

域与 Galois 理论笔记

魔法少女 Alkali

最后编译: 2023 年 6 月 2 日

0 前言

这份笔记是笔者学习 Fields 奖得主 Richard Borcherds 所讲授的网课 *Galois Theory* (链接: [YouTube](#) 或 [bilibili](#)) 时记录的笔记. 原始的笔记是英文的, 但笔者思考之后决定还是使用中文整理出最终的笔记.

这份笔记不是网课的逐字稿, Borcherds 教授所讲的内容中有些部分没有被记录下来 (例如正十七边形的具体构造), 也有一些教授略过的部分被详细地补充 (例如任意集合的分裂域的同构延拓定理). 更多地, 这份笔记被整理成了笔者心目中适合自己与他人阅读的模样. 因此, 这份笔记便不可避免地带有了笔者的个人色彩, 从而许多地方的讲法与证明并不一定是最好的. 更为致命的是, 本份笔记是作者为备考中科院 2023 年“代数与数论”暑期学校而突击整理的笔记 (虽然应该没有办法在考前整理出来), 因此错误应当俯拾即是, 所以还盼望读者指正.

联系我可以通过[我的邮箱](#).

本笔记用到的参考文献

- [1] Emil Artin. *Galois theory*. second. Edited and with a supplemental chapter by Arthur N. Milgram. Dover Publications, Inc., Mineola, NY, 1998, pp. iv+82. ISBN: 0-486-62342-4.

- [2] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*. Second. Vol. 84. Graduate Texts in Mathematics. Springer-Verlag, New York, 1990, pp. xiv+389. ISBN: 0-387-97329-X. DOI: [10.1007/978-1-4757-2103-4](https://doi.org/10.1007/978-1-4757-2103-4).
- [3] Serge Lang. *Algebra*. third. Vol. 211. Graduate Texts in Mathematics. Springer-Verlag, New York, 2002, pp. xvi+914. ISBN: 0-387-95385-X. DOI: [10.1007/978-1-4613-0041-0](https://doi.org/10.1007/978-1-4613-0041-0).
- [4] Serge Lvovski. *Principles of complex analysis*. Vol. 6. Moscow Lectures. Translated from the 2017 Russian original by Natalia Tsilevich. Springer, Cham, 2020, pp. xiii+257. ISBN: 978-3-030-59364-3; 978-3-030-59365-0. DOI: [10.1007/978-3-030-59365-0](https://doi.org/10.1007/978-3-030-59365-0).
- [5] Patrick Morandi. *Field and Galois theory*. Vol. 167. Graduate Texts in Mathematics. Springer-Verlag, New York, 1996, pp. xvi+281. ISBN: 0-387-94753-1. DOI: [10.1007/978-1-4612-4040-2](https://doi.org/10.1007/978-1-4612-4040-2).
- [6] Jean-Pierre Serre. *Local fields*. Vol. 67. Graduate Texts in Mathematics. Translated from the French by Marvin Jay Greenberg. Springer-Verlag, New York-Berlin, 1979, pp. viii+241. ISBN: 0-387-90424-7.
- [7] 章璞. 伽罗瓦理论——天才的激情. 高等教育出版社, 2013.

1 域扩张

我们先给出域扩张的定义.

定义 1.1. 设 K, L 是域, 且满足 $K \subset L$, 那么称 L 是 K 的一个**扩域**, 记作 L/K .

例 1.2. 我们最熟悉的扩域的例子是 $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

定义 1.3. 设有域扩张 L/K .

1. 定义扩张的**度数**为 $[L : K] = \dim_K L$, 当 $[L : K] < \infty$ 时, 称 L/K 为**有限扩张**;

2. 设 $\alpha \in L$, 如果 α 是某个多项式 $p(x) \in K[x]$ 的根, 那么称 α 在 K 上是代数的, 否则称为是超越的;
3. 设 α 是 K 上的代数元, 设 $p(x) \in K[x]$ 是 α 的极小多项式, 即以 α 为根的次数最低的多项式, 那么定义 α 的度数 $\deg \alpha = \deg p(x)$.

例 1.4. 我们给出一些域扩张的例子.

1. 对 $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, 有 $[\mathbb{C} : \mathbb{R}] = 2, [\mathbb{R} : \mathbb{Q}] = \infty$. (具体而言, $[\mathbb{R} : \mathbb{Q}] = 2^{\aleph_0}$)
2. 取 $K = \mathbb{Q}$, 那么 $\alpha = \sqrt[5]{2}$ 是代数的, $\pi, e \in \mathbb{R}$ 是超越的.
3. 对 $\mathbb{Q} \subset \mathbb{Q}(x)$, 即 \mathbb{Q} 上的有理函数域作为 \mathbb{Q} 的扩域, x 在 \mathbb{Q} 上是超越的.
4. $\alpha = \cos(2\pi/7)$ 是代数的. 注意到对 $\zeta = e^{2\pi/7}$, 有 $\alpha = (\zeta + \zeta^{-1})/2$. 而

$$\begin{aligned}
 1 + \zeta + \cdots + \zeta^6 &= 0 \implies \zeta^{-3} + \zeta^{-2} + \cdots + 1 + \cdots + \zeta^3 = 0 \\
 &\implies (2\alpha)^3 + (2\alpha)^2 - 2(2\alpha) - 1 = 0 \\
 &\iff 8\alpha^3 + 4\alpha - 4\alpha - 1 = 0
 \end{aligned}$$

所以 α 是 \mathbb{Q} 上的代数元.

