且假设 $\overline{a}_1, \overline{a}_2 \notin J$, 那么根据 J 的选取从而

$$J + (\overline{a_1}) \cap \overline{S} \neq \varnothing$$
$$J + (\overline{a_2}) \cap \overline{S} \neq \varnothing$$

不妨假设 $\overline{s}_1 \in J + (\overline{a_1}) \cap \overline{S}$ 以及 $\overline{s}_1 \in J + (\overline{a_2}) \cap \overline{S}$, 那么 $\overline{s}_1\overline{s}_2 \in (J + (\overline{a_1}))(J + (\overline{a_2})) \subseteq J$, 与 J 的定义矛盾. □

假设 $a \notin I$, 考虑 $S = \{1, a, a^2, \dots\}$, 那么 $S \cap I = \varnothing$, 从而根据引理存在素理想 $\mathfrak{p}$ 使得 $\mathfrak{p} \cap S = \varnothing$, 即 $a \notin \mathfrak{p}$. 从而 $\mathfrak{p} \in V(p)$, 但是 $\mathfrak{p} \notin V(I + (a))$, 相矛盾. $\square$

例子. 根据 *Hilbert* 零点定理, $\operatorname{Spec} \mathbb{C}[x, y]$ 的极大理想都形如 $(x - \alpha, y - \beta)$, 其中 $\alpha, \beta \in \mathbb{C}$, 这构成了 $\operatorname{Spec} \mathbb{C}[x, y]$ 的所有闭点. $(f(x, y))$, 其中 $f(x, y) \in \mathbb{C}[x, y]$ 是不可约多项式以及 (0) 构成了 $\mathbb{C}[x, y]$ 中的其他元素. 现在来确定 $\operatorname{Spec} \mathbb{C}[x, y]$ 上的闭集, 由于 $\mathbb{C}[x, y]$ 是诺特的, 从而只需要确定其上的不可约闭集即可, 而根据定理*8.3.6*可知其上的不可约闭集都是形如点的闭包的样子, 因此除了闭点以外, $\operatorname{Spec} \mathbb{C}[x, y]$ 的不可约闭集还有

$$V(f(x, y)) = \{(f(x, y))\} \cup \{(x - \alpha, y - \beta) \mid f(\alpha, \beta) = 0\}$$

第九章　局部化

9.1　局部化的定义

从整数环 $\mathbb{Z}$ 构造有理数域 $\mathbb{Q}$ 的过程很容易扩展到任何整环 A, 由此得到它的分式域. 构造过程是取所有的有序对 (a,s), 其中 $a,s\in A, s\neq 0$, 并且在这个有序对上建立等价关系

$$(a,s)\sim(b,t)\iff at-bs=0$$

事实上, 分式域是使得 $A\setminus\{0\}$ 中所有元素都成为单位元的方法, 也就是可以找到它的逆元, 并且这是最经济的方式. 更一般地, 我们可以对于任何乘法封闭子集采取相同的做法.

定义 9.1.1. 令 A 是一个环, $S\subseteq A$ 被称为一个**乘法闭集** (multiplicative closed set), 如果

(1) $1\in S$.

(2) $xy\in S$, 如果 $x,y\in S$.

定义 9.1.2. 令 $f\colon A\to B$ 是一个环同态, $S\subseteq A$ 是一个乘法闭集. B 被称为 A 对于 S 的局部化, 如果

(1) 对任意的 $x\in S$, $f(x)$ 是单位.

(2) 假设 $g\colon A\to C$ 是另一个使得 $g(x)$ 对任意 $x\in S$ 是单位的环同态, 那么存在唯一的环同态 $h\colon B\to C$ 使得 $g=h\circ f$.

下面我们来给出局部化的具体构造, 这与我们之前的到分式域的操作类似. 定义 $A\times S$ 上如下的关系

$$(a,s)\sim(b,t)\iff(at-bs)u=0,\quad \text{对于某个 } u\in S$$

不难验证这是一个等价关系, 我们用 $S^{-1}A$, 或 $A[S^{-1}]$ 来记这个等价类组成的集合. 我们如下给 $S^{-1}A$ 上一个环结构

$$(a/s)+(b/t)=(at+bs)/st$$

$$(a/s)(b/t)=ab/st$$

练习. 如上运算给出了 $S^{-1}A$ 上的环结构.

我们有自然的映射 $f\colon A\to S^{-1}A$, 由于 $a\mapsto a/1$ 给出. 现在我们来证明 $S^{-1}A$ 满足局部化定义中的两条性质.

(1) 对于任意的 $s\in S$, 我们有 $f(s)=s/1$, 逆元为 $1/s$, 因为 $(s/1)(1/s)=s/s\sim 1/1$.

(2) 对于任意的 $g\colon A\to C$, 满足 $g(x)$ 是 C 的可逆元, S 中的任意 x 都成立, 我们定义 $h(a/s)=g(a)g(s)^{-1}$.

(a) 它是良定的: 如果 $a/s = b/t$, 那么存在 $u \in S$, 使得 $(at - bs)u = 0$, 于是 $g((at - bs)u) = g(at-bs)g(u) = 0$, 但 $g(u)$ 是可逆元, 因此 $g(a)g(t) = g(b)g(s)$, 即 $g(a)g(s)^{-1} = g(b)g^{-1}(t)$.

(b) 它是唯一的, 因为 $h \circ f = g$, 对于所有的 $a \in A$, 我们有 $h(a/1) = h \circ f(a) = g(a)$; 因此如果 $s \in S$, 那么我们有 $h(1/s) = h(s/1)^{-1} = g(s)^{-1}$, 因此 $h(a/s) = h(a/1)h(1/s) = g(a)g(s)^{-1}$, 这意味着 h 由 g 唯一确定.

我们可以用 A-模 M 替换环 A 来进行对 S 的局部化构造. 用下列方式定义 $M \times S$ 上的关系 $\sim$:

$$(m, s) \sim (m', s') \iff (sm' - s'm)t = 0, \quad \text{对于某个 } t \in S$$

和以前一样, 这也是一个等价关系. 我们用 m/s 来表示 (m, s) 的等价类, 并用 $S^{-1}M$ 或 $M[S^{-1}]$ 来表示等价类的集合. 有一种自然的方式使 $S^{-1}M$ 成为 $S^{-1}A$-模: 取 $a/s \in S^{-1}A$, 则它在 $S^{-1}M$ 上的作用如下: 取 $m/s' \in S^{-1}M$, 那么

$$a/s \cdot (m/s') := a \cdot m/ss'$$

设 $u \colon M \to N$ 是一个 A-模同态, 则它给出了一个 $S^{-1}A$-模同态 $S^{-1}u \colon S^{-1}M \to S^{-1}N$, 即 $S^{-1}u$ 将 m/s 映射为 $u(m)/s$, 不难验证这是一个良好定义的映射.

9.2 局部化与局部环

一个局部环 $(A, \mathfrak{m})$ 是只有一个极大理想 $\mathfrak{m}$ 的环, 因此一个自然的问题是局部环和局部化之间有什么关系. 为了回答这个问题, 我们需要研究在局部化之后理想会发生什么变化.

回顾理想的扩张: 给定一个环 A 的一个理想 $\mathfrak{a}$ 和一个同态 $f \colon A \to B$, 则 $\mathfrak{a}$ 的扩张是 $A\mathfrak{a}$, 即所有形如 $\sum y_i f(x_i)$ 的元素, 其中 $x_i \in \mathfrak{a}$, $y_i \in B$. 特别地, 如果我们用 $S^{-1}\mathfrak{a}$ 来记由局部化的到的理想的扩张, 那么 $S^{-1}\mathfrak{a}$ 中的元素形如 $\sum_i a_i/s_i$, 其中 $a_i \in \mathfrak{a}$, $s_i \in S$.

定理 9.2.1. *设 A 是一个环, $S^{-1}A$ 是它关于某个乘法闭集 S 的局部化, 则有以下结论:*

(1) $S^{-1}A$ 中的每个理想都是扩张理想.

(2) $S^{-1}A$ 的素理想与 A 中不与 S 相交的素理想一一对应, 即 $(\mathfrak{p} \leftrightarrow S^{-1}\mathfrak{p})$.

证明: 对于 (1), 设 $\mathfrak{b}$ 是 $S^{-1}A$ 中的一个理想, $x/s \in \mathfrak{b}$. 则 $x/1 \in \mathfrak{b}$, 因此 $x \in \mathfrak{b}^c$. 于是, 我们得到 $x/s \in \mathfrak{b}^{ce}$. 这表明 $\mathfrak{b} \subseteq \mathfrak{b}^{ce}$. 同时由于 $\mathfrak{b}^{ce} \subseteq \mathfrak{b}$ 总是成立的, 因此我们得到了 $\mathfrak{b} = \mathfrak{b}^{ce}$.

