Contents

1

Galois 理论

1.1 域扩张

首先回顾关于环同态的一个重要定理:

定理 1.1. 环 $R \subseteq S$ 是两个有相同单位元的环，任取 $u \in S$，那么环同态 $\sigma : R \to S$ 诱导出一个同态 $\sigma_u : R[x] \to S$，满足 $\sigma_u(x) = u$ 以及 $\sigma_u|_R = \sigma$.

证明直接验证同态的条件即可. 该定理的重要性在于: 如果我们取 σ 为单位映射, 即对于 $a \in R$ 有 $\sigma(a) = a$, 那么对于 $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$, 有

$$\sigma_u(f(x)) = a_0 + a_1u + \cdots + a_nu^n,$$

此时 σ_u 也叫 $R[x]$ 的求值同态, 看上去就像将 x 替换成了 u, 得到一个值 $f(u) \in S$. 使用同态基本定理, 那么 $R[x]/\ker\sigma_u \simeq R[u]$, $R[u]$ 表示 S 中包含 R 和 u 的最小的子环. 如果我们对 R 和 S 再限制一些条件, 比如令 R, S 都是域, 那么 $R[x]$ 是 PID, 所以 $\ker\sigma_u$ 是一个主理想, 此时就会有两种情况:

(1) $\ker\sigma_u = (0)$, 那么 $R[u] \simeq R[x]$ 是一个整环, 此时称 u 是 R 上的超越元.

(2) $\ker\sigma_u = (f(x))$, 那么 $R[u] \simeq R[x]/(f(x))$, 但是 $R[u]$ 作为域 S 的子环, 必然也是一个整环, 再结合 $R[x]$ 是 PID, 那么 $(f(x))$ 是一个素（极大）理想, 从而 $f(x)$ 是不可约多项式, 且 $R[u]$ 也是一个域, 此时称 u 是 R 上的代数元, 规定 $f(x)$ 首一, 称 $f(x)$ 是 u 在 R 上的极小多项式, 我们记为 $\min(R, u)$.

若 K 是域 F 的一个扩域, 对于 $\alpha \in K$, 我们记 $F(\alpha)$ 为 K 中包含 F 和 α 的最小的子域, 不难发现 $F(\alpha)$ 就是 $F[\alpha]$ 的分式域. 通过上面的叙述, 我们实际上证明了:

命题 1.2. 若 K 是域 F 的一个扩域，$\alpha \in K$ 是 F 上的代数元，那么

(1) 多项式 $\min(F, \alpha) \in F[x]$ 是不可约多项式.

(2) 若 $g(x) \in F[x]$，那么 $g(\alpha) = 0$ 当且仅当 $\min(F, \alpha)$ 整除 $g(x)$.

(3) $F(\alpha) = F[\alpha]$. 此外，若 $n = \deg(\min(F, \alpha))$，那么 $\{1, \alpha, \ldots, \alpha^{n-1}\}$ 组成了 F-向量空间 $F(\alpha)$ 的一组基，这表明 $[F(\alpha) : F] = n$.

Proof. 我们只需要证明 3 即可. 由于 $F[\alpha]$ 是域, 且同时包含 F 和 α, 所以 $F(\alpha) \subseteq F[\alpha]$. 另一方面, 根据域对运算的封闭性, 自然有 $F[\alpha] \subseteq F(\alpha)$. 所以 $F(\alpha) = F[\alpha]$.

要说明 $\{1, \alpha, \ldots, \alpha^{n-1}\}$ 是一组基, 即证明它们线性无关且张成 $F(\alpha) = F[\alpha]$. 任取 $f(\alpha) = a_0 + a_1\alpha + \cdots + a_m\alpha^m \in F[\alpha]$, 若 $m \geq n$, 记 $p(x) = \min(F, \alpha)$, 作带余除

法, 那么存在 $q(x), r(x) \in F[x]$ 且 $\deg r < \deg p = n$, 使得

$$f(x) = q(x)p(x) + r(x),$$

于是 $f(\alpha) = q(\alpha)p(\alpha) + r(\alpha) = r(\alpha) \in \operatorname{span}\{1, \alpha, \dots, \alpha^{n-1}\}$. 令

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} = 0, \quad c_i \in F.$$

那么 $h(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ 满足 $h(\alpha) = 0$, 所以 $p(x) \mid h(x)$, 但是 $\deg p > \deg h$, 所以 $h(x) = 0$, 即 $c_i = 0$, 所以 $\{1, \alpha, \dots, \alpha^{n-1}\}$ 线性无关. □

K 是域 F 的一个扩域, 令 $\alpha_1, \dots, \alpha_n \in K$, 我们定义 $F[\alpha_1, \dots, \alpha_n]$ 和 $F(\alpha_1, \dots, \alpha_n)$ 分别为 K 的包含 F 和 $\alpha_1, \dots, \alpha_n$ 的最小的子环和子域. 此时 $F(\alpha_1, \dots, \alpha_n)$ 依然是 $F[\alpha_1, \dots, \alpha_n]$ 的分式域.

更一般地, 令 $X \subseteq K$ 是任意子集, 定义 $F(X)$ 为 K 的包含 F 和 X 的最小子域, 我们称 $F(X)$ 是 **由 F 和 X 生成的子域**. 同样的, 定义 $F[X]$ 为 K 的包含 F 和 X 的最小子环, 我们称 $F[x]$ 是 **由 F 和 X 生成的子环**. 对于任意域扩张 K/F, 总是有 $K = F(K)$, 所以 K 总是由 F 和 K 的某个子集生成. 对于 $F(X)$, 我们可以有如下刻画:

命题 1.3. *K 是域 F 的一个扩域, $X \subseteq K$ 是任意子集. 如果 $\alpha \in F(X)$, 那么存在一些 $a_1, \dots, a_n \in X$ 使得 $\alpha \in F(a_1, \dots, a_n)$. 因此,*

$$F(X) = \bigcup \{F(a_1, \dots, a_n) \mid a_1, \dots, a_n \in X\},$$

其中并集取遍 X 的所有有限子集.