记号 1.5. 对 L/K 及集合 $S \subset L$, 我们记 $K(S)$ 为包含 S 中所有元素的最小的扩域, 并称为由 S 生成的扩域. 特别地, 当 $S = \{\alpha_1, \dots, \alpha_n\}$ 时, 我们记 $K(S) = K(\alpha_1, \dots, \alpha_n)$.

考虑由单个代数元 α 生成的扩域, 我们有如下的引理

引理 1.6. 设 $L/K, \alpha \in L$ 是 K 上的代数元, 有极小多项式 $m(x) \in K[x]$, 那么 $K(\alpha) \simeq K[x]/\langle m(x) \rangle$, 其中 $\langle m(x) \rangle$ 是 $p(x)$ 生成的理想.

证明. 定义同态

$$\begin{aligned}
 \varphi : K[x] &\rightarrow K(\alpha) \\
 p(x) &\mapsto p(\alpha)
 \end{aligned}$$

考虑核 $\ker \varphi$, 显然 $\ker \varphi \neq K[x]$, 且极小多项式 $m(x) \in \ker \varphi$. 由于 $K[x]$ 是主理想整环, $\ker \varphi$ 单生成, 且生成元整除 $m(x)$. 但容易证明 $m(x)$ 是不可约多项式, 结合 $\ker \varphi \neq K[x]$ 可知生成元与 $m(x)$ 相伴, 从而 $\ker \varphi = \langle m(x) \rangle$. 由第一同构定理即知

$$K(\alpha) \simeq \frac{K[x]}{\langle m(x) \rangle} \quad \square$$

关于有限扩张与代数扩张,有如下的结论

定理 1.7. 设有域扩张 M/K , $\alpha \in M$ 是 K 上的代数元当且仅当 α 包含在 K 的一个有限扩张中.

证明. 一方面, 假设 α 是代数元, 那么 $\alpha \in K(\alpha)$. 设 $\deg \alpha = n$, 那么 $1, \alpha, \dots, \alpha^{n-1}$ 是 $K(\alpha)$ 的一组基, $K(\alpha)/K$ 是有限扩张. 另一方面, 假设 α 包含在 K 的有限扩张中, 不妨设 $[M:K] = n < \infty$. 那么 $1, \alpha, \dots, \alpha^{n-1}, \alpha^n$ 一定线性相关, 从而 α 是一个多项式的根, 是一个代数元. \square

定理 1.8 (望远镜公式). 设 $K \subset L \subset M$ 均为有限扩张, 那么有 $[M:K] = [M:L][L:K]$

证明. 设 x_1, \dots, x_m 是 L/K 的一组基, y_1, \dots, y_n 是 M/L 的一组基. 我们考虑 $\{x_i y_j\}_{(i,j) \in [m] \times [n]}$ ¹. 首先对 $a_{ij} \in K$ 及指标 $(i, j) \in R \times S \subset [m] \times [n]$ 有

$$\begin{aligned} \sum_{(i,j) \in R \times S} a_{ij}(x_i y_j) &= 0 \\ \implies \sum_{j \in S} a_{ij} y_j &= 0, \forall i \in R \\ \implies a_{ij} &= 0, \forall (i, j) \in R \times S \end{aligned}$$

所以 $x_i y_j$ 线性无关. 其次, 显然 M 中的每个元素可以表示为 $x_i y_j$ 的 K -线性组合, 所以 $\{x_i y_j\}_{(i,j) \in [m] \times [n]}$ 是 M/L 的一组基. 从而命题得证. \square

通过望远镜公式, 我们可以证明

定理 1.9. 设 α, β 是 K 上的代数元, 那么 $\alpha \pm \beta, \alpha\beta, \alpha/\beta (\beta \neq 0)$ 均为 K 上的代数元.

证明. 考虑扩张链 $K \subset K(\alpha) \subset K(\alpha, \beta)$, 两个扩张均为代数扩张, 所以都是有限扩张. 由定理 1.8, $K(\alpha, \beta)/K$ 是代数扩张. 而 $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ 均包含在 $K(\alpha, \beta)$ 中, 所以都是代数元. \square

¹ $[m] = \{1, \dots, m\}$, 组合数学中的常用记号.

定理 1.10. 设 α 是一个由 K 上代数元系数构成的多项式的根, 那么 α 是代数的.

证明. 设

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$$

且 a_{n-1}, \cdots, a_0 均为 K 上代数元. 考虑域扩张链

$$\begin{aligned} K &\subset K(a_0) \\ &\subset K(a_0, a_1) \\ &\cdots \\ &\subset K(a_0, \cdots, a_{n-1}) \\ &\subset K(a_0, \cdots, a_{n-1}, \alpha) \end{aligned}$$

前 n 步扩张每一步都是添加一个代数元 a_i , 所以都是有限的, 因此 K 上的扩域 $K(a_0, \cdots, a_{n-1})$ 是有限的. 而由假设, α 在 $K(a_0, \cdots, a_{n-1})$ 上代数, 所以最后一步扩张也是有限的. 因此扩张 $K(a_0, \cdots, a_{n-1}, \alpha)/K$ 是有限的, 从而 α 是 K 上代数元. \square

推论 1.11. 假设 $E/L, L/K$ 均为代数扩张, 那么 E/K 也是代数扩张.