对于 (2), 若 $\mathfrak{q}$ 是 $S^{-1}A$ 中的一个素理想, 则 $\mathfrak{p} = \mathfrak{q}^c$ 是 A 中的一个素理想. 并且 $\mathfrak{p} \cap S = \varnothing$, 因为 $\mathfrak{q}$ 不包含 $S^{-1}A$ 的单位元. 反过来, 如果 $\mathfrak{p}$ 是 A 中的一个素理想且 $\mathfrak{p} \cap S = \varnothing$, 则有:

$$\frac{a}{s}\frac{b}{t} \in S^{-1}\mathfrak{p} \implies \text{存在 } r \in S \text{ 使得 } rab \in \mathfrak{p}$$

但是 $r \notin \mathfrak{p}$, 所以 a 或 b 在 $\mathfrak{p}$ 中, 即 a/t 或 b/s 在 $S^{-1}\mathfrak{p}$ 中. 因此, $S^{-1}\mathfrak{p}$ 是素理想. □

推论 9.2.2. *设 A 是一个环, $S^{-1}A$ 是它关于某个乘法闭集 S 的局部化. 环同态 $A \to S^{-1}A$ 诱导的素谱之间的映射 $\operatorname{Spec} S^{-1}A \to \operatorname{Spec} A$ 是单射, 并且映射的像是 $\operatorname{Spec} A$ 中与 S 不交的元素.*

推论 9.2.3. 诺特环的局部化是诺特的.

例子. 给定环 A. 设 $\mathfrak{p}$ 是 A 的一个素理想, 则 $S = A - \mathfrak{p}$ 是一个乘法闭集. 在这种情况下, 我们用 $A_\mathfrak{p}$ 表示 $S^{-1}A$. 对于 $A_\mathfrak{p}$, 我们断言它是一个局部环, 其最大理想为 $S^{-1}\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$, 我们将其记作 $\mathfrak{p}A_\mathfrak{p}$. 现在我们来证明断言: 取任意一个不在 $\mathfrak{p}A_\mathfrak{p}$ 中的元素 $a/s \in A_\mathfrak{p}$. 由于 $a, s \in A - \mathfrak{p}$, 所以 a/s 是可逆的, 因为它的逆元是 $s/a \in A_\mathfrak{p}$. 因此, 任何不在 $\mathfrak{p}A_\mathfrak{p}$ 中的元素都是可逆的, 因此 $\mathfrak{p}A_\mathfrak{p}$ 是 $A_\mathfrak{p}$ 的唯一极大理想. 即对一个环以素理想的补集构成的乘法闭集进行局部化, 我们得到的是一个局部环.

例子. 给定环 A, 取一个不是幂零元的元素 $f \in A$, 考虑乘法闭集 $S = \{1, f, f^2, \dots\}$. 在这种情况下, 我们将 $S^{-1}A$ 记做 A_f. 根据定理9.2.1我们知道 A_f 中的素理想与不包含 f 的 A 中的素理想具有一一对应关系, 事实上, 我们有 $\operatorname{Spec} A_f$ 与 U_f 同胚.

9.3 局部性质与层

给定环 A, 如果我们想将 A 中的元素看作是 $\operatorname{Spec} A$ 上的函数, 首先我们有下面的这样做法: 任取 $f \in A$, 其在素理想 $\mathfrak{p}$ 处的取值可以定义为 $\overline{f} \in R/\mathfrak{p}$, 从而的到一个函数

$$\begin{aligned} A &\to \prod_{\mathfrak{p} \in \operatorname{Spec} A} A/\mathfrak{p} \\ f &\mapsto (\pi_\mathfrak{p}(f)) \end{aligned}$$

其中 $\pi_\mathfrak{p} \colon A \to A/\mathfrak{p}$ 是自然投影. 但是如果这样将 $f \in A$ 视作是 $\operatorname{Spec} A$ 上的函数, 这个函数并没有由其在每一个点处的取值完全刻画, 因为上述映射的核是 A 的幂零根, 即所有幂零元都给出了平凡的函数. 借助局部化, 我们可以给出另一种更好的办法.

命题 9.3.1. 给定环 A, 对于 $\mathfrak{p} \in \operatorname{Spec} A$, $A \to A_\mathfrak{p}$ 诱导了如下的单同态

$$A \to \prod_{\mathfrak{p} \in \operatorname{Spec} A} A_\mathfrak{p}$$

即我们要证明, 任取 $f \in A$, 如果 f 在每一个局部化 $A_\mathfrak{p}$ 中都是零, 那么 $f = 0$. 实际上我们可以将如上的命题改写为对一般的 A-模的局部化的一个命题, 这是局部化的一个重要性质.

命题 9.3.2. M 是一个 A-模, 如下叙述等价.

1. $M = 0$.
2. $M_\mathfrak{p} = 0$ 对任意的 $\mathfrak{p} \in \operatorname{Spec} A$ 成立.
3. $M_\mathfrak{m} = 0$ 对任意的 $\mathfrak{m} \in \operatorname{mSpec} A$ 成立.

证明: (1) 推 (2) 推 (3) 是显然的, 现在我们来证明 (3) 推 (1). 如果 $M \neq 0$, 任取 $0 \neq x \in M$, 以及令 $\mathfrak{a}$ 是全体零化 x 的元素组成的理想, 由于 $x \neq 0$, 从而不妨假设 $\mathfrak{a}$ 包含在极大理想 $\mathfrak{m}$ 中. 任取 $x/1 \in M_\mathfrak{m}$, 由于 $M_\mathfrak{m} = 0$, 因此 $x/1 = 0$, 这意味着存在 $A \setminus \mathfrak{m}$ 中的元素零化了 x, 矛盾. □

此外, 映射的单射满射性也是局部性质, 特别地, 映射是否是同构也是局部性质.

命题 9.3.3. 令 $\phi \colon M \to N$ 是一个 A-模同态, 如下叙述等价.

1. ϕ 是单射.
2. $\phi_{\mathfrak{p}}\colon M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ 对于任意的 $\mathfrak{p} \in \operatorname{Spec} A$ 是单射.
3. $\phi_{\mathfrak{m}}\colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ 对任意的 $\mathfrak{m} \in \operatorname{mSpec} A$ 是单射.

命题 9.3.4. 令 $\phi\colon M \to N$ 是一个 A-模同态, 如下叙述等价.

1. ϕ 是满射.
2. $\phi_{\mathfrak{p}}\colon M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ 对于任意的 $\mathfrak{p} \in \operatorname{Spec} A$ 是满射.
3. $\phi_{\mathfrak{m}}\colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ 对任意的 $\mathfrak{m} \in \operatorname{mSpec} A$ 是满射.

特别地, 对于环 A 以及素理想 $f \subseteq A$, A_f 可以视作是 $\operatorname{Spec} A_f$ 上的函数环, 而我们知道, 带有 Zariski 拓扑, A_f 同胚于 U_f, 而 $\operatorname{Spec} A$ 可以被有限多个 U_f 覆盖, 因此 A_f 实际上给出了 $\operatorname{Spec} A$ 上的一些局部定义的函数, 但实际上, 这给出了 $\operatorname{Spec} A$ 上一个**层** (sheaf)结构, 被称为**结构层** (structure sheaf).

命题 9.3.5. 给定环 A 以及 $X = \operatorname{Spec} A$.

1. 如果基本开集 $U \subseteq \operatorname{Spec} A$ 满足 $U = U_f = U_g$, 其中 $f, g \in A$, 那么 $A_f \cong A_g$, 并将其记做 $A(U)$.
2. 如果基本开集 $U' = X_g$ 包含在 $U = X_f$ 中, 证明存在等式 $g^n = uf$, 其中 $n \in \mathbb{Z}_{>0}, u \in A$, 用这个等式定义环同态 $\rho\colon A(U) \to A(U')$, $a/f^m \to au^m/g^{mn}$.
3. 如果 $U = U'$, 则 $\rho\colon A(U) \to A(U)$ 是恒等映射.
4. 如果 $U'' \subseteq U' \subseteq U$ 都是 X 的基本开集, 则有如下交换图

$$\begin{tikzcd} A(U) \arrow[rr] \arrow[dr] & & A(U'') \\ & A(U') \arrow[ur] & \end{tikzcd}$$

5. 取 $\mathfrak{p} \in X$, 则

$$\varinjlim_{\mathfrak{p} \in U} A(U) \cong A_{\mathfrak{p}}$$

9.4 Hom 函子与张量函子

实际上, 局部化与张量函子有着密切的联系, 在介绍这个联系之前, 我们来复习一些有关 Hom 函子与张量函子的同调代数知识.

9.4.1 Hom 函子

给定环 R 以及 R-模 M, N, $\operatorname{Hom}_R(M, N)$ 上自然的有 R-模结构, 可以如下给出: 任取 $\varphi \in \operatorname{Hom}_R(M, N), r \in R$, 定义

$$(r \cdot \varphi)(x) := r\varphi(x)$$

其中 $x \in M$.

练习. 给定 R-模 M.

1. 有作为 R-模的同构 $\operatorname{Hom}_R(R, M) \cong M$.

2. $\mathrm{Hom}_R(\text{-}, M)$ 是一个反变函子.
3. $\mathrm{Hom}_R(M, \text{-})$ 是一个协变函子.

练习. 给定 R-模 $\{M_i\}_{i\in I}$ 以及 N.

1. $\mathrm{Hom}_R(\oplus_i M_i, N) = \prod_i \mathrm{Hom}_R(M_i, N)$.
2. $\mathrm{Hom}_R(N, \prod_i M_i) = \prod_i \mathrm{Hom}_R(N, M_i)$.