Proof. 记 $S = \bigcup \{F(a_1, \dots, a_n) \mid a_1, \dots, a_n \in X\}$, 由于每个 $F(a_1, \dots, a_n) \subseteq F(X)$, 所以 $S \subseteq F(X)$. 显然 S 包含 F 和 X, 如果我们能证明 S 是一个域, 那么根据 $F(X)$ 的最小性, 就有 $F(X) \subseteq S$, 从而推出 $F(X) = S$. 现在我们证明 S 确实是一个域. 任取 $\alpha, \beta \in S$, 那么存在 $a_1, \dots, a_n \in X$ 和 $b_1, \dots, b_m \in X$, 使得 $\alpha \in F(a_1, \dots, a_n)$ 以及 $\beta \in F(b_1, \dots, b_m)$. 此时 $\alpha, \beta \in F(a_1, \dots, a_n, b_1, \dots, b_m)$, 所以 $\alpha \pm \beta, \alpha\beta$ 和 α/β 都在 S 中, 故 S 是域. □

定义 1.4. *K 是域 F 的一个扩域, 如果每个 $\alpha \in K$ 都是 F 上的代数元, 即存在一个非零多项式 $f(x) \in F[x]$ 在 K 中满足 $f(\alpha) = 0$, 那么我们说 K/F 是代数扩张, 否则称 K/F 是超越扩张. 如果 K 作为 F-向量空间是有限维的, 那么我们称 K/F 是有限扩张.*

由于 π 不是任何有理系数多项式的零点, 所以 $\mathbb{Q}(\pi)/\mathbb{Q}$ 是超越扩张. 由于 $\sqrt{2}$ 是多项式 $x^2 - 2 \in \mathbb{Q}[x]$ 的零点, 所以 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 是有限扩张. 由于 $x^2 - 2$ 在 $\mathbb{Q}$ 上不可约, 根据 命题 1.2, 所以 $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

例 1.5. 这是一个有限扩张的非平凡的有趣的例子. 令 k 是域, $K = k(t)$ 是有理函数域. 令 $u \in K$ 且 $u \notin k$, 记 $u = f(t)/g(t)$ 且 $\gcd(f(t), g(t)) = 1$, $F = k(u)$. 我们断言

$$[K : F] = \max\{\deg f, \deg g\}.$$

注意到 $K = k(t) = F(t)$, 于是我们需要确定 t 在 F 上的最小多项式. 考虑多项式 $p(x) = ug(x) - f(x) \in F[x]$, 那么 $p(t) = 0$. 这表明 t 是 F 上的代数元. 首先, 我们说明 $p(x)$ 的次数是 $\max\{\deg f, \deg g\}$. 设 $f(t) = \sum_{i=0}^{n} a_i t^i$ 以及 $g(t) = \sum_{i=0}^{m} b_i t^i$, 那么 $m = n$ 时 $p(x)$ 的最高次项为 $(ub_n - a_n)x^n$, 由于 $u \notin k$, 所以 $(ub_n - a_n)x^n \neq 0$, 所以 $\deg p = m = n$. 这就表明 $p(x)$ 的次数就是 $\max\{\deg f, \deg g\}$.

然后, 我们证明 $p(x) \in k(u)[x]$ 不可约即可. u 在 k 上不可能是代数的, 否则 $[K : k] = [K : k(u)][k(u) : k] < \infty$, 这是不可能的. 这表明 $k[u]$ 同构于 $k[x]$. 于是 p 既可以视为 x 的多项式, 也可以视为 u 的多项式. p 视为 u 的多项式是 1 次的, 所以 p 是 $k(x)$ 上的不可约多项式. 又因为 $\gcd(f(x), g(x)) = 1$, 所以 $p \in k(x)[u]$ 是本原多项式, 所以 p 是 $k[x][u] = k[u][x]$ 中的不可约多项式. 于是 p 是 $k(u)$ 上的不可约多项式, 即 $\min(F, t) = p(x)$.

接下来我们证明如果 K/F 是有限扩张, 那么 K 在 F 上是有限生成的, 即存在 $\alpha_1, \ldots, \alpha_n \in K$ 使得 $K = F(\alpha_1, \ldots, \alpha_n)$.

命题 1.6. 若 K/F 是有限扩张, 那么 K 在 F 上是有限生成的且 K/F 是代数扩张.

Proof. 设 $[K : F] = n$, 也就是说存在 $\alpha_1, \ldots, \alpha_n \in K$, 使得其成为 K 的一组基, 由于 K 中的任意元素都可以唯一地表示成 $\alpha_1, \ldots, \alpha_n$ 的 F-线性组合, 所以 $K = F(\alpha_1, \ldots, \alpha_n)$, 这就证明了第一句话. 任取 $\alpha \in K$, 那么 $n + 1$ 个向量 $1, \alpha, \ldots, \alpha^n$ 一定 F-线性相关, 即存在不全为零的 $c_i \in F$, 使得 $c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0$, 这表明 α 是多项式 $c_0 + c_1 x + \cdots c_n x^n$ 的根, 即 α 在 F 上代数, 从而 K/F 是代数扩张. □

结合 命题 1.2, 该命题告诉我们 $\alpha \in K$ 在 F 上代数当且仅当 $[F(\alpha) : F] < \infty$, 这是后面我们判断一个元素是否为代数元的主要方法.

该命题的逆命题也成立: 若 K/F 是代数扩张且 $K = F(\alpha_1, \ldots, \alpha_n)$, 那么 K/F 是有限扩张. 为了证明这一点, 我们需要说明 $[K : F]$ 有限, 根据 命题 1.2, 我们知道当 α 是 F 上的代数元的时候, $F(\alpha)/F$ 是有限的, 注意到 $F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2)$, 所以我们需要考虑 $F \subseteq L \subseteq K$ 的时候, K/F 有限和 $K/L, L/F$ 有限的关系.

命题 1.7. 若 $F \subseteq L \subseteq K$, 那么 K/F 是有限扩张当且仅当 $K/L, L/F$ 都是有限扩张, 并且

$$[K : F] = [K : L][L : F].$$

Proof. 设 $\{\alpha_i\}_{1 \le i \le m}$ 是 L/F 的一组基, $\{\beta_j\}_{1 \le j \le n}$ 是 K/L 的一组基, 我们证明 $\{\alpha_i\beta_j\}$ 是 K/F 的一组基. 设 $\sum_j \sum_i c_{ij}\alpha_i\beta_j = 0, c_{ij} \in F$, 先对 j 求和, 由于 $\{\beta_j\}$ L-线性无关, 所以对于每个 j 有 $\sum_i c_{ij}\alpha_i = 0$, 又因为 $\{\alpha_i\}$ F-线性无关, 所以 $c_{ij} = 0$. 任取 $x \in K$, 那么 x 可以表示成 $\{\beta_j\}$ 的 L-线性组合, 每一项系数又可以表示成 $\{\alpha_i\}$ 的 F-线性组合, 所以 x 可以表示成 $\{\alpha_i\beta_j\}$ 的 F-线性组合, 即 $\{\alpha_i\beta_j\}$ 张成 K. □

命题 1.8. K/F 是域扩张, 若 $\alpha_1, \ldots, \alpha_n \in K$ 都是 F 上的代数元且 $K = F(\alpha_1, \ldots, \alpha_n)$, 那么 $F[\alpha_1, \ldots, \alpha_n] = F(\alpha_1, \ldots, \alpha_n)$ 且

$$[K : F] \le \prod_{i=1}^{n} [F(\alpha_i) : F].$$

这表明 $[K:F]$ 是有限扩张.