而关于超越元, 我们已知 e, π 在 \mathbb{Q} 上是超越的, 但是有如下的公开问题

问题. $e + \pi, e\pi$ 在有理数域上超越吗?

不过我们可以有这样的结论

命题 1.12. $e + \pi, e\pi$ 至多有一个是代数的.

证明. 否则 $e + \pi, e\pi$ 都是代数的, 由定理 1.10 可知方程

$$x^2 - (e + \pi)x + e\pi = 0 \tag{1}$$

的根是代数的. 但方程 (1) 的根是 e 和 π , 这与我们已知的 e 与 π 的超越性矛盾. \square

2 分裂域

给定一个域 K 及 K 上的多项式 $p(x) \in K[x]$, 我们希望找到一个扩域 L/K 使得 $p(x)$ 在 L 上“有所有的根”. 给“有根”这一点以严格的定义, 我们便得到了**分裂域**的概念:

定义 2.1. 设 K 是域, $p(x) \in K[x]$, 如果扩域 L/K 使得 $p(x)$ 在 L 上可以分解为一次因式的乘积 (简称为**分裂**)

$$p(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

且 $L = K(\alpha_1, \dots, \alpha_n)$, 那么称 L 是 $p(x)$ 在 K 上的**分裂域**.

在证明分裂域的存在性与唯一性之前, 我们先给出一些分裂域的例子.

例 2.2. 给定底域 K , 讨论多项式 $p(x) \in K[x]$.

1. $p(x) = x - a_0$, $a_0 \in K$, 那么分裂域就是 K .
2. $p(x) = x^2 - a_1x + a_0$, $a_1, a_0 \in K$, 且 $p(x)$ 不可约. 那么 $L = K[x]/\langle p(x) \rangle$ 包含了 $p(x)$ 的一个根 α , 而事实上, L 也包含了另一个根 $a_1 - \alpha$. 所以 L 是 $p(x)$ 的一个分裂域.
3. 取 $K = \mathbb{Q}$ 及 $p(x) = x^3 - 2$. $L = \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[x]/\langle x^3 - 2 \rangle$ 包含了 $\sqrt[3]{2}$, 但不包含 $x^3 - 2$ 的复根, 此时 $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$. 于是取 $M = L[y]/\langle y^2 + \sqrt[3]{2}y + \sqrt[3]{4} \rangle$, 则 M 是一个分裂域, 并且有 $[M : k] = 6$.
4. $p(x) = 8x^3 + 4x^2 - 4x - 1$.

我们现在证明分裂域的存在性.

证明. 给定域 K 及 $p = p_1 p_2 \cdots p_m \in K[x]$, 其中 p_i ($i = 1, \dots, m$) 均不可约. 我们对 $\deg p$ 用归纳法. 当 $\deg p = 1$ 时, K 本身就是 $p(x)$ 的分裂域. 假设对 $\deg p = n - 1$ 成立. 对 $\deg p = n$, 考虑域 $K_1 = K[x]/\langle p_1(x) \rangle$, 那么 p 在 K_1 上至少有一个根 α , p 在 K_1 上可以分解为

$$p(x) = (x - \alpha)p_a(x)$$

对 $p_a(x)$ 用归纳假设, 存在扩域 L/K_1 使得 $p_a(x)$ 分裂为一次因式的乘积, 从而在扩域 L/K 上 $p(x)$ 分裂为一次因式的乘积. 由归纳原理得证. \square

我们着手证明分裂域的同构唯一性. 我们把这个命题加强为分裂域作为域扩张是同构唯一的, 即对域 K 及分裂域 L, L' , 有如下的图表交换

$$\begin{array}{ccc} L & \xrightarrow{\sim} & L' \\ & \nwarrow \quad \nearrow & \\ & K & \end{array}$$

定理 2.3 (分裂域的同构唯一性). 设 K 是域, $p(x) \in K[x]$, 域 K' 与 K 同构, 且 $p(x)$ 在同构映射下的像为 $p'(x)$. 设 L, L' 分别是 $p(x), p'(x)$ 的分裂域, 那么存在同构 $L \rightarrow L'$ 使得以下图表交换

$$\begin{array}{ccc} L & \xrightarrow{\sim} & L' \\ \uparrow & & \uparrow \\ K & \xrightarrow{\sim} & K' \end{array}$$

证明. 设 $i: K \xrightarrow{\sim} K'$ 是同构, 我们也用 i 表示延拓到 $K[x] \rightarrow K'[x]$ 的同构. 依然对 $p(x)$ 的次数用归纳法. $\deg p = 1$ 时, $K = L, K' = L'$, 命题显然成立. 假设命题对 $\deg p = n - 1$ 成立, 那么对 p 的某个不可约因子 p_1 , 有

$$K(\alpha) = \frac{K[x]}{\langle p(x) \rangle} \simeq \frac{K'[x]}{\langle i(p(x)) \rangle} = K(\alpha')$$

从而可以得到交换图

$$\begin{array}{ccc} K(\alpha) & \xrightarrow{\sim} & K'(\alpha') \\ \uparrow & & \uparrow \\ K & \xrightarrow{\sim} & K' \end{array}$$

而在 $K(\alpha), K'(\alpha')$ 上 $p(x), p'(x)$ 分别分解为一次因式与一个 $n - 1$ 次多项式的乘积, 从而按归纳假设, 可以得到两个 $n - 1$ 次多项式的分裂域的同构

$$\begin{array}{ccc} L & \xrightarrow{\sim} & L' \\ \uparrow & & \uparrow \\ K(\alpha) & \xrightarrow{\sim} & K'(\alpha') \end{array}$$