命题 9.4.1 (米田引理)**.** 给定 R-模 M, M', 如果对于任意 R-模 P 都存在自然同构

$$\varphi_P\colon \mathrm{Hom}_R(M, P) \to \mathrm{Hom}_R(M', P)$$

其中自然意味着对于任意 R-模同态 $\alpha\colon P_1 \to P_2$, 有如下交换图

$$\begin{tikzcd}
\mathrm{Hom}_R(M, P_1) \arrow[r] \arrow[d, "\varphi_{P_1}"] & \mathrm{Hom}_R(M, P_2) \arrow[d, "\varphi_{P_2}"] \\
\mathrm{Hom}_R(M', P_1) \arrow[r] & \mathrm{Hom}_R(M', P_2)
\end{tikzcd}$$

那么有 R-模同构 $M \cong M'$.

命题 9.4.2 (左正合)**.** 给定 R-模 M 以及 R-模正合列

$$0 \to A \to B \to C \to 0$$

那么

$$0 \to \mathrm{Hom}_R(M, A) \to \mathrm{Hom}_R(M, B) \to \mathrm{Hom}_R(M, C)$$
$$\mathrm{Hom}_R(C, M) \to \mathrm{Hom}_R(B, M) \to \mathrm{Hom}_R(A, M) \to 0$$

是正合列.

证明: 留作习题. □

9.4.2 张量函子

定义 9.4.3. 给定 R-模 M, N, $M \otimes N$ 是一个由 $m \otimes n, m \in M, n \in N$ 生成的自由 R-模商掉如下关系

$$m \otimes (n_1 + n_2) - m \otimes n_1 - m \otimes n_2$$
$$(rm) \otimes n - r(m \otimes n)$$
$$(m_1 + m_2) \otimes n - m_1 \otimes n - m_2 \otimes n$$
$$m \otimes (rn) - r(m \otimes n)$$

得到的 R-模.

例子. 给定环同态 $A \to B$, 我们可以将 B 视作 A-模. 任取 A-模 M, 则 $M_B := B \otimes_A M$ 是一个 B-模, 这个操作又被称为**系数扩张** *(extension of coefficient)*或者**基扩张** *(base extension)*. 另一方面, 任何一个 B-模 M 总可以视作 A-模, 这称为**系数限制** *(restriction of coefficient)*

定理 9.4.4. 给定 R-模 M, N, P, 如下集合间存在自然的同构

$$\mathrm{Hom}_R(M \otimes N, P) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$$

证明: 留作习题. □

注记. Hom 函子与张量函子互为伴随.

推论 9.4.5. 对于 R-模 M, 有 $M \otimes R \cong M$.

证明: 注意到 $\mathrm{Hom}_R(R, M) \cong M$. □

命题 9.4.6. 给定 R-模 $\{M_i\}_{i\in I}$ 以及 R-模 N.

$$N \otimes (\bigoplus_i M_i) \cong \bigoplus_i (N \otimes M_i)$$

证明: 任取 R-模 P, 有如下自然的同构

$$\begin{aligned}
\mathrm{Hom}_R(N \otimes (\bigoplus_{i\in I} M_i), P) &\cong \mathrm{Hom}_R(N, \mathrm{Hom}_R(\bigoplus_{i\in I} M_i, P)) \\
&\cong \mathrm{Hom}_R(N, \prod_{i\in I} \mathrm{Hom}_R(M_i, P)) \\
&\cong \prod_{i\in I} \mathrm{Hom}_R(N, \mathrm{Hom}_R(M_i, P)) \\
&\cong \prod_{i\in I} \mathrm{Hom}_R(N \otimes M_i, P) \\
&\cong \mathrm{Hom}_R(\bigoplus_{i\in I} (N \otimes M_i), P)
\end{aligned}$$

从而根据米田引理, 即命题9.4.1可知

$$N \otimes (\bigoplus_{i\in I} M_i) \cong \bigoplus_{i\in I} (N \otimes M_i)$$

□

注记. 一般来说, $N \otimes (\prod_{i\in I} M_i) \not\cong \prod_{i\in I}(N \otimes M_i)$, 见习题.

命题 9.4.7 (右正合)**.** 给定 R-模 M 以及 R-模正合列

$$0 \to A \to B \to C \to 0$$

那么

$$A \otimes M \to B \otimes M \to C \otimes M \to 0$$

是正合列.

证明: 利用 Hom 函子的左正合性以及定理9.4.4即可. □

推论 9.4.8. 给定 R-模 M 以及理想 $I \subseteq R$, 则 R-模同构 $(R/I) \otimes M \cong M/IM$.

证明: 考虑函子 - $\otimes M$ 作用在正合列 $0 \to I \to R \to R/I \to 0$ 上. □

9.5 平坦性与局部化

9.5.1 平坦模

定义 9.5.1. 给定 R-模 M, 其被称为**平坦的** (flat), 如果张量函子 $-\otimes M$ 是正合函子.

命题 9.5.2. *如下叙述等价.*

1. *R-模 M 平坦.*
2. *张量函子 $-\otimes M$ 左正合.*
3. *如果 $f\colon A\to B$ 是 R-模单同态以及 A,B 是有限生成模, 则 $A\otimes M\to B\otimes$ 是单射.*

推论 9.5.3. *给定环同态 $f\colon A\to B$ 以及平坦 A-模 M, 那么 $M_B=B\otimes_A M$ 是平坦 B-模.*

证明: 任取 B-模的正合列 $0\to N_1\to N_2$, 我们只需要证明

$$0\to N_1\otimes_B(B\otimes_A M)\to N_2\otimes_B(B\otimes_A M)$$

是正合列即可. 利用张量的典范同构我们只需要证明

$$0\to(N_1\otimes_B B)\otimes_A M\to(N_2\otimes_B B)\otimes_A M$$

是正合的. 注意到 $N_1\otimes_B B=N_1, N_2\otimes_B B=N_2$ 以及 M 是平坦 A-模即可. □

注记. 这意味着平坦性在基扩张下稳定.

命题 9.5.4. *M 是一个 R-模, 如下叙述等价.*

1. *M 平坦.*
2. *$M_{\mathfrak{p}}$ 平坦对任意的 $\mathfrak{p}\in\operatorname{Spec}R$ 成立.*
3. *$M_{\mathfrak{m}}$ 平坦对任意的 $\mathfrak{m}\in\operatorname{mSpec}R$ 成立.*

9.5.2 张量函子与局部化

命题 9.5.5. *给定乘法闭集 S, 局部化函子 S^{-1} 是一个正合函子.*

证明: 对于一个 R-模正合列 $M'\xrightarrow{f}M\xrightarrow{g}M''$, 我们需要证明 $S^{-1}M'\xrightarrow{S^{-1}f}S^{-1}M\xrightarrow{S^{-1}g}S^{-1}M''$ 是正合的. 显然有 $S^{-1}g\circ S^{-1}f=0$, 因为 $S^{-1}g\circ S^{-1}f=S^{-1}(g\circ f)=S^{-1}(0)=0$. 反过来, 对于 $m/s\in\ker S^{-1}g$, 我们有 $g(m)/s=0\in S^{-1}M''$, 因此存在一个 $t\in S$ 使得 $tg(m)=0$ 在 M'' 中成立, 即 $tm\in\ker g=\operatorname{im}f$. 因此, 存在 $m'\in M'$, 使得 $f(m')=tm$. □

推论 9.5.6. *局部化与有限和, 有限交以及商交换, 即如果 N,P 都是 A-模 M 的子模, 则*

1. *$S^{-1}(N+P)=S^{-1}(N)+S^{-1}(P)$*
2. *$S^{-1}(N\cap P)=S^{-1}(N)\cap S^{-1}(P)$*
3. *有 $S^{-1}A$-模同构 $S^{-1}(M/N)\cong S^{-1}(M)/S^{-1}(N)$.*

证明: (1) 是显然的. 对于 (2), 如果 $y/s=z/t$, 其中 $y\in N,z\in P,s,t\in S$, 那么存在 $u\in S$ 使得 $u(ty-sz)=0$, 因此 $w=uty=usz\in N\cap P$, 因此 $y/s=w/stu\in S^{-1}(N\cap P)$. 因此, $S^{-1}N\cap S^{-1}P\subseteq S^{-1}(N\cap P)$, 反向包含则是显然的. 对于 (3), 用正合函子 S^{-1} 作用正合序列 $0\to N\to M\to M/N\to 0$ 即可. □

命题 9.5.7. *令 M 是一个 A-模, 则 $S^{-1}M$ 和 $S^{-1}A\otimes_A M$ 作为 $S^{-1}A$-模同构.*

证明: 考虑 $S^{-1}A$-双线性映射

$$S^{-1}A\times M\to S^{-1}M$$

$$(a/s,m)\mapsto am/s$$

则它诱导了一个 $S^{-1}A$-模同态 $f\colon S^{-1}A\otimes_A M\to S^{-1}M$. 显然 f 是满射的. 设 $\sum_i(a_i/s_i)\otimes m_i$ 为 $S^{-1}A\otimes M$ 的任意元素. 如果 $s=\prod_i s_i\in S, t_i=\prod_{i\neq j}s_j$, 那么

$$\sum_i\frac{a_i}{s_i}\otimes m_i=\sum_i\frac{a_it_i}{s}\otimes m_i=\sum_i\frac{1}{s}\otimes a_it_im=\frac{1}{s}\otimes\sum_i a_it_im_i$$