Proof. 对 n 归纳. $n=1$ 的时候, 根据 命题 1.2, 结论成立. 假设结论在 $n-1$ 的时候成立, 对于 n 的时候, 记 $L=F(\alpha_1,\dots,\alpha_{n-1})$, 根据假设 $F(\alpha_1,\dots,\alpha_{n-1})=F[\alpha_1,\dots,\alpha_{n-1}]$, 此时 α_n 在 L 上代数, 所以 $K=L(\alpha_n)=L[\alpha_n]$. 在 $L[x]$ 中, 有 $\min(L,\alpha_n)\mid\min(F,\alpha_n)$, 所以 $[K:L]\le[F(\alpha_n):F]$, 再根据假设和 命题 1.7, 就有

$$[K:F]=[K:L][L:F]\le[F(\alpha_n):F]\prod_{i=1}^{n-1}[F(\alpha_i):F]=\prod_{i=1}^{n}[F(\alpha_i):F]. \qquad \square$$

定理 1.9. $F\subseteq L\subseteq K$, 如果 K/L 和 L/F 都是代数扩张, 那么 K/F 是代数扩张.

Proof. 任取 $\alpha\in K$, 那么 α 在 L 上是代数的, 设

$$\min(L,\alpha)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+x^n \quad a_i\in L,$$

考虑 $E=F(a_0,\dots,a_{n-1})$, 由于 a_i 在 F 上代数, 根据 命题 1.8, 所以 E/F 是有限扩张, 又因为 α 是 E 上多项式的一个根, 所以 $E(\alpha)/E$ 是有限扩张, 所以

$$[E(\alpha):F]=[E(\alpha):E][E:F]<\infty,$$

注意到 $F(\alpha)\subseteq E(\alpha)$, 所以 $F(\alpha)/F$ 是有限扩张, 即 α 是 F 上的代数元, 这就说明了 K/F 是代数扩张. $\square$

反过来, 如果 K/F 是代数扩张, 很容易说明 K/L 和 L/F 都是代数扩张. 所以, 对于本节中的概念, 如果有域塔 $F\subseteq L\subseteq K$, 那么:

- K/F 是代数扩张 $\Leftrightarrow$ $K/L, L/F$ 是代数扩张.
- K/F 是有限扩张 $\Leftrightarrow$ $K/L, L/F$ 是有限扩张.

接下来, 我们给出 $\alpha\in K$ 在 F 上代数当且仅当 $[F(\alpha):F]<\infty$ 的一个应用作为本节的结尾.

定义 1.10. 令 K/F 是一个域扩张. 定义集合

$$\{a\in K\mid a \text{ is algebraic over } F\}$$

为 F 在 K 中的**代数闭包**.

对于扩张 $\mathbb{C}/\mathbb{Q}$, $\mathbb{Q}$ 在 $\mathbb{C}$ 中的代数闭包被称为代数数域, 我们记为 $\mathbb{A}$, 下面我们证明 F 在 K 中的代数闭包确实是一个域, 这意味着其是 K 中 F 的最大的代数扩域.

命题 1.11. 令 K/F 是一个域扩张, L 是 F 在 K 中的代数闭包, 那么 L 是一个域, 因此 L 是 K 中 F 的最大的代数扩域.

Proof. 任取 $a,b\in L$, 那么 a,b 在 F 上代数, 所以 $F(a)/F$ 和 $F(b)/F$ 都是有限扩张, 根据 命题 1.8, 我们有

$$[F(a,b):F]\le[F(a):F][F(b):F]<\infty,$$

所以 $F(a,b)/F$ 是有限扩张, 从而是代数扩张, 而 $a\pm b, ab$ 和 a/b 都在 $F(a,b)$ 中, 所以 $a\pm b, ab$ 和 a/b 都在 L 中, 所以 L 确实是一个域. $\square$

问题

1. 令 K 是 F 的扩域, 证明 $[K:F]=1$ 当且仅当 $K=F$.

Proof. 若 $K=F$,那么 K 作为 F-向量空间有基 $\{1\}$,所以 $[K:F]=1$.若 $[K:F]=1$, 那么 K 作为 F-向量空间是 1 维的, 设 K 的基为 $\{\alpha\}$, 那么 $1\in K$ 满足 $1=a\alpha$, 其中 $a\in F$. 所以 $\alpha=a^{-1}\in F$, 故 $K=F$. □

2. 证明 $\mathbb{Q}(\sqrt{5},\sqrt{7})=\mathbb{Q}(\sqrt{5}+\sqrt{7})$.

Proof. 显然 $\mathbb{Q}(\sqrt{5}+\sqrt{7})\subseteq\mathbb{Q}(\sqrt{5},\sqrt{7})$. 设 $x=\sqrt{5}+\sqrt{7}$, 那么 $(x-\sqrt{7})^2=5$, 即 $x^2-2\sqrt{7}x+2=0$, 即

$$\sqrt{7}=\frac{x^2+2}{2x}\in\mathbb{Q}(\sqrt{5}+\sqrt{7}),$$

同理 $\sqrt{5}\in\mathbb{Q}(\sqrt{5}+\sqrt{7})$, 所以 $\mathbb{Q}(\sqrt{5},\sqrt{7})=\mathbb{Q}(\sqrt{5}+\sqrt{7})$. □

3. 验证下列多项式环的泛性质:

(1) 令 A 是包含域 F 的环. 如果 $a_1,\dots,a_n\in A$, 证明存在唯一的 F-环同态 $\varphi: F[x_1,\dots,x_n]\to A$ 使得 $\varphi(x_i)=a_i$.