从而有大图表

$$\begin{array}{ccc}
 L & \xrightarrow{\sim} & L' \\
 \uparrow & & \uparrow \\
 K(\alpha) & \xrightarrow{\sim} & K'(\alpha') \\
 \uparrow & & \uparrow \\
 K & \xrightarrow{\sim} & K'
 \end{array}$$

交换, 即得到所欲证命题. □

评注 2.4. 需要注意到, 两个分裂域之间的同构不一定是唯一的. 例如分别使用 i, j 表示虚数单位, $x^2 + 1$ 在 \mathbb{R} 上的两个分裂域

$$\begin{array}{ccc}
 \mathbb{C} = \mathbb{R}(i) & \xrightarrow{h} & \mathbb{R}(j) \\
 & \nwarrow \quad \nearrow & \\
 & \mathbb{R} &
 \end{array}$$

其中 $h: \mathbb{R}(i) \rightarrow \mathbb{R}(j)$ 可以取为 $i \mapsto j$ 与 $i \mapsto -j$, 得到两个同构.

3 代数闭包

定义 3.1. 设 K 是一个域, 如果扩域 \overline{K}/K 满足

- (1) $K[x]$ 中的任意多项式在 \overline{K} 中均分裂;
- (2) \overline{K} 由 $K[x]$ 中多项式的根生成,

那么称 \overline{K} 是 K 的**代数闭包**.

我们给出代数闭包的构造.

定理 3.2. 任意域 K 均存在代数闭包.

引理 3.3. 设 L/K 是代数扩张, 那么有 $|L| \leq \max\{|K|, |\mathbb{N}|\}$.

证明. 我们有分解

$$L = \bigcup_{n \geq 1} \{\alpha \in L : \deg \alpha = n\}$$

而对每个 $\{\alpha \in L : \deg \alpha = n\}$ 中的元素 α , α 与另外至多 $n-1$ 个元素与 K 中 n 个系数决定的首一多项式对应, 从而有

$$\{\alpha \in L : \deg \alpha = n\} \subset [n] \times K^n$$

对无限的 K 而言, $|[n] \times K^n| = |K|$, 从而

$$\begin{aligned} |L| &= \left| \bigcup_{n \geq 1} \{\alpha \in L : \deg \alpha = n\} \right| \\ &\leq |\mathbb{N} \times K| \\ &= |K| \end{aligned}$$

对有限的 F 而言, $|[n] \times K^n| = n|K|^n \leq |\mathbb{N}|$, 此时

$$\begin{aligned} |L| &= \left| \bigcup_{n \geq 1} \{\alpha \in L : \deg \alpha = n\} \right| \\ &\leq |\mathbb{N} \times \mathbb{N}| \\ &= |\mathbb{N}| \end{aligned}$$

综上, 可以得到

$$|L| \leq \max\{|K|, |\mathbb{N}|\} \quad \square$$

代数闭包存在性的证明. 设 A 是 K 上所有代数扩域的集合. 取 S 满足 $F \subset S$ 且 $|S| > \max\{|K|, |\mathbb{N}|\}$, 那么由引理, K 的代数扩张均包含在 S 中, 从而 $A \subset \mathcal{P}(S)$ 是一个集合. 使用包含关系作为偏序, 那么注意到对任意一条链 $c : (\{K_i\}, \subset)$, 易见 $\bigcup_{i \geq 1} K_i$ 是 c 的一个上界. 因此由 Zorn 引理, A 中存在极大元 M . 断言在 M 中任意 $p(x) \in K[x]$ 分裂. 否则假设存在一个 $p(x)$ 在 M 上不能分解为一次因式的乘积, 那么设 $p(x)$ 在 M 上具有分裂域 E , $E/M, M/K$ 都是代数扩张, 从而 E/K 是代数扩张 (推论 1.11), $E \in A$. 然而 $M \subsetneq E$, 这与 M 在 A 中的极大性矛盾. 因此 M 中任意 $p(x) \in K[x]$ 分裂, 取 M 的由 $K[x]$ 中所有多项式的根生成的子域 \overline{K} 即得到 K 的代数闭包. (证明中用到的集合论结论可以参考 [3, 附录 2 第 2, 3 节]) \square

关于代数闭包, 有一个密切相关的概念是代数闭域:

定义 3.4. 域 L 被称为是**代数闭域**, 如果 $L[x]$ 中的任意多项式都在 L 中有根.

命题 3.5. 域 K 的代数闭包 \overline{K} 是代数闭域.

证明. 设 $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $a_i \in \overline{K}$. 由于 \overline{K} 由 $K[x]$ 中多项式的根生成, 因此 a_i 均为 K 上的代数元. 对 $p(x)$ 在某个根 α , 考虑扩张链

$$K \subset K(a_0, \cdots, a_{n-1}) \subset K(a_0, \cdots, a_{n-1}, \alpha)$$

容易发现两个扩张都是有限的, 所以 α 也是 K 上的代数元, 从而在 \overline{K} 内. 因此 \overline{K} 是代数闭域. \square

我们接下来讨论一种弱于代数闭的性质. 我们希望找到一个扩域 L/K , 使得 L 在开根号下封闭.