因此 $S^{-1}A\otimes M$ 中的每个元素都可以表示为 $(1/s)\otimes m$ 的形式. 假设 $f((1/s)\otimes m)=0$, 则 $m/s=0$, 因此存在某个 $t\in S$, 使得 $tm=0$. 因此,

$$\frac{1}{s}\otimes m=\frac{t}{st}\otimes m=\frac{1}{st}\otimes tm=\frac{1}{st}\otimes 0=0$$

因此, $\ker f=\{0\}$, 因此 f 是一个单同态, 所以 $S^{-1}A\otimes_A M$ 作为 $S^{-1}A$-模同构于 $S^{-1}M$. □

推论 9.5.8. *$S^{-1}A$ 是平坦 A-模.*

证明: 对于任意的 A-模 $0\to M'\to M$ 的正合列, 我们需要证明

$$0\to S^{-1}A\otimes_A M'\to S^{-1}A\otimes_A M$$

是正合的. 但是这同构于

$$0\to S^{-1}M'\to S^{-1}M$$

根据 S^{-1} 是正合函子即可得到想要的结论. □

第十章　整性与 Nullstellensatz 定理

10.1　整性

定义 10.1.1. 给定环 R 以及 R-代数 A, $\alpha \in A$ 被称为在 R 上**整** (integral), 如果 α 满足某个 R 系数首一多项式, 即存在 $r_{n-1}, \dots, r_0 \in R$ 使得

$$\alpha^n + r_{n-1}\alpha^{n-1} + \cdots + r_0 = 0$$

定义 10.1.2. 给定环 R 以及 R-代数 A, 用 B 来记 A 中在 R 上整的元素组成的子环.

1. 如果 $B = A$, 则称 A 在 R 上**整** (integral).
2. 如果 $B = R$, 则称 R 在 A 中**整闭** (integrally closed)

定义 10.1.3. 给定整环 R, 如果 R 在其分式域中整闭, 则称其为**整闭整环** (integrally closed domain), 或**正规环** (normal ring)

例子. $\mathbb{Q}$ 中在 $\mathbb{Z}$ 上整的元素全体为 $\mathbb{Z}$.

例子. $\mathbb{C}$ 中在 $\mathbb{Z}$ 上整的元素全体为代数整数.

命题 10.1.4. *给定环 R,R-代数 A 以及 $\alpha \in A$, 如下叙述等价.*

1. α 在 R 上整.
2. $R[\alpha]$ 是有限生成 R-模.
3. $R[\alpha]$ 被包含在 A 的一个子环 B 中, 并且 B 是有限生成 R-模.
4. 存在一个忠实的 $R[\alpha]$-模 M, 并且作为 R-模是有限生成的.

推论 10.1.5. *给定环 R 以及 R-代数 A, A 中在 R 上整的元素全体构成了 A 的子环.*

推论 10.1.6. *给定环 R, A, B 以及环同态 $R \to A \to B$, 如果 B 在 A 上整, A 在 R 上整, 那么 B 在 R 上整.*

命题 10.1.7. *给定环 A 以及 A-代数 B, 假设 B 在 A 上整.*

1. 如果 $\mathfrak{b} \subseteq B$ 是理想, 并且 $\mathfrak{a} = \mathfrak{b}^c$, 则 $B/\mathfrak{b}$ 在 $A/\mathfrak{a}$ 上整.
2. 如果 S 是 A 中的乘法闭集, 则 $S^{-1}B$ 在 $S^{-1}A$ 上整.

证明: (1). 任取 $b \in B$, 由于 B 在 A 上整, 从而满足

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0$$

其中 $a_i \in A$. 因此对系数模 $\mathfrak{a}$ 即可知 $B/\mathfrak{b}$ 在 $A/\mathfrak{a}$ 上整.

(2). 任取 $b/s \in S^{-1}B$, 假设 $b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0, a_i \in A$, 则

$$(\frac{b}{s})^n + \cdots + (\frac{a_{n-1}}{s})(\frac{b}{s})^{n-1} + \cdots + \frac{a_0}{s^n} = 0$$

意味着 b/s 在 $S^{-1}A$ 上整, 从而 $S^{-1}B$ 在 $S^{-1}A$ 上整. □

10.2 Cayley-Hamilton 定理

定理 10.2.1 (Cayley-Hamilton). *给定环 R 以及理想 $I \subseteq R$. 令 M 是一个由 n 个元素生成的有限生成 R-模, $\varphi\colon M \to M$ 满足 $\varphi(M) \subseteq IM$, 则存在一个首一多项式*

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

使得 $a_i \in I$ 以及 $p(\varphi)$ 是零映射.

证明: φ 通过 $x \cdot m = \varphi(m), m \in M$ 赋予了 M 上一个 $R[x]$-模结构. 假设 M 作为 R-模由 $m_1, \ldots, m_n$ 生成, 并且用 K 来记 φ 在 $m_1, \ldots, m_n$ 下的矩阵, 即

$$x \cdot m_i = \sum_{j=1}^{n} r_{ij} m_j$$

并且由于 $\varphi(M) \subseteq IM$, 从而 $K \in M_n(I)$. 注意到

$$(xI - K)\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0$$

从而 $\det(xI - K) = 0$, 即 φ 满足一个系数在 I 中的首一多项式. □

推论 10.2.2. *给定环 R 以及有限生成 R-模 M, 如果 $I \subseteq R$ 是使得 $IM = M$ 的理想, 那么存在 $x \in R$ 满足 $x \equiv 1 \pmod I$ 使得 $xM = 0$.*

推论 10.2.3 (Nakayama). *给定环 R 以及有限生成 R-模 M, 任取包含在 Jacobson 根中的理想 I, 如果 $IM = M$, 那么 $M = 0$.*

证明: 根据推论10.2.2, 存在 $x \in R$ 使得 $xM = 0$ 以及 $x \equiv 1 \pmod I$. 根据 $1 - x \in I \subseteq \mathfrak{R}$, 从而对任意 $y \in R$ 有 $1 - y(1-x)$ 是 R 中的单位, 特别地, x 是 R 中的单位, 从而 $M = 0$. □

10.3 上升定理

定理 10.3.1 (lying over and going-up). *设 $A \subseteq B$ 为环, B 在 A 上整. 任取素理想 $\mathfrak{p} \subseteq A$, 存在素理想 $\mathfrak{q} \subseteq B$ 使得 $\mathfrak{q} \cap A = \mathfrak{p}$, 并且 $\mathfrak{q}$ 可以被选为包含任意给定的 $\mathfrak{q}' \subseteq B$, 其中 $\mathfrak{q}' \cap A \subseteq \mathfrak{p}$.*

证明: 由于整性在做商运算下保持, 通过商掉 $\mathfrak{q}'$ 与 $\mathfrak{q}' \cap A$, 我们不妨假设 $\mathfrak{q}'$ 是零理想, 因此只需要证明满足 $\mathfrak{q} \cap A = \mathfrak{p}$ 的素理想 $\mathfrak{q}$ 的存在性. 令 $S = A \setminus \mathfrak{p}$ 是乘法闭集, 通过考虑局部化 $S^{-1}A$ 以及 $S^{-1}B$, 我们不妨假设 A 是以 $\mathfrak{p}$ 为唯一极大理想的局部环. B 的任何包含 $\mathfrak{p}B$ 的极大理想

$\mathfrak{q}$ 与 R 做交总是包含 $\mathfrak{p}$, 根据 $\mathfrak{p}$ 是极大理想有 $\mathfrak{q}\cap R=\mathfrak{p}$. 因此我们只需要证明 $\mathfrak{p}B\neq B$ 即可. 若假设 $\mathfrak{p}B=B$, 则 $1\in B$ 可以被表示为有限个 $\mathfrak{p}$ 中的元素的 B 线性组合, 令 B' 是这些元素生成的子代数, 从而 $\mathfrak{p}B'=B'$. 由于 B 在 A 上整, 从而 B' 也在 A 上整, 从而 B' 是有限生成 A-模. 根据推论10.2.3, 即 Nakayama 引理可知 $B'=0$, 矛盾. □

推论 10.3.2. *给定整环 $A\subseteq B$, 如果 B 在 A 上整, 则 B 是一个域当且仅当 A 也是一个域.*

证明: 假设 A 是域, 由于 B 在 A 上整, 从而任何 $b\in B$ 满足

$$b^n+a_{n-1}b^{n-1}+\cdots+a_0=0$$

其中 $a_i\in A$, 因此 $b^{-1}=-1/a_0(b^{n-1}+a_{n-1}b^{n-2}+\cdots+a_1)$, 即 B 是域. 另一方面, 如果 B 是域, 任取 A 的极大理想 $\mathfrak{m}$, 根据定理10.3.1可知存在素理想 $\mathfrak{q}\cap A=\mathfrak{m}$, 但是 B 的素理想, 即 $\mathfrak{q}=0$, 进而 $\mathfrak{m}=0$, 因此 A 是一个域. □

推论 10.3.3. *设 $A\subseteq B$ 为环, B 在 A 上整, $\mathfrak{q}$ 是 B 的素理想, $\mathfrak{p}=\mathfrak{q}^c$, 则 $\mathfrak{q}$ 是极大理想当且仅当 $\mathfrak{p}$ 是极大理想.*