(2) 此外, 假设 B 是包含 F 的环, 有一个函数 $f:\{x_1,\dots,x_n\}\to B$ 满足: 对于任意包含 F 的环 A 和 $a_1,\dots,a_n\in A$, 都存在唯一的 F-环同态 $\varphi: B\to A$ 满足 $\varphi(f(x_i))=a_i$. 证明 B 同构于 $F[x_1,\dots,x_n]$.

Proof. (1) 任取 $f(x_1,\dots,x_n)=\sum c_{i_1\dots i_n}x_1^{i_1}\cdots x_n^{i_n}\in F[x_1,\dots,x_n]$, 那么环同态 φ 必须满足

$$\varphi(f)=\sum c_{i_1\dots i_n}\varphi(x_1)^{i_1}\cdots\varphi(x_n)^{i_n},$$

所以 φ 的值由其在 $x_1,\dots,x_n$ 上的取值唯一确定.

(2) 根据 B 的性质, 对于 $x_1,\dots,x_n$, 存在唯一的 F-环同态 $\varphi: B\to F[x_1,\dots,x_n]$ 使得 $\varphi(f(x_i))=x_i$. 另一方面, 根据 (a), 对于 $f(x_1),\dots,f(x_n)\in B$, 存在唯一的 F-环同态 $\psi: F[x_1,\dots,x_n]\to B$ 使得 $\psi(x_i)=f(x_i)$.那么 $\varphi(\psi(x_i))=\varphi(f(x_i))=x_i$, 以及 $\psi(\varphi(f(x_i)))=\psi(x_i)=f(x_i)$. 由于恒等映射 $1_B: B\to B$ 也满足 $1_B(f(x_i))=f(x_i)$, 再根据 B 的性质, 就有 $\psi\circ\varphi=1_B$. 这就表明 φ,ψ 是同构. □

4. 令 A 是环. 如果 A 同时是 F-向量空间且对于任意 $\alpha\in F, a,b\in A$ 有 $\alpha(ab)=(\alpha a)b=a(\alpha b)$, 那么我们说 A 是一个 F-代数. 如果 A 是 F-代数, 证明 A 包含一个同构于 F 的子集. 此外, 证明: 如果 K/F 是域扩张, 那么 K 是一个 F-代数.

Proof. 令 $f: F\to A$ 为映射 $f(\alpha)=\alpha\cdot 1$, 那么 f 是线性映射. 此外, 由于 $f(\alpha\beta)=(\alpha\beta)\cdot 1=\alpha\cdot(\beta\cdot 1)=\alpha\cdot((\beta\cdot 1)1)=(\alpha\cdot 1)(\beta\cdot 1)=f(\alpha)f(\beta)$, 所以 f 是环同态. 这就表明 $f(F)$ 可以嵌入到 A 中.

若 $K\supseteq F$ 是扩域, 那么 K 中的乘法自然定义了 F 在 K 上的标量乘法, 所以 K 自然是一个 F-向量空间, 即成为一个 F-代数. □

5. 令 $K = F(a)$ 是 F 的有限扩张. 对于 $\alpha \in K$, 令 $L_\alpha : K \to K$ 是 $L_\alpha(x) = \alpha x$. 证明 L_α 是 F-线性变换. 此外, 证明 $\det(xI - L_a)$ 是 a 的最小多项式 $\min(F, a)$. 对于哪些 $\alpha \in K$ 有 $\det(xI - L_\alpha) = \min(F, \alpha)$?

Proof. L_α 是 F-线性变换直接验证即可. K/F 有基 $1, a, \dots, a^{n-1}$, $\min(F, a) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. 那么 L_a 在这组基下的表示矩阵为

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix},$$

不难证明 $\det(xI - L_a) = \min(F, a)$.

对于 $\alpha \in K$, 由于 $\det(xI - L_\alpha)$ 是 n 次多项式, 所以 $\min(F, \alpha)$ 也是 n 次多项式, 所以 $F(\alpha) = F(a)$. 所以 $\det(xI - L_\alpha) = \min(F, \alpha)$ 当且仅当 $F(\alpha) = F(a)$. □

6. 如果 K/F 是域扩张, $a \in K$ 使得 $[F(a) : F]$ 是奇数, 证明 $F(a) = F(a^2)$. 举出一个反例表明 $[F(a) : F]$ 是偶数的时候不成立.

Proof. 首先我们有 $F(a^2) \subseteq F(a)$. 考虑扩张 $F(a)/F(a^2)$, 那么 a 满足多项式 $x^2 - a^2 \in F(a^2)[x]$. 若 $x^2 - a^2$ 不可约, 那么 $[F(a) : F(a^2)] = 2 \mid [F(a) : F]$, 这与 $[F(a) : F]$ 矛盾, 所以 $[F(a) : F(a^2)] = 1$, 即 $F(a) = F(a^2)$.

反例考虑 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ 即可. □

7. 如果 K/F 是代数扩张, R 是 K 的子环且 $F \subseteq R \subseteq K$, 证明 R 是域.

Proof. 任取 $r \in R$, 设 r 满足

$$r^n + a_{n-1}r^{n-1} + \cdots + a_0 = 0, \quad a_i \in F,$$

那么

$$r^{-1} = -a_0^{-1}\left(r^{n-1} + a_{n-1}r^{n-2} + \cdots + a_1\right) \in R,$$

所以 R 是域. □

8. 证明 $\mathbb{Q}(\sqrt{2})$ 和 $\mathbb{Q}(\sqrt{3})$ 是 $\mathbb{Q}$-向量空间同构, 但是不是域同构.

Proof. $\mathbb{Q}(\sqrt{2})$ 和 $\mathbb{Q}(\sqrt{3})$ 都是 2 维的 $\mathbb{Q}$-向量空间, 自然是同构的. 设 $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$ 是域同构. 由于 $0 = (\sqrt{2})^2 - 2$, 所以

$$0 = \sigma(0) = \sigma(\sqrt{2})^2 - 2,$$

故 $\sigma(\sqrt{2}) = \pm\sqrt{2}$, 所以 $\sqrt{2} \in \mathbb{Q}(\sqrt{3})$. 设 $\sqrt{2} = a + b\sqrt{3}$, 那么 $2 - a^2 - 3b^2 = 2\sqrt{3}ab$. 这只可能 $a = 0$ 或者 $b = 0$. $a = 0$ 表明 $b = \sqrt{2/3} \notin \mathbb{Q}$, $b = 0$ 表明 $a = \sqrt{2} \notin \mathbb{Q}$, 矛盾. 所以不存在这样的域同构 σ. □

1.2 自同构

Galois 理论的核心思想在于将域扩张和群论联系起来. K, L 是域 F 的两个扩张, 一个 **F-同态** $\tau : K \to L$ 指的是一个环同态, 并且使得 $\tau|_F = \mathrm{id}$. 由于 τ 是从域出发的同态, 并且不是零映射, 所以 τ 必是单同态. 如果 τ 是同构, 那么称 τ 是 F-同构. $K \to K$ 的 F-同构被称为 F-自同构.