构造. 想法是不断地添加平方根. 取 $K_0 = K$, K_1 为 K_0 上所有形如 $x^2 - a$, $a \in K_0$ 的多项式的分裂域 (它包含在 K_0 的一个代数闭包中, 所以存在). 递归地定义 K_{n+1} 为 K_n 上所有形如 $x^2 - b$, $b \in K_n$ 的多项式的分裂域. 取 $L = \bigcup_{n \in \mathbb{N}} K_n$, 那么容易验证 L 是一个域; 同时对任意 $\alpha \in L$, 存在某个 K_i 使得 $\alpha \in K_i$, 那么 α 的平方根按定义在 $K_{i+1} \subset L$ 中. 因此 L 关于开根号封闭. \square

接下来我们给出一些代数闭包的例子.

例 3.6. 我们最熟悉的代数闭包莫过于 \mathbb{R} 的代数闭包 \mathbb{C} . 这个结论被称为代数基本定理. 在之后我们会利用 Galois 理论证明代数基本定理, 但是比较简单的方法是利用复分析中的 Liouville 定理或者卷绕数. 对这些证明, 可以参考 [4, 命题 8.13].

其他的一些“自然”的代数闭包的例子有

例 3.7. 1. \mathbb{C}/\mathbb{R} ;

2. 有理数的代数闭包 $\overline{\mathbb{Q}} \subset \mathbb{C}$, 称为代数数.

3. 考虑形式 Laurent 级数 $\mathbb{C}[[x]][x^{-1}]$, 它的代数闭包被称为 Puiseux 级数, 即

$$\bigcup_{n \geq 1} \mathbb{C}[[x^{1/n}]] [x^{-1/n}]$$

证明参考 [6, 命题 II.8].

现在我们证明代数闭包的同构唯一性. 我们证明一个更强的命题

定理 3.8 (同构延拓定理). 设 K 是一个域, $S \subset K[x]$ 是一族多项式, K' 与 K 同构且 S 在同构映射下的像为 S' . 设 E, E' 分别是 S, S' 的分裂域, 那么存在同构 $S \rightarrow S'$ 使得下图交换

$$\begin{array}{ccc} S & \xrightarrow{\sim} & S' \\ \uparrow & & \uparrow \\ K & \xrightarrow{\sim} & K \end{array}$$

证明. 设 A 是由子域与嵌入 (F, τ) 构成的集合, 其中 $K \subset F \subset E$ 且使得下图交换

$$\begin{array}{ccccc} & E' & & & \\ & \uparrow \sigma & \nwarrow \tau & & \\ K & \longrightarrow & F & \longrightarrow & E \end{array}$$

我们在 A 上定义偏序 $(F, \tau) \prec (F', \tau')$ 当且仅当 $F \subset F'$ 且 $\tau'|_F = \tau$. 对任意一条链 $\{(F_i, \tau_i)\}$, 取 $F = \bigcup_{i \geq 0} F_i$, $\tau: F \rightarrow E'$ 满足 $\tau|_{F_i} = \tau_i$. 那么容易验证 (F, τ) 是这条链的一个上界. 由 Zorn 引理, A 中存在一个极大元 $(M, \tilde{\sigma})$. 断言 $M = E$. 否则的话存在一个 S 中的多项式 $p(x)$ 在 M 上不分裂, 那么对 $p(x)$ 的一个根 α , 可以按下图延拓得到 $\tilde{\sigma}': M(\alpha) \rightarrow E'$

$$\begin{array}{ccccc} & & E' & & \\ & & \uparrow & & \\ M(\alpha) & \xrightarrow{\tilde{\sigma}_\alpha} & \tilde{\sigma}(M)(\alpha') & \xrightarrow{\tilde{\sigma}'} & E' \\ \uparrow & & \uparrow & & \\ M & \xrightarrow{\tilde{\sigma}} & \tilde{\sigma}(M) & & \end{array}$$

这与 M 的极大性矛盾, 所以 $M = E$. 注意到 E 包含了 S 中所有多项式的根, 并被 $\tilde{\sigma}$ 一一地映到 E' 中. 而 E' 是包含 S' 中所有多项式的根的最小的域, 所以一定有 $\tilde{\sigma}(E) = E'$. 因此命题得证. \square

评注 3.9. 我们指出代数闭包间的同构也不是唯一的. 并且我们也无法“自然地”找出两个代数闭包之间的同构, 也就是说 \overline{K} 的**绝对 Galois 群**是没有单位元的. 这种情形与拓扑空间 X 中的道路的同伦类 $\pi_1(X)$ 相似: 我们可以定义道路的同伦类之间的乘法, 但是无法自然地找到单位元. 在这种情形下, 我们会把 $\text{Aut}(\overline{K}/K)$ 及 $\pi_1(X)$ 称为**群胚**. 在范畴论中, 群胚被定义为所有态射都是同构的范畴.

4 有限域

回忆整数到一个域 K 有一个自然的同态

$$\begin{aligned}\lambda: \mathbb{Z} &\rightarrow K \\ m &\mapsto m \cdot 1\end{aligned}$$

如果 $\ker \lambda = \mathbb{Z}$, 那么称 K 的**特征**为 0; 如果 $\ker \lambda = \langle n \rangle$, 那么称 K 的特征为 $n > 0$. 记 K 的特征为 $\text{char } K$. 容易证明, 当 $\text{char } K = 0$ 时, K 一定包含 \mathbb{Q} 作为子域; 当 $\text{char } K > 0$ 时, K 的特征一定是素数 (设为 p), 且包含 $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ 作为子域. 我们将 \mathbb{Q} 与 \mathbb{F}_p (p 素数) 称为**素域**.

