域与 Galois 理论笔记

魔法少女 Alkali

最后编译: 2023 年 5 月 26 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] 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.

[2] 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.

[3] 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 $S = \{\alpha_1, \cdots, \alpha_n\}$ 时, 我们记 $K(S) = K(\alpha_1, \cdots, \alpha_n)$.

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

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

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 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 $1, \alpha, \cdots, \alpha^{n-1}$ 是 $K(\alpha)$ 的一组基, $K(\alpha)/K$ 是有限扩张. 另一方面, 假设 α 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 α 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 $\{x_iy_j\}_{(i,j)\subset[m]\times[n]}$[1]. 首先对 $a_{ij}\in K$ 及指标 $(i,j)\in R\times S\subset[m]\times[n]$ 有

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

所以 x_iy_j 线性无关. 其次, 显然 M 中的每个元素可以表示为 x_iy_j 的 K–线性组合, 所以 $\{x_iy_j\}_{(i,j)\subset[m]\times[n]}$ 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 α,β 是 K 上的代数元, 那么 $\alpha\pm\beta,\alpha\beta,\alpha/\beta(\beta\neq0)$ 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 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

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

[1] $[m]=\{1,\cdots,m\}$, 组合数学中的常用记号.

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. □

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