注意到 F-同态 $\tau : K \to L$ 同时是 F-线性映射, 所以如果 $[K : F] = [L : F] < \infty$ 的时候, 由于 τ 是单射, 所以 τ 必然是满射. 也就是说, 如果 K, L 都是 F 上的相同维数的有限维向量空间, 那么 F-同态 $\tau : K \to L$ 必然为 F-同构. 特别地, $K \to K$ 的 F-同态必为 F-自同构.

定义 1.12. K/F 是域扩张, 定义 K/F 的 **Galois 群**为 K 的所有 F-自同构构成的群, 记为 $\mathrm{Gal}(K/F)$.

引理 1.13. 令 $K = F(X)$, 那么 K 的 F-自同构完全由其在 X 上的行为决定, 更准确地说, 如果 $\sigma, \tau \in \mathrm{Gal}(K/F)$ 并且 $\sigma|_X = \tau|_X$, 那么 $\sigma = \tau$.

Proof. 任取 $\alpha \in K$, 根据 命题 1.3, 存在 $a_1, \dots, a_n \in X$ 使得 $\alpha \in F(a_1, \dots, a_n)$, 即存在 $f, g \in F[x_1, \dots, x_n]$ 使得 $\alpha = f(a_1, \dots, a_n)/g(a_1, \dots, a_n)$, 设

$$f(x_1, \dots, x_n) = \sum b_{i_1,\dots,i_n} x_1^{i_1} \cdots x_n^{i_n}, \quad g(x_1, \dots, x_n) = \sum c_{i_1,\dots,i_n} x_1^{i_1} \cdots x_n^{i_n},$$

其中 $b_{i_1,\dots,i_n}, c_{i_1,\dots,i_n} \in F$. 如果 $\sigma|_X = \tau|_X$, 那么

$$\begin{aligned}\sigma(\alpha) &= \frac{\sum \sigma(b_{i_1,\dots,i_n})\sigma(x_1)^{i_1} \cdots \sigma(x_n)^{i_n}}{\sum \sigma(c_{i_1,\dots,i_n})\sigma(x_1)^{i_1} \cdots \sigma(x_n)^{i_n}} \\ &= \frac{\sum b_{i_1,\dots,i_n}\tau(x_1)^{i_1} \cdots \tau(x_n)^{i_n}}{\sum c_{i_1,\dots,i_n}\tau(x_1)^{i_1} \cdots \tau(x_n)^{i_n}} \\ &= \tau(\alpha).\end{aligned}$$

□

引理 1.14. 令 $\tau : K \to L$ 是 F-同态, $\alpha \in K$ 是 F 上的代数元. 如果 $f(x) \in F[x]$ 使得 $f(\alpha) = 0$, 那么 $f(\tau(\alpha)) = 0$. 特别地, 若 $\tau \in \mathrm{Gal}(K/F)$, 那么 τ 一定是 $\min(F, \alpha)$ 的所有根的一个置换, 此外我们还有 $\min(F, \alpha) = \min(F, \tau(\alpha))$.

Proof. 设 $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$ 使得 $f(\alpha) = 0$, 那么

$$\begin{aligned}f(\tau(\alpha)) &= a_0 + a_1\tau(\alpha) + \cdots + a_n\tau(\alpha)^n \\ &= \tau(a_0 + a_1\alpha + \cdots + a_n\alpha^n) \\ &= \tau(f(\alpha)) = \tau(0) = 0.\end{aligned}$$

若 $\tau \in \mathrm{Gal}(K/F)$, 那么 $\tau(\alpha)$ 也是 $\min(F, \alpha)$ 的零点. 设 $p(x) = \min(F, \tau(\alpha))$, 那么有 $p(x) \mid \min(F, \alpha)$, 由于 $\min(F, \alpha)$ 是不可约多项式, 所以 $p(x) = \min(F, \alpha)$. □

推论 1.15. 如果 $[K : F] < \infty$, 那么 $|\mathrm{Gal}(K/F)| < \infty$.

Proof. $[K:F]<\infty$ 表明 $K=F(\alpha_1,\dots,\alpha_n)$，其中 $\alpha_1,\dots,\alpha_n$ 都是 F 上的代数元. 根据前面的两个引理，那么 $\tau\in\mathrm{Gal}(K/F)$ 完全由 $\tau(\alpha_i)$ 决定，而 $\tau(\alpha_i)$ 又只可能是 $\min(F,\alpha_i)$ 的零点，所以 $\tau(\alpha_i)$ 的取值只可能是有限个，故 τ 也只有有限种可能. □

令 K 是域，$S\subseteq\mathrm{Aut}(K)$ 是自同构群 $\mathrm{Aut}(K)$ 的子集，定义 S 的**不动域**为

$$\mathrm{Fix}(S)=\{\alpha\in K\mid\forall\tau\in S,\tau(\alpha)=\alpha\}.$$

不难验证 $\mathrm{Fix}(S)$ 确实是 K 的一个子域. 满足 $F\subseteq L\subseteq K$ 的域 L 被称为 K/F 的**中间域**，此时，如果 $S\subseteq\mathrm{Gal}(K/F)$，那么 $\mathrm{Fix}(S)$ 是 K/F 的中间域.

记 $\mathcal{L}$ 为 K 的所有子域的集合，$\mathcal{S}$ 为 $\mathrm{Aut}(K)$ 的所有子集的集合. 那么 Gal 可以视为 $\mathcal{L}\to\mathcal{S}$ 的映射，将 $L\subseteq K$ 送到 $\mathrm{Gal}(K/L)$. 反之，Fix 可以视为 $\mathcal{S}\to\mathcal{L}$ 的映射，将 $S\subseteq\mathrm{Aut}(K)$ 送到 $\mathrm{Fix}(S)$.