假设 F 是有限域, 那么 F 一定有正的特征 $p > 0$. 那么此时素域 $\mathbb{F}_p \subset F$, F 是 \mathbb{F}_p 上的向量空间. 如果 $\dim_{\mathbb{F}_p} F = n$, 那么每个坐标分量有 p 种取法, 则 $|F| = p^n$. 因此我们得到

命题 4.1. 有限域 F 的阶为 p^n , 其中 $p = \text{char } F$ 是素数, $n = [F : \mathbb{F}_p]$.

相同的论证我们可以得到

命题 4.2. 有限域 $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ 当且仅当 $n|m$.

记号 4.3. 对素数 p , 在上下文意义明确时我们记它的一个方幂 $p^n := q$. 对 q 阶有限域, 我们将其记为 $\text{GF}(q) = \text{GF}(p^n) = \mathbb{F}_q = \mathbb{F}_{p^n}$.²

²似乎这需要先证明有限域是唯一的, 不过这件事情之后我们确实会做.

首先我们证明有限域的存在性.

定理 4.4. 对素数 p 及 $q = p^n$, 存在 q 阶有限域.

证明. 取 $x^q - x$ 在 \mathbb{F}_p 上的一个分裂域 L , 我们证明 L 恰好由 $x^q - x$ 的所有根构成. 我们先证明 $x^q - x$ 的根构成一个域. 对根 x, y , 由 $\text{char } L = p$ 可知 $\binom{q}{k} = 0$, $k = 1, \dots, q-1$, 从而

$$\begin{aligned}(x-y)^q &= x^q - y^q \quad (p=2 \text{ 时 } 1 = -1, \text{ 所以均写为减号}) \\ &= x - y\end{aligned}$$

所以 $x - y$ 是 $x^q - x$ 的一个根; 而当 $y \neq 0$ 时

$$\begin{aligned}\left(\frac{x}{y}\right)^q - \frac{x}{y} &= \frac{x^q y - x y^q}{y^{q+1}} \\ &= \frac{xy - yx}{y^{q+1}} \\ &= 0\end{aligned}$$

所以 x/y 也是一个根. 因此 $x^q - x$ 的根在减法与除法下封闭, 构成一个域. 由于分裂域由根生成, 所以 L 恰好由 $x^q - x$ 的根构成. 另一方面, 由于 $(x^q - x)' = qx^{q-1} - 1 = -1$, 与 $x^q - x$ 互素, 所以 $x^q - x$ 没有重根. 因此 $|L| = \deg(x^q - x) = q$. \square

然后我们证明有限域的唯一性.

定理 4.5. 两个有限域同构当且仅当它们阶数相同.

证明. 设有限域 F 的阶数为 q , 我们证明 F 一定是 $x^q - x$ 的分裂域. 这只需要证明对任意 $a \in F$ 有 $a^q = a$ 即可. $a = 0$ 时这是平凡的. 对 $a \in F^*$, 由 Lagrange 定理, $a^{|F^*|} = 1$, 即 $a^{q-1} = 1$, 从而 $a^q = a$. 因此 F 是 $x^q - x$ 的分裂域, 在同构意义下是唯一的. \square

对于给定的 q , 我们希望问

问题. 如何构造 q 阶有限域?

回答很简单, 我们取一个 n 次不可约多项式 $f(x) \in \mathbb{F}_p[x]$, 那么就有 $\text{GF}(q) = \mathbb{F}_p[x]/\langle f(x) \rangle$. 我们看一个例子.

例 4.6. 给定 $p = 2$. 我们写一些低次数的不可约多项式:

$$\begin{aligned} x, x+1, \\ x^2+x+1, \\ x^3+x+1, x^3+x^2+1, \\ x^4+x+1, x^4+x^3+x^2+x+1, x^4+x^3+1 \end{aligned}$$

那么我们有

- (1) 次数为 $4 = 2^2$: $\text{GF}(4) = \mathbb{F}_2[x]/\langle x^2+x+1 \rangle$, 习惯上把 x 记为三次单位根 ω , 域中的元素为

$$0, 1, \omega, \omega+1$$

- (2) 次数为 $8 = 2^3$: $\text{GF}(8) = \mathbb{F}_2[x]/\langle x^3+x+1 \rangle$, 此时域中的元素为

$$0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$$

同时也有 $\text{GF}(8) = \mathbb{F}_2[y]/\langle y^3+y^2+1 \rangle$, 这两种构造下的域应当是同构的. 事实上, 注意到 $(y+1)^3 + (y+1) + 1 = 0$, 所以同构映射可以由 $x = y+1$ 给出.

通过以上这个例子, 我们可以看出确实没有“典范”的构造有限域的方法.

最后, 我们讨论求有限域上不可约多项式的个数的问题. 我们只在有限素域上考虑这个问题.

命题 4.7. 设 $F_d(x)$ 是 \mathbb{F}_p 上所有 d 次不可约多项式的乘积, 那么有

$$x^{p^n} - x = \prod_{d|n} F_d(x)$$

引理 4.8. $\mathbb{F}_p[x]$ 中的不可约多项式均没有重根.