证明: 由于整性在做商运算下保持, 在 A,B 中分别商掉 $\mathfrak{p}$ 和 $\mathfrak{q}$, 再利用推论10.3.2即可. □

引理 10.3.4. *给定整环 $A\subseteq B$. 如果 $K(B)/K(A)$ 是代数扩张, 则任何 B 的非零理想和 A 的交都非零.*

证明: 我们只需要证明 B 的任何非零主理想 (b) 与 A 的交都非零即可. 由于 $K(B)/K(A)$ 是代数扩张, 从而 b 满足如下的方程

$$b^n+a_{n-1}b^{n-1}+\cdots+a_1b+a_0=0$$

其中 $a_i\in K(A)$. 乘以 a_i 分母的最大公因子, 我们不妨假设上述所有的 $a_i\in A$, 并且由于 b 是整环, 我们不妨假设 $a_0\neq 0$, 从而 $a_0\in(b)\cap A$. □

推论 10.3.5 (incomparability)**.** *设 $A\subseteq B$ 为环, B 在 A 上整, $\mathfrak{q},\mathfrak{q}'$ 是 B 的素理想, 且 $\mathfrak{q}\subseteq\mathfrak{q}'$. 如果 $\mathfrak{q}\cap A=\mathfrak{q}'\cap A=\mathfrak{p}$, 则 $\mathfrak{q}=\mathfrak{q}'$.*

证明: 由于整性在做商运算下保持, 通过在 A,B 中商掉 $\mathfrak{p},\mathfrak{q}$, 不妨假设 $\mathfrak{p}=\mathfrak{q}=(0)$, 以及 $\mathfrak{q}'\cap A=(0)$. 由于 B 在 A 上整, 从而 $K(B)/K(A)$ 是代数扩张, 因此 $\mathfrak{q}'=(0)$. □

10.4 Nullstellensatz 定理

在本节中我们要证明如下的定理.

定理 10.4.1. *令 R 是一个 Jacobson 环, $A=R[x_1,\ldots,x_n]/I$ 是有限生成 R-代数, 则 A 也是 Jacobson 环, 任取极大理想 $\mathfrak{n}\subseteq A$, $\mathfrak{m}=\mathfrak{n}\cap R$ 是 R 的极大理想, 并且 $A/\mathfrak{n}$ 是 $R/\mathfrak{m}$ 的有限扩张.*

推论 10.4.2 (Nullstellensatz)**.** *给定代数闭域 k, $A=k[x_1,\ldots,x_n]$ 的极大理想都形如 $(x_1-\alpha_1,\ldots,x_n-\alpha_n)$, 其中 $\alpha_1,\ldots,\alpha_n\in k$.*

证明: 根据定理10.4.1, 任取极大理想 $\mathfrak{m} \subseteq A$, $\mathfrak{n} \cap k$ 是 k 的极大理想, 从而 $\mathfrak{n} \cap k = (0)$, 并且由于 k 是代数闭域, 不存在有限扩张, 因此

$$
\begin{aligned}
A/\mathfrak{n} &\to k \\
x_i &\mapsto \alpha_i
\end{aligned}
$$

是同构, 从而 $\mathfrak{n} = (x_1 - \alpha_1, \ldots, x_n - \alpha_n)$. □

为了证明定理10.4.1, 我们需要如下引理.

引理 10.4.3 (Rabinowitch trick)**.** *如下叙述是等价的.*

(1) *R 是 Jacobson 环.*

(2) *给定素理想 $P \subseteq R$, 记 $S = R/P$. 如果存在 $0 \neq b \in S$, 使得 S_b 是一个域, 则 S 是一个域.*

证明: (1) 推 (2): 由于 R 是 Jacobson 环, 从而 S 也是 Jacobson 环, 并且由于 S 是整环, 从而其幂零根为零理想, 从而 S 的 Jacobson 根也是零理想. 注意到 S_b 所有的素理想与 S 不含 b 的素理想有一一对应, 而当 S_b 是域时, 不等于整个环的理想只有零理想, 从而 b 被包含在 S 的所有非零理想中, 因此 (0) 是 S 的极大理想, 即 S 是域.

(2) 推 (1): 任取 R 的素理想 Q, 并且令 I 是所有包含 Q 的极大理想的交, 我们断言 $I = Q$. 若 $I \neq Q$, 任取 $f \in I \setminus Q$, 根据 Zorn 引理我们可以选素理想 P, 使得 P 是包含 Q 但不包含 f 的最大的素理想. 根据假设 P 不是极大理想, 从而 $S = R/P$ 不是域. 然而 P 生成了 R_f 的极大理想, 从而 $(R/P)_f$ 是域, 这与假设矛盾, 从而 $I = Q$, 因此 R 是 Jacobson 环. □

推论 10.4.4. *假设 R 是一个 Jacobson 环, 则 R 的商环都是 Jacobson 环.*

引理 10.4.5. *假设 R 是一个域, $A = R[x]$, 则 A 是 Jacobson 环, 任取极大理想 $\mathfrak{n} \subseteq A$, $\mathfrak{m} = \mathfrak{n} \cap R$ 是 R 的极大理想, 并且 $A/\mathfrak{n}$ 是 $R/\mathfrak{m}$ 的有限扩张.*

证明: A 是一个 Jacobson 环已经在作业 9 中证明过. 由于 A 是主理想整环, 从而 A 的极大理想和素理想相同, 因此极大理想 $\mathfrak{n} \subseteq A$ 形如 $(f(x))$, 其中 $f(x) \in R[x]$ 是不可约多项式. 显然 $\mathfrak{n} \cap R = (0)$ 以及 $A/(f(x))$ 是 R 的有限扩张. □

引理 10.4.6. *给定 Jacobson 整环 R, 对于素理想 $\mathfrak{p} \subseteq R[x]$, 如果存在 $0 \neq b \in R[x]/\mathfrak{p}$ 满足 $(R[x]/\mathfrak{p})_b$ 是域, 则 R 和 $R[x]/\mathfrak{p}$ 都是域, 特别的, $R[x]$ 是 Jacobson 环.*

证明: 我们先证明这样的 $\mathfrak{p} \neq (0)$. 若 $\mathfrak{p} = (0)$, 根据假设存在 $0 \neq b \in R[x]$ 使得 $R[x]_b$ 是域. 记 K 是 R 的分式域, 那么 $(K[x])_b$ 也是域. 根据引理10.4.5可知 $K[x]$ 是 Jacobson 环, 从而再利用引理10.4.3可知 $K[x]$ 是域, 相矛盾, 从而 $\mathfrak{p} \neq (0)$. 任取 $0 \neq f(x) = p_n x^n + \cdots + p_0 \in \mathfrak{p}$, 其中 $p_i \in R, 0 \leq i \leq n$, 可知 $(R[x]/\mathfrak{p})_{p_n}$ 在 R_{p_n} 上整. 由于 $b \in R[x]/\mathfrak{p}$ 也满足某个系数在 R 中的多项式, 不妨假设

$$q_m b^m + \cdots + q_0 = 0$$

并且由于 $R[x]/\mathfrak{p}$ 是整环, 不妨假设 $q_0 \neq 0$. 记 $\beta = b^{-1}$, 则

$$\beta^m + (q_1/q_0)\beta^{m-1} + \cdots + q_m/q_0$$

由于 $(R[x]/\mathfrak{p})_b$ 是域, 从而 $(R[x]/\mathfrak{p})_b=(R[x]/\mathfrak{p})_{p_n b}$, 而后者在 $R_{p_n q_0}$ 上整, 根据推论10.3.2可知 $R_{p_n q_0}$ 是一个域, 由于 R 是 Jacobson 整环, 再利用引理10.4.3可知 R 是域, 从而 $\mathfrak{p}\subseteq R[x]$ 是极大理想, 进而 $R[x]/\mathfrak{p}$ 是域. $\square$

现在我们开始定理10.4.1的证明.

定理10.4.1的证明. 首先考虑一个特殊情况: R 是一个 Jacobson 环, $A=R[x]$. 为了证明 A 是 Jacobson 环, 我们需要使用引理10.4.3: 对于素理想 $\mathfrak{p}\subseteq A$, 如果存在 $0\neq b\in A/\mathfrak{p}$ 使得 $(A/\mathfrak{p})_b$ 是域, 则 $A/\mathfrak{p}$ 是域. 令 $R'=R/\mathfrak{p}\cap R$, 则根据推论10.4.4可知 R' 是一个 Jacobson 整环. 注意到我们有自然满射 $\varphi\colon R[x]\to R'[x]$, 并且映射的核为 $(\mathfrak{p}\cap R)[x]\subseteq\mathfrak{p}$, 即有同构

$$R'[x]\cong R[x]/(\mathfrak{p}\cap R)[x]$$

记 $\mathfrak{p}'$ 为 $\varphi(\mathfrak{p})$ 在 $R'[x]$ 中生成的理想, 上述同构两侧同时商掉 $\mathfrak{p},\mathfrak{p}'$ 则有 $A/\mathfrak{p}\cong R'[x]/\mathfrak{p}'$, 利用引理10.4.6可知 $A/\mathfrak{p}\cong R'[x]/\mathfrak{p}'$ 是域, 从而 A 是 Jacobson 环. 归纳地我们可以证明 $A=R[x_1,\ldots,x_n]$ 都是 Jacobson 环.