引理 1.16. *K 是一个域.*

(1) *如果 $L_1\subseteq L_2\subseteq K$，那么 $\mathrm{Gal}(K/L_1)\supseteq\mathrm{Gal}(K/L_2)$.*

(2) *如果 $S_1\subseteq S_2\subseteq\mathrm{Aut}(K)$，那么 $\mathrm{Fix}(S_1)\supseteq\mathrm{Fix}(S_2)$.*

(3) *如果 $L\subseteq K$，那么 $\mathrm{Fix}(\mathrm{Gal}(K/L))\supseteq L$.*

(4) *如果 $S\subseteq\mathrm{Aut}(K)$，那么 $\mathrm{Gal}(K/\mathrm{Fix}(S))\supseteq S$.*

(5) *如果 $L\subseteq K$，那么 $\mathrm{Gal}\big(K/\mathrm{Fix}(\mathrm{Gal}(K/L))\big)=\mathrm{Gal}(K/L)$. 也就是说，如果 $H<\mathrm{Aut}(K)$ 是 K 的某个子域 L 对应的 Galois 群，即存在 $L\subseteq K$ 使得 $H=\mathrm{Gal}(K/L)$，那么 $\mathrm{Gal}(K/\mathrm{Fix}(H))=H$.*

(6) *如果 $S\subseteq\mathrm{Aut}(K)$，那么 $\mathrm{Fix}\big(\mathrm{Gal}(K/\mathrm{Fix}(S))\big)=\mathrm{Fix}(S)$. 也就是说，如果 $L\subseteq K$ 是 $\mathrm{Aut}(K)$ 的某个子集对应的不动域，即存在 $S\subseteq\mathrm{Aut}(K)$ 使得 $L=\mathrm{Fix}(S)$，那么 $\mathrm{Fix}(\mathrm{Gal}(K/L))=L$.*

Proof. 前四点根据定义可以立即得到.

(5) 若 $H=\mathrm{Gal}(K/L)$，由 (4)，总是有 $\mathrm{Gal}(K/\mathrm{Fix}(H))\supseteq H$. 另一方面，我们有 $L\subseteq\mathrm{Fix}(\mathrm{Gal}(K/L))=\mathrm{Fix}(H)$，所以 $H=\mathrm{Gal}(K/L)\supseteq\mathrm{Gal}(K/\mathrm{Fix}(H))$.

(6) 若 $L=\mathrm{Fix}(S)$，由 (3)，总是有 $\mathrm{Fix}(\mathrm{Gal}(K/L))\supseteq L$. 另一方面，我们有 $S\subseteq\mathrm{Gal}(K/\mathrm{Fix}(S))=\mathrm{Gal}(K/L)$，所以 $L=\mathrm{Fix}(S)\supseteq\mathrm{Fix}(\mathrm{Gal}(K/L))$. □

推论 1.17. *记 $\mathcal{L}'$ 为 K 的子域的集合，满足 $L\in\mathcal{L}'$ 当且仅当存在子群 $H<\mathrm{Aut}(K)$ 使得 $L=\mathrm{Fix}(H)$. 记 $\mathcal{H}'$ 为 $\mathrm{Aut}(K)$ 的子群的集合，满足 $H\in\mathcal{H}'$ 当且仅当存在子域 $L\subseteq K$ 使得 $H=\mathrm{Gal}(K/L)$. 那么 $\mathcal{L}'$ 和 $\mathcal{H}'$ 之间存在一一对应，对应关系为 $L\mapsto\mathrm{Gal}(K/L)$，$\mathrm{Fix}(H)\mapsto H$.*

Proof. 由 引理 1.16 的 (5) 和 (6) 即得. □

推论 1.18. *K/F 是域扩张. 记 $\mathcal{L}'$ 为 K/L 的中间域的集合，满足 $L\in\mathcal{L}'$ 当且仅当存在子群 $H<\mathrm{Gal}(K/F)$ 使得 $L=\mathrm{Fix}(H)$. 记 $\mathcal{H}'$ 为 $\mathrm{Gal}(K/F)$ 的子群的集合，满足 $H\in\mathcal{H}'$ 当且仅当存在子中间域 $F\subseteq L\subseteq K$ 使得 $H=\mathrm{Gal}(K/L)$. 那么 $\mathcal{L}'$ 和 $\mathcal{H}'$ 之间存在一一对应，对应关系为 $L\mapsto\mathrm{Gal}(K/L)$，$\mathrm{Fix}(H)\mapsto H$.*

Proof. 由 引理 1.16 的 (5) 和 (6) 即得. □

若 K/F 是有限扩张, 推论 1.18 能否推广到一般的情况是后面重点研究的问题. 也就是说, 有没有一种域扩张 K/F, 使得 K/F 的所有中间域的集合 $\mathcal{L}$ 与 $\mathrm{Gal}(K/F)$ 的所有子群的集合 $\mathcal{H}$ 之间一一对应? 如果存在一一对应, 那么我们便可以将寻找中间域转化为寻找有限群的子群, 这通常要容易的多. Galois 理论的核心内容便在于研究这一类扩张. 现在, 我们可以通过两个例子来说明上面的情况可能存在也可能不存在.

例 1.19. 考虑 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. 根据 引理 1.13 和 引理 1.14, $\tau \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ 完全由 $\tau(\sqrt[3]{2})$ 确定, 并且 $\tau(\sqrt[3]{2})$ 为 $\min(\mathbb{Q}, \sqrt[3]{2}) = x^3 - 2$ 的零点, 但是 $x^3 - 2$ 在 $\mathbb{Q}(\sqrt[3]{2})$ 中只有一个根, 所以 $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$, 故 $\tau = \mathrm{id}$, 所以 $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ 为平凡群. 显然 $\mathrm{Fix}(\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})) = \mathbb{Q}(\sqrt[3]{2})$. 所以在这种情况下, $\mathbb{Q}$ 并不是 $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ 的某个子群的不动域.

