# 域与 Galois 理论笔记

魔法少女 Alkali

最后编译: 2023 年 5 月 28 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和他人阅读的模样. 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] 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.

[3] 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.

[4] 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.

[5] 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 $\alpha$ 是某个多项式 $p(x) \in K[x]$ 的根, 那么称 $\alpha$ 在 $K$ 上是**代数**的, 否则称为是**超越**的;
3. 设 $\alpha$ 是 $K$ 上的代数元, 设 $p(x) \in K[x]$ 是 $\alpha$ 的极小多项式, 即以 $\alpha$ 为根的次数最低的多项式, 那么定义 $\alpha$ 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 $\alpha$ 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 $S = \{\alpha_1, \cdots, \alpha_n\}$ 时, 我们记 $K(S) = K(\alpha_1, \cdots, \alpha_n)$.

考虑由单个代数元 $\alpha$ 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

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

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

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

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 $\alpha$ 包含在 $K$ 的一个有限扩张中.*

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

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

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

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 $\{x_i y_j\}_{(i,j)\subset[m]\times[n]}$ 是 $M/L$ 的一组基. 从而命题得证. □

通过望远镜公式, 我们可以证明

**定理 1.9.** 设 $\alpha, \beta$ 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. □

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

证明. 设

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

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

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, $\alpha$ 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 $\alpha$ 是 $K$ 上代数元. □

而关于超越元, 我们已知 $e,\pi$ 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 1.11.** *$e+\pi, e\pi$ 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 $\pi$, 这与我们已知的 $e$ 与 $\pi$ 的超越性矛盾. □

# 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 $L = K(\alpha_1, \cdots, \alpha_n)$, 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. $p(x) = x^2 - a_1 x + a_0$, $a_1, a_0 \in K$, 且 $p(x)$ 不可约. 那么 $L = K[x]/\langle p(x) \rangle$ 包含了 $p(x)$ 的一个根 $\alpha$, 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 $M = L[y]/\langle y^2 + \sqrt[3]{2}y + \sqrt[3]{4}$, 则 $M$ 是一个分裂域, 并且有 $[M : k] = 6$.
4. $p(x) = 8x^3 + 4x^2 - 4x - 1$.

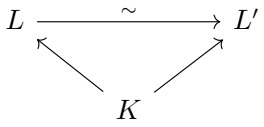
我们现在证明分裂域的存在性.

证明. 给定域 $K$ 及 $p = p_1 p_2 \cdots p_m \in K[x]$, 其中 $p_i$ $(i = 1, \cdots, m)$ 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 $\alpha$, $p$ 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. □

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



**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 $L \to L'$ 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 $K[x] \to K'[x]$ 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

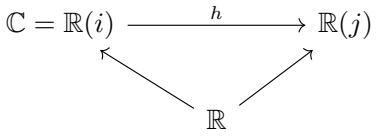
$$\begin{array}{ccc} L & \xrightarrow{\sim} & L' \\ \uparrow & & \uparrow \\ K(\alpha) & \xrightarrow{\sim} & K'(\alpha') \end{array}$$

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




其中 $h : \mathbb{R}(i) \to \mathbb{R}(j)$ 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.*

*证明.* 使用良序定理 ([2, 附录 2, 定理 4.1]) 在 $K[x]$ 上赋予良序 $(K[x], \prec)$. 对任意一条链 $c : p_1 \prec p_2 \prec \cdots$, 我们取 $K_0 = K$, $K_1$ 为 $p_1$ 在 $K_0$ 上的分裂域, $K_2$ 为 $p_2$ 在 $K_1$ 上的分裂域, 得到域扩张链

$$F_c : K_0 \subset K_1 \subset K_2 \subset \cdots$$

考虑 $K^c = \bigcup_{i\in\mathbb{N}} K_i$, 那么 $K^c$ 是 $F_c$ 的上界, 并且 $K^c$ 恰好包含了 $c$ 中所有多项式的根. 取 $X$ 是每一条链 $F_c$ 与 $K^c$ 的集合, 那么由 Zorn 引理 ([2, 附录 2 第 2 节]), $X$ 中存在极大元 $\overline{K}$. 一方面, 任意 $p(x) \in K[x]$ 都在 $\overline{K}$ 中分裂, 否则具有 $p(x)$ 的一个根 $\alpha$ 使得 $\overline{K} \subsetneq \overline{K}(\alpha)$, 与 $\overline{K}$ 的极大性矛盾. 另一方面, $X$ 中没有添加 $K[x]$ 中多项式的根以外的元素, 所以 $\overline{K}$ 恰好由 $K[x]$ 中多项式的根生成. 因此 $\overline{K}$ 就是 $K$ 的代数闭包. □

关于代数闭包, 有一个密切相关的概念是代数闭域:

**定义 3.3.** 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 3.4.** *域 $K$ 的代数闭包 $\overline{K}$ 是代数闭域.*