任取极大理想 $\mathfrak{n}\subseteq R[x_1,\ldots,x_n]$, 根据引理10.4.5可知 $\mathfrak{n}\cap R[x_1,\ldots,x_{n-1}]\subseteq R[x_1,\ldots,x_{n-1}]$ 的极大理想, 并且 $R[x_1,\ldots,x_n]/\mathfrak{n}$ 是 $R[x_1,\ldots,x_{n-1}]/\mathfrak{n}\cap R[x_1,\ldots,x_{n-1}]$ 的有限扩张, 经过有限次归纳之后可知 $\mathfrak{m}=\mathfrak{n}\cap R\subseteq R$ 是极大理想, 并且 $R[x_1,\ldots,x_n]/\mathfrak{n}$ 是 $R/\mathfrak{m}$ 的有限扩张, 这对 $A=R[x_1,\ldots,x_n]$ 的情形证明了 Nullstellensatz 定理, 对于 $A=R[x_1,\ldots,x_n]/I$ 的情形, 只需要注意到 Jacobson 环的商环依然是 Jacobson 环即可. $\square$

第十一章 一维与余一维

11.1 离散赋值环

定义 11.1.1. 令 K 是一个域, K 上的一个**赋值** (valuation)是一个满射

$$\nu\colon K^\times \to \mathbb{Z}$$

满足对任意 $x, y \in K^\times$, 有

(1) $\nu(xy) = \nu(x) + \nu(y)$,

(2) $\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$.

注记. 为了之后方便定义赋值环, 我们一般约定 $\nu(0) = \infty$.

例子. 令 $K = k(x)$ 是域 k 系数的有理函数域, 任取 $0 \neq f(x) \in k[x]$, 如果 $f(x) = x^n f_0(x), x \nmid f_0(x)$, 则定义

$$\nu_0(f(x)) = n$$

以及

$$\nu_0\left(\frac{f(x)}{g(x)}\right) = \nu_0(f(x)) - \nu_0(g(x))$$

则 ν_0 给出了 K 上的一个赋值. 类似的如果考虑

$$\nu_\infty(f(x)) = -\deg f(x)$$

以及

$$\nu_\infty\left(\frac{f(x)}{g(x)}\right) = -\deg f(x) + \deg g(x)$$

则 ν_∞ 也给出了 K 上的一个赋值.

注记. ν_0 和 ν_∞ 可以看作是考虑有理函数的零点与极点个数给出的赋值, 实际上, 一般的赋值可以视作是如上的推广.

例子. 给定素数 p, 任取 $n \in \mathbb{Z} \setminus \{0\}$, 我们将其写作 $n = p^k m$, 其中 $p \nmid m$, 定义

$$\nu_p(n) = k$$
$$\nu_p\left(\frac{m}{n}\right) = \nu_p(m) - \nu_p(n)$$

给出了 $\mathbb{Q}$ 上的一个赋值.

定义 11.1.2. 给定域 K 以及其上的赋值 ν, 如下定义的集合

$$R = \{x \in K \mid \nu(x) \geq 0\} \cup \{0\}$$

被称为 K 的**赋值环** (valuation ring).

命题 11.1.3. 赋值环 R 是一个环, 并且是一个局部环, 其唯一的极大理想为 $\mathfrak{m} = \{x \in K \mid \nu(x) > 0\}$.

证明: 首先来验证 R 是一个环: 由于 $\nu(0) = \infty$ 以及 $\nu(1) = 0$, 所以 $1, 0 \in R$. 任取 $x, y \in R$, 注意到

$$\nu(x \pm y) \geq \min\{\nu(x), \nu(\pm y)\} = \min\{\nu(x), \nu(y)\} \geq 0$$

其中 $\nu(-y) = \nu(y)$ 是因为不难发现 $\nu(-1) = 0$, 因此 R 对加减封闭, 同时交换律和结合律也是满足的, 因为其作为 K 的运算具有交换律和结合律, 因此 R 构成了一个环.

下面来验证 $\mathfrak{m}$ 是唯一的极大理想: 任取 $x, y \in \mathfrak{m}, a, b \in R$, 注意到

$$\nu(ax + by) \geq \min\{\nu(ax), \nu(by)\} = \min\{\nu(a) + \nu(x), \nu(b) + \nu(y)\} \geq \min\{\nu(x), \nu(y)\} > 0$$

因此 $\mathfrak{m}$ 是一个理想, 并且由于 $1 \notin \mathfrak{m}$, 从而是真理想. 下面只需要证明任取 $a \in R \setminus \mathfrak{m}$, 都有 a 在 R 中可逆即可. 由于 $\nu(a) = 0$, 取 a^{-1} 是 a 在 K 中的逆, 根据 $\nu(a) + \nu(a^{-1}) = \nu(1) = 0$ 可知 $\nu(a^{-1}) = 0$, 因此 $a^{-1} \in R$, 即 a 在 R 中可逆. □

定义 11.1.4. 给定整环 R, 如果其分式域上存在一个赋值 ν 使得 R 是赋值 ν 对应的赋值环, 则 R 被称为**离散赋值环** (discrete valuation ring).

例子. 令 $K = k(x)$ 是域 k 系数的有理函数域, 则例子11.1中构造的赋值 ν_0 对应的赋值环为 $k[x]_{(x)}$, 即 $k[x]$ 关于 (x) 做局部化得到的环.

例子. 令 $K = \mathbb{Q}$, 则例子11.1中构造的赋值 ν_p 对应的赋值环为 $\mathbb{Z}_{(p)}$, 即 $\mathbb{Z}$ 关于 (p) 做局部化得到的环.

定义 11.1.5. 给定离散赋值环 R, 其上的赋值为 ν, $\pi \in R$ 使得 $\nu(\pi) = 1$ 被称为**一致化子** (uniformiser)

注记. 一致化子的存在性是由于赋值 ν 是满射保证的.

在本节如下的命题中, R 总是指离散赋值环, 其极大理想为 $\mathfrak{m}$.

命题 11.1.6. $\mathfrak{m} = (\pi)$, 其中 π 是 R 的一致化子.

证明: 给定一致化子 π, 由于 $\nu(\pi) = 1$, 从而 $(\pi) \subseteq \mathfrak{m}$; 另一方面, 任取 $a \in \mathfrak{m}$, 由于 $\nu(\pi^{-1}a) = \nu(\pi^{-1}) + \nu(a) = -1 + \nu(a) \geq 0$, 从而 $\pi^{-1}a = r \in R$, 因此 $a = \pi r \in (\pi)$, 从而 $\mathfrak{m} = (\pi)$. □

命题 11.1.7. 如果 $\mathfrak{m} = (\pi')$, 则 π' 是一致化子.

证明: 假设 $\mathfrak{m}$ 由元素 π' 生成, 从而 $\pi' \in \mathfrak{m}$, 因此至少有 $\nu(\pi') \geq 1$. 假设 π 是一个一致化子, 并且假设 $\pi = a\pi'$, 从而有

$$1 = \nu(\pi) = \nu(a) + \nu(\pi') \geq \nu(\pi')$$

从而 $\nu(\pi') = 1$, 即 π' 是一致化子. □

命题 11.1.8. *R 是主理想整环, 并且每个理想都形如 $\mathfrak{m}^k, k \geq 0$, 并且如果 $k \neq k'$, 则 $\mathfrak{m}^k \neq \mathfrak{m}^{k'}$.*

证明: 根据定义离散赋值环是整环, 从而只需要证明其为主理想即可. 任取理想 $I \subseteq R$, 令

$$\min\{\nu(a) \mid a \in I\} = k \geq 0$$

并且不妨假设 $a \in I$ 使得 $\nu(a) = k$, 从而 $\nu(a\pi^{-k}) = 0$, 即存在 R 中的单位 u 使得 $a\pi^{-k} = u$, 即 $a = \pi^k u$, 即 $\mathfrak{m}^k = (\pi^k) \subseteq I$; 另一方面, 任取 $b \in I$, 由于 $\nu(b) \geq k$, 从而 $b = \pi^k b'$, 其中 $b' \in R$, 即 $b \in (\pi^k)$, 从而 $I \subseteq \mathfrak{m}^k$, 至此我们证明了 R 是主理想整环, 并且任何一个理想都形如 $\mathfrak{m}^k$.

为了证明命题的后半部分, 不妨假设 $k > k'$ 以及 $\mathfrak{m}^k = \mathfrak{m}^{k'}$. 注意到 $\mathfrak{m}^{k-k'}\mathfrak{m}^{k'} = \mathfrak{m}^k = \mathfrak{m}^{k'}$, 根据中山正引理可知 $\mathfrak{m}^{k'} = 0$, 矛盾. □

11.2 离散赋值环、正规环与正则环

定义 11.2.1. 局部环 $(R, \mathfrak{m})$ 被称为**正则环** (regular ring), 如果 k-线性空间 $\mathfrak{m}/\mathfrak{m}^2$ 的维数等于 R 的 Krull 维数, 其中 $k = R/\mathfrak{m}$ 是 R 的剩余域.

定理 11.2.2. *假设 $(R, \mathfrak{m})$ 是诺特局部整环, 并且 R 不是域. 则如下叙述等价:*

(1) R 是离散赋值环.

(2) R 是主理想整环.

(3) $\mathfrak{m}$ 是主理想.

(4) R 是正规环, 并且 Krull 维数为 1.

(5) R 的任何理想 I 都形如 $\mathfrak{m}^k, k \geq 0$.