例 1.20. 考虑 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. 同样的, $\tau \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ 完全由 $\tau(\sqrt{2})$ 确定, 并且 $\tau(\sqrt{2})$ 为 $\min(\mathbb{Q}, \sqrt{2}) = x^2 - 2$ 的零点, 故 $\tau(\sqrt{2}) = \pm\sqrt{2}$. 容易验证 $\tau(\sqrt{2}) = -\sqrt{2}$ 时 τ 确实是 $\mathbb{Q}(\sqrt{2})$ 的自同构, 所以 $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\mathrm{id}, \tau\}$. 若 $a + b\sqrt{2} \in \mathrm{Fix}(\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}))$, 那么 $a + b\sqrt{2} = \tau(a + b\sqrt{2}) = a - b\sqrt{2}$, 即 $b = 0$, 所以 $\mathbb{Q} = \mathrm{Fix}(\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}))$. 另一边, 假设 L 是 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 的中间域, 那么 $[L : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, 所以 $[L : \mathbb{Q}] = 1$ 或者 $[L : \mathbb{Q}] = 2$, 即 $L = \mathbb{Q}$ 或者 $L = \mathbb{Q}(\sqrt{2})$. 所以在这种情况下, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 的中间域和 $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ 的子群是一一对应的.

为了研究上面的问题, 仅仅知道 $\mathrm{Gal}(K/F)$ 是有限群还不够, 我们需要进一步研究 $\mathrm{Gal}(K/F)$ 的大小.

引理 1.21. *K/F 是有限扩张, 令 $\tau_1, \dots, \tau_n \in \mathrm{Gal}(K/F)$, 并且 τ_i 之间互不相同, 注意到 τ_i 可以视为 K-线性映射, 我们断言 $\tau_1, \dots, \tau_n$ 是 K-线性无关的.*

Proof. 对 $k = n$ 归纳. 显然 $k = 1$ 时结论成立. 假设 $k = m - 1$ 时结论成立. 考虑 $k = m$ 的情况. 令 $a_1, \dots, a_m \in K$ 使得

$$a_1\tau_1 + \cdots + a_m\tau_m = 0, \tag{1.1}$$

对于 $1 \le i \le m - 1$, 由于 $\tau_i \neq \tau_m$, 所以存在非零的 $\alpha_i \in K$ 使得 $\tau_i(\alpha_i) \neq \tau_m(\alpha_i)$. 由于 $\tau_j(\alpha x) = \tau_j(\alpha)\tau_j(x)$, 所以

$$a_1\tau_1(\alpha_i)\tau_1 + \cdots + a_m\tau_m(\alpha_i)\tau_m = 0, \tag{1.2}$$

将 (1.1) 式乘以 $\tau_m(\alpha_i)$ 减去 (1.2) 式, 所以

$$\sum_{j=1}^{m-1} a_j(\tau_m(\alpha_i) - \tau_j(\alpha_i))\tau_j = 0,$$

根据假设, $\tau_1, \dots, \tau_{m-1}$ 线性无关, 由于 $\tau_m(\alpha_i) - \tau_i(\alpha_i) \neq 0$, 所以 $a_i = 0$. 所以 $a_1 = \cdots = a_{m-1} = a_m = 0$, 即 $\tau_1, \dots, \tau_m$ 线性无关. □

命题 1.22. *若 K/F 是有限扩张, 那么 $|\mathrm{Gal}(K/F)| \le [K : F]$.*

Proof. 设 $[K:F]=n$. 令 $\tau_1,\dots,\tau_m\in \mathrm{Gal}(K/F)$, 假设 $m>n$. 设 $\alpha_1,\dots,\alpha_n$ 为 K 的一组基. 考虑 K 上的矩阵

$$A=(\tau_i(\alpha_j))_{m\times n}=\begin{pmatrix}\tau_1(\alpha_1) & \tau_1(\alpha_2) & \cdots & \tau_1(\alpha_n)\\ \tau_2(\alpha_1) & \tau_2(\alpha_2) & \cdots & \tau_2(\alpha_n)\\ \vdots & \vdots & \ddots & \vdots\\ \tau_m(\alpha_1) & \tau_m(\alpha_2) & \cdots & \tau_m(\alpha_n)\end{pmatrix},$$

$m>n$ 表明 $\mathrm{rank}(A)\le n<m$, 所以 A 的行向量是 K-线性相关的, 所以存在不全为零的 $c_1,\dots,c_m\in K$, 使得对于任意的 $1\le j\le n$ 有

$$c_1\tau_1(\alpha_j)+\cdots+c_m\tau_m(\alpha_j)=0,$$

任取 $\alpha\in K$, 那么 $\alpha=a_1\alpha_1+\cdots+a_n\alpha_n$, 其中 $a_i\in F$, 所以

$$\sum_i c_i\tau_i(\alpha)=\sum_i c_i\tau_i\left(\sum_j a_j\alpha_j\right)=\sum_i\sum_j a_jc_i\tau_i(\alpha_j)=\sum_j a_j\left(\sum_i c_i\tau_i(\alpha_j)\right)=0,$$

这表明 $c_1\tau_1+\cdots+c_m\tau_m=0$, 且 $c_1,\dots,c_m$ 不全为零, 即 $\tau_1,\dots,\tau_m$ 是 K-线性相关的, 与 引理 1.21 矛盾. 所以有 $m\le n$. □

例 1.19 表明 命题 1.22 中的等号可能取不到. 那么什么时候有 $|\mathrm{Gal}(K/F)|=[K:F]$? 下面的命题告诉我们, 对于自同构群的有限子群而言, 引理 1.16 的 (5) 总是成立的.

命题 1.23. 令 G 是 $\mathrm{Aut}(K)$ 的有限子群, $F=\mathrm{Fix}(G)$, 那么 $|G|=[K:F]$, 进而有 $G=\mathrm{Gal}(K/F)$.

Proof. 由于 $G\subseteq\mathrm{Gal}(K/F)$, 若 $[K:F]<\infty$, 根据 命题 1.22, 有 $|G|\le|\mathrm{Gal}(K/F)|\le[K:F]$, 所以 $|G|\le[K:F]$. 若 $[K:F]=\infty$, 同样有 $|G|\le[K:F]$. 假设 $|G|<[K:F]$. 设 $|G|=n$, 那么可以取 $\alpha_1,\dots,\alpha_{n+1}\in K$ 使得它们 F-线性无关. 设 $G=\{\tau_1,\dots,\tau_n\}$, 考虑 K 上的矩阵

$$A=(\tau_i(\alpha_j))_{n\times(n+1)}=\begin{pmatrix}\tau_1(\alpha_1) & \tau_1(\alpha_2) & \cdots & \tau_1(\alpha_{n+1})\\ \tau_2(\alpha_1) & \tau_2(\alpha_2) & \cdots & \tau_2(\alpha_{n+1})\\ \vdots & \vdots & \ddots & \vdots\\ \tau_n(\alpha_1) & \tau_n(\alpha_2) & \cdots & \tau_n(\alpha_{n+1})\end{pmatrix},$$

那么 $\mathrm{rank}(A)\le n<n+1$, 所以 A 的列向量 K-线性相关. 将 A 的列向量依次记为 $A_1,\dots,A_{n+1}\in K^n$, 选取使得 $A_1,\dots.A_m$ 线性相关的最小的 m. 根据 m 的最小性, 存在全不为零的 $c_1,\dots,c_m\in K$, 使得 $\sum_i c_iA_i=0$, 即 $\sum_i c_i\tau_j(\alpha_i)=0$, 其中 $1\le j\le n$. 通过等式两边同时除以 c_m, 我们可以假设 $c_m=1$.