证明. 设 $f(x) \in \mathbb{F}_p[x]$ 不可约. 如果 $f'(x) \neq 0$, 那么 $(f(x), f'(x)) = 1$, 从而 $f(x)$ 没有重根. 如果 $f'(x) = 0$, 那么 $f(x)$ 一定具有形式 (不妨设首一)

$$\begin{aligned} f(x) &= x^{np} + a_{n-1}x^{(n-1)p} + \cdots + a_1x^p + a_0 \\ &= (x^n + a_{n-1}x^{n-1} + \cdots + a_0)^p \end{aligned}$$

与 $f(x)$ 不可约矛盾. 所以 $f(x)$ 没有重根. \square

命题 4.7 的证明. 首先我们说明如果次数至少为 1 的多项式 $f(x)|x^{p^n} - x$, 那么 $f^2(x) \nmid x^{p^n} - x$. 事实上如果有 $x^{p^n} - x = f^2(x)g(x)$, 那么计算形式导数有

$$-1 = 2f(x)f'(x)g(x) + f^2(x)g'(x)$$

从而 $f(x)|1$, 矛盾. 其次我们说明 $f(x)|x^{p^n} - x$ 当且仅当 $d = \deg f(x)|n$. 设 L 是 $x^{p^n} - x$ 的分裂域, 即 $\text{GF}(p^n)$. 对 $f(x)$ 的一个根 α , 考虑 $\mathbb{F}_p(\alpha)$. 那么 $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = d$, 由命题 4.2, $\mathbb{F}_p(\alpha) \subset L$ 当且仅当 $d|n$, 即 $x - \alpha|x^{p^n} - x$ 当且仅当 $d|n$. 因此 $f(x)|x^{p^n} - x$ 时一定有 $x - \alpha|x^{p^n} - x$, 从而 $d|n$; $d|n$ 时 $f(x)$ (在 L 上) 的所有根 α, β, \dots 满足 $x - \alpha, x - \beta, \dots$ 均整除 $x^{p^n} - x$, 又因为 $f(x)$ 没有重根, 这些一次因式两两互素, 有 $f(x)|x^{p^n} - x$. 综上可知命题成立. \square

对命题 4.7 使用 Möbius 变换 ([2, 第 2 章定理 2]), 我们可以得到

定理 4.9. $\mathbb{F}_p[x]$ 上 n 次不可约多项式的个数为

$$\frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$$

推论 4.10. 对任意正整数 n , $\mathbb{F}_p[x]$ 中存在 n 次不可约多项式.

证明. n 次不可约多项式的个数为 $n^{-1}(p^n \pm \cdots + p\mu(n))$, 括号中的式子被 p 恰整除 (即 p^2 不整除这个式子), 所以一定不是 0. \square

5 正规扩张与可分扩张

对于一个代数扩张 L/K 及 K 上的一个多项式 $p(x) \in K[x]$, 假设 L 中包含了 $p(x)$ 的一个根. 那么我们会问, L 包含了 $p(x)$ 的所有根吗? 看以下两个例子.

例 5.1. 取底域为 \mathbb{Q} .

- (1) $p(x) = x^3 - 2$ 在 $\mathbb{Q}(\sqrt[3]{2})$ 上有一个根, 但是 $\mathbb{Q}(\sqrt[3]{2})$ 不包含 $x^3 - 2$ 的复根;
- (2) $p(x) = 8x^3 + 4x^2 + 4x - 1$, 取 $\alpha = \cos 2\pi/7$, 那么 α 是 $p(x)$ 的一个根. 而 $p(x)$ 的另外两个根为 $\cos 4\pi/7 = 2\alpha^2 - 1$, $\cos 6\pi/7 = 2(2\alpha^2 - 1)^2 - 1$, 均在 $\mathbb{Q}(\alpha)$ 中.

以下我们给出关于代数扩张的三个等价命题, 每一个命题都可以用来描述正规扩张.

定理 5.2. 设 $K \subset L$ 是代数扩张, 那么以下三个命题等价:

- (1) $K[x]$ 中任何在 L 上有根的多项式 $p(x)$ 在 $L[x]$ 中分裂;
- (2) L 是 K 上某一族多项式的分裂域;
- (3) \overline{K} 的所有固定 K 不动的自同构都将 L 映为 L .

定义 5.3. 满足定理 5.2 中三个等价条件中任意一个的代数扩张称为正规扩张.

定理 5.2 的证明. 我们按照 $(1) \implies (2) \implies (3) \implies (1)$ 的顺序证明它们等价.

$(1) \implies (2)$: 对任意 $\alpha \in L$, 由于 L/K 是代数扩张, 因此可以取 α 在 K 上的极小多项式 $p_\alpha(x)$, 那么 L 是 $S = \{p_\alpha \in K[x] : \alpha \in L\}$ 的分裂域.

$(2) \implies (3)$: 设 L 是 $S \subset K[x]$ 的分裂域, $\sigma \in \text{Aut } \overline{K}$ 固定 K 不动. 那么 σ 也固定 S 中多项式的系数不动, 从而 S 中多项式的根也被固定不动. 而 L 是 S 中多项式的根的分裂域, 所以也被固定不动.