(6) R 是正则环.

证明: 我们如下来证明上述六条是等价的: 首先我们证明 (1) ⇒ (2) ⇒ (3) 与 (1) ⇒ (2) ⇒ (4), 再利用 (4) 中的条件可以得到 (1) ⇒ (2) ⇒ (3) ⇒ (6), 并且 (6) ⇒ (3) 是容易的; 之后再证明 (4) ⇒ (3) ⇒ (2) ⇒ (1), 至此我们有 (1), (2), (3), (4), (6) 是等价的; 最后我们证明 (1) ⇒ (5) 以及 (5) ⇒ (3) 来完成证明.

根据命题11.1.8可知 (1) ⇒ (2), 并且 (2) ⇒ (3) 是显然的. 现在我们证明 (2) ⇒ (4): 首先不难证明任何主理想整环都是正规的, 并且每个非域的主理想整环一定是一维的, 否则任取非零的素理想 $\mathfrak{p} = (p)$, 假设 $\mathfrak{q} = (q)$ 是另一个素理想满足 $\mathfrak{p} \subsetneq \mathfrak{q}$, 那么存在 $a \in R \setminus R^\times$ 使得 $p = aq$, 由于 $\mathfrak{p}$ 是素理想, 从而 $a \in \mathfrak{p}$, 即存在 $b \in R$ 使得 $a = b\mathfrak{p}$, 从而 $p = abp$, 进而有 $ab = 1$, 与 $a \in R \setminus R^\times$ 相矛盾, 从而证明了 (2) ⇒ (4).

现在我们在 (4) 的条件下证明 (3) ⇒ (6): 如果 $\mathfrak{m}$ 是主理想, 那么 $\mathfrak{m}/\mathfrak{m}^2$ 最多由一个元素生成, 即 $\dim \mathfrak{m}/\mathfrak{m}^2 \leq 1$. 如果 $\mathfrak{m} = \mathfrak{m}^2$, 根据中山正引理可知 $\mathfrak{m} = 0$, 与 R 不是域矛盾, 从而 $\dim \mathfrak{m}/\mathfrak{m}^2 = 1$, 即 R 是正则环.

现在来证明 (4) ⇒ (3): $\dim_{Krull} R = 1$ 意味着任何非零的素理想都是极大理想, 并且由于 R 是局部环, 从而所有的非零素理想都等于唯一的极大理想 $\mathfrak{m}$. 任取 $0 \neq t \in \mathfrak{m}$, 我们断言根式理想 $\sqrt{(t)} = \mathfrak{m}$, 并且存在 $k \in \mathbb{N}$ 使得 $\mathfrak{m}^k \subseteq (t) \subseteq \mathfrak{m}$. 注意到

$$\sqrt{(t)} = \bigcap_{\substack{(t) \subseteq \mathfrak{p} \\ \mathfrak{p} \text{ is prime}}} \mathfrak{p}$$

从而 $\sqrt{(t)}=\mathfrak{m}$. 由于 R 是诺特的, 不妨假设 $\mathfrak{m}$ 由有限个元素 $m_1,\ldots,m_t$ 生成. 由于 $\sqrt{(t)}=\mathfrak{m}$, 从而存在 $k_1,\ldots,k_t$ 使得 $m_i^{k_i}\in(t)$. 令 $k=\max_{1\le i\le t}\{k_i\}$ 即有 $\mathfrak{m}^k\subseteq(t)$, 至此我们证明了断言. 我们不妨假设 $n\in\mathbb{N}$ 使得 $\mathfrak{m}^n\subseteq(t)$, 但是 $\mathfrak{m}^{n-1}\not\subset(t)$. 如果 $n=1$, 那么我们已经证明了 $\mathfrak{m}=(t)$, 从而是主理想; 如果 $n>1$, 那么存在 $a\in\mathfrak{m}^{n-1}\subset\mathfrak{m}$ 但是 $a\notin(t)$. 令 $b=a/t$, 那么 $b\notin R$, 否则 $a=bt\in(t)$ 相矛盾, 从而根据 R 是正规的可知 b 不在 R 上整, 我们断言 $b\mathfrak{m}\not\subseteq\mathfrak{m}$, 从而 $b\mathfrak{m}=(1)$, 进而 $\mathfrak{m}=(1/b)$ 是主理想.

现在来证明 (3) $\Rightarrow$ (2): 不妨假设 $\mathfrak{m}=(\pi)$, 我们断言 $\bigcap_{k\ge0}\mathfrak{m}^k=\{0\}$. 如果存在 $0\neq a\in\cap_{k\ge0}\mathfrak{m}^k$, 我们记 $a=b_k\pi^k$, 其中 $b_k\in R$. 从而 $b_k\pi^k=b_{k+1}\pi^{k+1}$, 由于 R 是整环从而 $b_k=b_{k+1}\pi$, 即 $(b_k)\subseteq(b_{k+1})$. 由于 R 是诺特的可知存在足够大的 n 使得 $(b_n)=(b_{n+1})$, 从而存在 R 中的单位 u 使得 $b_n=b_{n+1}u$, 从而 $b_n=b_{n+1}\pi=b_{n+1}u$, 从而 $\pi=u$, 相矛盾, 从而证明了我们的断言. 现在任取非零理想 I, 令 $n\in\mathbb{N}$ 满足 $I\subseteq\mathfrak{m}^n$ 但 $I\not\subseteq\mathfrak{m}^{n+1}$. 取 $a\in I$ 使得 $a\notin\mathfrak{m}^{n+1}$, 不妨将其写成 $a=\pi^n u$, 如果 $u\in\mathfrak{m}$, 那么 $a\in\mathfrak{m}$; 如果 $u\notin\mathfrak{m}$, 从而是单位, 从而依然有 $a\in\mathfrak{m}$, 因此 $I=\mathfrak{m}^n$.

现在来证明 (2) $\Rightarrow$ (1): 对于 $a\in R$, 如果 $(a)\subseteq(\pi^n)$ 并且 $(a)\not\subset(\pi^{n+1})$, 则定义 $\nu(a)=n$, 并且定义 $\nu(a/b)=\nu(a)-\nu(b)$, 可以直接验证 ν 给出了 R 的分式域 K 上的一个赋值, 并且使得 $R=\{a\in K^\times\mid\nu(a)\ge0\}$, 即 R 是离散赋值环.

根据命题11.1.8可知 (1) $\Rightarrow$ (5) 成立. 对于 (5) $\Rightarrow$ (3), 假设 $\mathfrak{m}$ 不是主理想, 根据中山正引理可知 $\mathfrak{m}^2\neq\mathfrak{m}$, 从而存在 $\pi\in\mathfrak{m}$ 使得 $\pi\notin\mathfrak{m}^2$, 从而 $(\pi)\subseteq\mathfrak{m}$ 但是 $(\pi)\not\subset\mathfrak{m}^2$. 但是 $(\pi)=\mathfrak{m}^k$ 对某个 $k\in\mathbb{N}$ 成立, 从而 k 只能等于 1, 即 $\mathfrak{m}=(\pi)$ 是主理想. □

11.3 Serre 判据

定理 11.3.1. *令 R 是一个诺特整环, R 是正规环当且仅当如下两条成立:*

(1) *对任意余一维的素理想 $\mathfrak{p}$, $R_\mathfrak{p}$ 是离散赋值环.*

(2) *$R=\bigcap R_\mathfrak{p}$, 其中取交运算取遍所有余一维的素理想.*

我们不加证明地引用, 证明 Serre 判据时会用到的, 关于准素分解的事实.

命题 11.3.2. *令 R 是诺特环, M 是 R-模, $a\in M$, 则 $a=0$ 当且仅当: a 在 M_p 中成为 0 元素, 其中 p 是任意一个, 成为 M 中某个元素零化子的素理想.*

证明: 我们首先证明上述两个性质能够推出 R 的正规性. 首先我们宣称: 设 R 是一个整环, K 是 R 的分式域, 对于包含 R 且含于 K 的一族正规环 R_i, 它们的交 $\cap R_i$ 仍然是的正规环. 首先注意到:$\cap R_i$ 也是具有分式域 K 的整环. 设 $a\in K$ 在 $\cap R_i$ 上整, 则 a 在 R_i 上整, 对任意 i 成立, 于是由于 R_i 的正规性, $a\in R_i$ 对所有 i 成立, 即 $a\in\cap R_i$, $\cap R_i$ 正规. 注意到条件中的 $\mathfrak{p}$, $R_\mathfrak{p}$ 是包含 R, 并且含于 R 分式域的一族离散赋值环, 于是它们都是正规环. 根据上述引理, R 作为这一族正规环的交, 也是正规环.

接下来我们证明正规性推出第一个性质. 我们只需要注意到以下该事实成立. 令 B 是一个交换环, 而 A 是 B 的子环, C 是 A 在 B 中的整闭包, 若 S 是 A 中的乘法封闭集, 那么 $A[S^{-1}]$ 具有 $C[S^{-1}]$ 作为其在 $B[S^{-1}]$ 中的整闭包. 一方面, 我们发现 $C[S^{-1}]$ 在 $A[S^{-1}]$ 上整, 这是因为 $\forall\alpha=a/s\in C[S^{-1}]$, 其中 $a\in C,s\in S$, 有

$$A[S^{-1}][\alpha]=A[S^{-1}][a]=A[a][S^{-1}]$$

由于 a 在 A 上整, 所以 $A[a]$ 是有限 A-模, 于是 $A[a][S^{-1}]=A[S^{-1}][\alpha]$ 是有限 $A[S^{-1}]$-模, 这等价于 α 在 $A[S^{-1}]$ 上整. 另一方面, 设 $b/s\in B[S^{-1}]$ 在 $A[S^{-1}]$ 上整, 则存在 $a_0/s_0,\dots,a_{n-1}/s_{n-1}\in A[S^{-1}]$, 使得

$$(\frac{b}{s})^n+\frac{a_{n-1}}{s_{n-1}}(\frac{b}{s})^{n-1}+\cdots+\frac{a_1}{s_1}\frac{b}{s}+\frac{a_0}{s_0}=0$$

在两边同时乘以 $s^ns_0\dots s_{n-1}$, 有

$$b^n+a_{n-1}ss_0\dots s_{n-2}+\cdots+a_0s^nss_1\dots s_{n-1}=0$$

从而 b 在 A 上整, 即 $b\in C$, $b/s\in C[S^{-1}]$. 令 $A=R$, $S=R-\mathfrak{p}$, 其中 $\mathfrak{p}$ 是 R 的任意素理想, 又有 $C=R$, 知 $R_{\mathfrak{p}}$ 正规, 特别地，事情在 $\mathfrak{p}$ 为余一维时也是成立的.

最后, 利用之前承认的事实, 我们证明正规性能推出第二个性质. 首先, 任取 $a/u\in K(R)$, 如果 $a/u\notin R$, 则有 $a\notin(u)$. 对 $R/(u)$ 应用证明前举出的事实, 我们能找到一个素理想 $\mathfrak{p}$, 满足它是 $R/(u)$ 中某个元素的零化子, 而 $0\neq a\in(R/(u))_{\mathfrak{p}}=R_{\mathfrak{p}}/(u)_{\mathfrak{p}}$, 也就是说: $a\notin(u)_{\mathfrak{p}}\subset R_{\mathfrak{p}}$. 如果 $a/u\in R_{\mathfrak{p}}$, 则 $a/u=b/s$, 对于某些 $b\in R$, $s\in R-\mathfrak{p}$ 成立. 这将导致 $a=b/su\in(u)_{\mathfrak{p}}$, 这与 $\mathfrak{p}$ 的选取矛盾, 于是 $a/u\notin R_{\mathfrak{p}}$. 于是有

$$R=\bigcap R_{\mathfrak{p}}$$

其中 $\mathfrak{p}$ 历遍了满足如下条件的素理想: $\mathfrak{p}$ 是 $R/(u)$ 中某个元素的零化子, (u) 是由 $u\in R$ 生成的主理想.

接下来我们证明这样的 $\mathfrak{p}$, 一定具有余维数 1, 从而完成我们的整个证明. 利用局部化时素理想的对应关系, 我们只要证明 $\mathfrak{p}_{\mathfrak{p}}$ 在 $R_{\mathfrak{p}}$ 中是一个主理想. 而必要的时候进行局部化, 我们不妨假设 R 是局部环, 而 $\mathfrak{p}$ 是 R 中那唯一的极大理想. 令 $\mathfrak{p}$ 是 $R/(a)$ 中 b 的零化子, 考虑 $\mathfrak{p}^{-1}=r\in K(R)|r\mathfrak{p}\in R$. 我们有 $\mathfrak{p}\subset\mathfrak{p}^{-1}\mathfrak{p}\subset R$. 所以或者 $\mathfrak{p}\mathfrak{p}^{-1}=\mathfrak{p}$, 或者 $\mathfrak{p}\mathfrak{p}^{-1}=R$. 如果 $\mathfrak{p}\mathfrak{p}^{-1}=\mathfrak{p}$, 利用哈密顿-凯莱定理, 我们有 $\forall r\in\mathfrak{p}^{-1}$, r 在 $\mathfrak{p}$ 上整. 利用 R 的正规性, 有 $\mathfrak{p}^{-1}=R$. 但 $b\mathfrak{p}\subset(a)$, 故而 $b/a\in\mathfrak{p}^{-1}=R$, 这导致 $b\in(a)$, 矛盾. 于是 $\mathfrak{p}^{-1}\mathfrak{p}=R$, 则对于某个 $r\in\mathfrak{p}^{-1}$, $r\mathfrak{p}=R$, 否则 $\mathfrak{p}^{-1}\mathfrak{p}\subset\sum_{r\in\mathfrak{p}^{-1}}r\mathfrak{p}\subset\sum_{r\in\mathfrak{p}^{-1}}\mathfrak{p}\subset\mathfrak{p}$, 矛盾. 从而 $\mathfrak{p}=r^{-1}R$, 是一个主理想. 这就完成了证明. □

11.4 戴得金整环

定义 11.4.1. 一个**戴得金整环** (Dedekind domain)是一个正规的维数为一的诺特整环.

例子. 上个学期, 我们已经看到, $\mathbb{Z}[\sqrt{-5}]$ 是 $\mathbb{Q}[\sqrt{-5}]$ 的整数环. 代数数论中的定理将告诉我们, 所有 $\mathbb{Q}$ 的有限扩张的整数环, 都是戴德金整环. 于是 $\mathbb{Z}[\sqrt{-5}]$ 关于任何一个素理想的局部化, 都是一个离散赋值环, 特别地，它们都是主理想整环. 然而, 就 $\mathbb{Z}[\sqrt{-5}]$ 自身而言, 它甚至不是唯一分解整环, 因此, 局部唯一分解, 或者局部是主理想整环, 并不能推出整体是唯一分解整环或主理想整环.

注记. 给定戴德金整环 R, 任取素理想 $\mathfrak{p}$, 由于局部化与整闭包交换, 从而 $R_{\mathfrak{p}}$ 是一个诺特局部整环, 并且维数为一, 从而是离散赋值环, 其赋值记为 $\nu_{\mathfrak{p}}$.

定理 11.4.2. *给定戴德金整环 R, 任取理想 $0\neq I\subseteq R$, 存在唯一的分解*

$$I=\mathfrak{p}_1^{n_1}\dots\mathfrak{p}_k^{n_k}$$

其中 $\mathfrak{p}_i$ 是互不相同的包含 I 的素理想, 并且 $IR_{\mathfrak{p}_i} \subseteq R_{\mathfrak{p}_i}$ 是主理想, n_i 等于 $R_{\mathfrak{p}_i}$ 的赋值在这个主理想的生成元上的取值.

为了定理的证明, 我们先介绍一个引理.

引理 11.4.3. 令 M 是 R-模, N_1, N_2 是 M 的子模, 则 $N_1 = N_2$ 当且仅当: 对 R 中所有极大理想 $\mathfrak{m}$, 有

$$(N_1)_\mathfrak{m} = (N_2)_\mathfrak{m} \in (M)_\mathfrak{m}$$

证明: 只有充分性需要证明: 首先, 直接比较元素, 我们有

$$(N_1)_\mathfrak{m} + (N_2)_\mathfrak{m} = (N_1 + N_2)_\mathfrak{m}$$

我们有短正合列:

$$0 \xrightarrow{f} N_1 \longrightarrow N_1 + N_2 \longrightarrow \operatorname{coker} f \longrightarrow 0$$

其中 f 是自然嵌入. 注意到

$$(\operatorname{coker} f)_\mathfrak{m} = \operatorname{coker}(f_\mathfrak{m}) = \frac{(N_1 + N_2)_\mathfrak{m}}{(N_1)_\mathfrak{m}} = \frac{(N_1+)_\mathfrak{m} + (N_2)_\mathfrak{m}}{(N_1)_\mathfrak{m}} = \frac{(N_2)_\mathfrak{m}}{(N_1)_\mathfrak{m}} = 0$$

这里 $\mathfrak{m}$ 取遍所有 R 的极大理想. 于是 $\operatorname{coker} f = 0$, $N_1 = N_1 + N_2 = N_2$. □

下面我们来证明戴德金整环中，理想的唯一分解定理.

证明: 依据上面的引理, 我们只要证明对于 R 中的非零素理想 $\mathfrak{p}$, 有

$$I_\mathfrak{p} = (\mathfrak{p}_1^{n_1} \dots \mathfrak{p}_k^{n_k})_\mathfrak{p}$$

如果 $I \subset \mathfrak{p}$, 则依据假设, $\mathfrak{p} = \mathfrak{p}_i$，对于某个指标 i 成立. 于是

$$I_\mathfrak{p} = I_{\mathfrak{p}_i} = IR_{\mathfrak{p}_i} = \mathfrak{p}_i^{n_i}$$

对某个正整数 n_i 成立. 而最后一个等号是因为 $R_{\mathfrak{p}_i}$ 是一个离散赋值环. 而由于各个 $\mathfrak{p}_i$ 没有包含关系, 有

$$(\mathfrak{p}_1^{n_1} \dots \mathfrak{p}_k^{n_k})_{\mathfrak{p}_i} = \mathfrak{p}_i^{n_i}$$

如果 $I \not\subset \mathfrak{p}$, 则两边取局部化后, 都成为单位理想, 于是定理的等式成立.

而分解的唯一性, 只需要回忆 n_i 的选取方式就可以得知. □

索引