$(3) \implies (1)$: 设 $p(x) \in K[x]$ 具有一个根 $\alpha \in L$, 不妨设 $p(x)$ 不可约. 设 $\beta \in \overline{K}$ 是 $p(x)$ 的另一个根, 由于 $p(x)$ 不可约, 所以存在固定 K 不动的同构

$K(\alpha) \rightarrow K(\beta)$. 按照同构延拓定理 (定理 3.8), 这个同构可以延拓为 \overline{K} 的同构 $\sigma: \overline{K} \rightarrow \overline{K}$

$$\begin{array}{ccccc} K & \longrightarrow & K(\alpha) & \longrightarrow & \overline{K} \\ \downarrow = & & \downarrow \sim & & \downarrow \sigma \\ K & \longrightarrow & K(\beta) & \longrightarrow & \overline{K} \end{array}$$

那么按照假设, σ 将 L 中的 α 映成 L 中的 β , 即 $\beta \in L$. 从而 $p(x)$ 的根均在 L 中, $p(x)$ 在 $L[x]$ 中分裂. \square

例 5.4. 我们再看几个例子.

- (1) 我们在前面知道了 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 不是正规的, 但 $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ 是正规的.
- (2) 如果 $K \subset L$ 且 $[L:K] = 2$, 那么 L/K 一定是正规的: L 一定是单生成的, 否则存在三个 K -线性无关的元素 $1, \alpha, \beta$, 矛盾. 那么设 $L = K(\alpha)$, 由于 $[L:K] = 2$, α 的极小多项式是二次的, 不妨设为 $x^2 + bx + c$. 从而极小多项式的另一个根为 $-b - \alpha \in L$, 所以极小多项式在 $L[x]$ 中分裂, L/K 是正规的.
- (3) 假设 $L/K, M/L$ 都是正规扩张, 那么 M/K 是正规扩张吗? 答案是否定的, 一个简单的例子是 $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$.

接下来我们给出可分多项式, 可分元及可分扩张的定义.

定义 5.5. 设 K 是域, $f(x) \in K[x]$, 如果 $f(x)$ 在 \overline{K} 中没有重根, 那么称 $f(x)$ 是一个**可分多项式**. 如果 $K \subset L, \alpha \in L$ 是一个可分多项式的根, 那么称 α 是**可分元**. 如果 L/K 中每个元素都是可分的, 那么称 L/K 是**可分扩张**.

可分多项式的一个简单的判别法是

命题 5.6. $f(x) \in K[x]$ 是可分多项式当且仅当它的形式导数 $f'(x)$ 与其互素.

证明. 设 α 是 $f(x)$ 的一个根, 那么 $f(x)$ (在分裂域或者代数闭包上) 有分解

$$f(x) = (x - \alpha)^{n_1} f_1(x), \quad f_1(\alpha) \neq 0$$

当 $n_1 \geq 2$ 时, 求导有

$$f'(x) = n_1(x - \alpha)^{n_1-1} f_1(x) + (x - \alpha)^{n_1} f_1'(x)$$

仍被 $x - \alpha$ 整除, 从而 $x - \alpha \mid (f, f')$, 两者不互素. 当 $n_1 = 1$ 时, 求导的结果为

$$f'(x) = f_1(x) + (x - \alpha)^{n_1} f_1'(x)$$

此时 $f'(\alpha) = f_1(\alpha) \neq 0$, 从而 $x - \alpha \nmid f'(x)$. 那么当 f 可分时, f 的任意根都不是 f' 的根, 从而 $(f, f') = 1$. \square

例 5.7. 我们给出一些可分或不可分扩张的例子.

- (1) 设 $K \subset L$ 是代数扩张, $\text{char } K = 0$, 那么 L 是可分扩张. 事实上, 对任意 $\alpha \in L$, 取 α 在 K 上的极小多项式 $f(x)$, 那么 $f(x)$ 在 K 上是不可约的. 从而对非零的 $f'(x)$ 一定有 $(f, f') = 1$, 即 α 的极小多项式可分, α 是可分元.
- (2) 而当 $\text{char } K > 0$ 时, K 的代数扩张不一定是可分的. 因为此时 $f'(x)$ 可以是 0, 比如 $f(x) = a_n x^{np} + a_{n-1} x^{(n-1)p} + \cdots + a_0$. 具体地举一个例子, 设 k 是一个特征 p 的域, 取 $K = k(t^p), L = k(t)$, 其中 t 是 k 上的超越元. 那么 L/K 是有限扩张, 从而是代数的. 但 t 不是可分元: t 在 K 上具有极小多项式 $x^p - t^p$, 但 $x^p - t^p = (x - t)^p$ 只有一个根.
- (3) 有限域的代数扩张都是可分的. 事实上设 α 是 \mathbb{F}_q 上的代数元, 设其是 n 次的, 那么 $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = n$. 从而 α 是多项式 $f(x) = x^{q^n} - x$ 的根, 而 $f'(x) = -1$, 与 $f(x)$ 互素, 从而 $f(x)$ 可分, 则 α 可分.

而对于不可分扩张, 最极端的情况是如下定义的纯不可分扩张

定义 5.8. 设 $K \subset L$, $\text{char } K = p$, 如果对任意 $\alpha \in L$, α 都是 K 上某个多项式 $x^{p^n} - a$ 的根, 那么称 L/K 是**纯不可分扩张**.

对一般的代数扩张, 我们有如下命题

定理 5.9. 设 L/K 是代数扩张, 那么 L/K 可以分解为 $K \subset K^{\text{sep}} \subset L$, 使得 K^{sep}/K 是可分扩张, L/K^{sep} 是纯不可分扩张. K^{sep} 称为 K 的**可分闭包**.

由于本笔记中只处理可分扩张, 所以这个命题的证明我们直接引用 [3, 第 V 章, 命题 6.6]