下面我们断言: 系数 $c_1,\dots,c_m\in F$. 任取 $\sigma\in G$, 那么 $\sigma G=G$, 所以

$$0=\sum_i\sigma(c_i)\sigma\tau_j(\alpha_i)=\sum_i\sigma(c_i)\tau'_j(\alpha_i),$$

其中随着 j 取遍 1 到 n, τ_j' 取遍 G, 所以对于所有的 j 还是有 $\sum_i \sigma(c_i)\tau_j(\alpha_i) = 0$. 那么

$$\sum_i (c_i - \sigma(c_i))\tau_j(\alpha_i) = 0,$$

由于 $c_m = 1$, 所以 $\sum_{i=1}^{m-1}(c_i - \sigma(c_i))\tau_j(\alpha_i) = 0$, m 的最小性表明 $c_i - \sigma(c_i) = 0$. 根据 σ 的任意性, 所以 $c_i \in \mathrm{Fix}(G) = F$.

回到最开始的证明, 由于 $\sum_i c_i\tau_j(\alpha_i) = 0$ 对于所有的 j 都成立并且 $c_i \in F$, 所以 $\tau_j(\sum_i c_i\alpha_i) = \sum_i c_i\tau_j(\alpha_i) = 0$, 所以 $\sum_i c_i\alpha_i = 0$, 而 $c_1, \ldots, c_m$ 全不为零, $\alpha_1, \ldots, \alpha_m$ 线性无关, 这是矛盾的. 所以 $|G| \geq [K : F]$, 所以 K/F 是有限扩张并且 $|G| = [K : F]$.

我们总是有 $G \subseteq \mathrm{Gal}(K/F)$, 现在又有 $|G| = [K : F] \geq |\mathrm{Gal}(K/F)|$, 所以 $G = \mathrm{Gal}(K/F)$. □

命题 1.23 告诉我们, 对于有限扩张 K/F, $\mathrm{Gal}(K/F)$ 的子群必然是 K/F 的某个中间域对应的 Galois 群, 即 $\mathrm{Gal} : \mathcal{L} \to \mathcal{H}$ 是满射, 并且这个时候扩张次数刚好等于 Galois 群的阶数. 我们可以用一个例子验证这一点.

例 1.24. 考虑 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$. 那么 $\tau \in \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$ 将 $\sqrt[4]{2}$ 送到 $x^4 - 2$ 的零点, $x^4 - 2$ 在 $\mathbb{Q}(\sqrt[4]{2})$ 中只有两个零点, 即 $\tau(\sqrt[4]{2}) = \pm\sqrt[4]{2}$, 容易验证这两种情况都是自同构, 所以 $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}) = \{\mathrm{id}, \tau\}$. 考虑 $L = \mathrm{Fix}(\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}))$, 注意到

$$\tau(\sqrt{2}) = \tau(\sqrt[4]{2})^2 = \sqrt{2},$$

所以 $\sqrt{2} \in L$, 即 $\mathbb{Q}(\sqrt{2}) \subseteq L$. 同时 $[L : \mathbb{Q}(\sqrt{2})] \mid [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = 2$, 显然 $L \neq \mathbb{Q}(\sqrt[4]{2})$, 所以 $L = \mathbb{Q}(\sqrt{2})$. 不难验证 $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/L) = \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$, 所以此时有 $[\mathbb{Q}(\sqrt[4]{2}) : L] = 2 = |\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/L)|$. 这与 命题 1.23 的结论是相符的.

自然地, 我们会考虑什么时候 $\mathrm{Gal} : \mathcal{L} \to \mathcal{H}$ 是双射, 即 K/F 的任意中间域都是 $\mathrm{Gal}(K/F)$ 的某个子群的不动域. 当然, 这也相当于 Fix 是 Gal 的左逆. 为此, 我们做出以下定义.

定义 1.25. 若 K/F 是代数扩张, 如果 $F = \mathrm{Fix}(\mathrm{Gal}(K/F))$, 那么我们说 K/F 是 **Galois 扩张**.

推论 1.26. K/F 是有限扩张, 则 K/F 是 Galois 扩张当且仅当 $|\mathrm{Gal}(K/F)| = [K : F]$.

Proof. 若 K/F 是 Galois 扩张, 也就是说 $F = \mathrm{Fix}(\mathrm{Gal}(K/F))$, 根据 命题 1.23 ($G$ 取为 $\mathrm{Gal}(K/F)$), 我们有 $|\mathrm{Gal}(K/F)| = [K : F]$. 若 $|\mathrm{Gal}(K/F)| = [K : F]$, 令 $L = \mathrm{Fix}(\mathrm{Gal}(K/F))$, 那么总是有 $L \supseteq F$. 根据 命题 1.23, 有 $\mathrm{Gal}(K/F) = \mathrm{Gal}(K/L)$, 所以 $[K : F] = |\mathrm{Gal}(K/L)| \leq [K : L]$, 结合 $L \supseteq F$, 只可能 $L = F$, 即 F 是 Galois 扩张. □

实际上, 对于有限 Galois 扩张而言, $\mathrm{Gal} : \mathcal{L} \to \mathcal{H}$ 是双射, 逆映射就是 $\mathrm{Fix} : \mathcal{H} \to \mathcal{L}$, 即 K/F 的中间域和 $\mathrm{Gal}(K/F)$ 的子群是一一对应的. 我们留到第五章来证明这一点. 推论 1.26 十分重要, 提供了判断 Galois 扩张的一种数值方法. 对于单扩张而言, 我们有更方便的判别方法.

推论 1.27. K/F 是域扩张，令 $a \in K$ 是 F 上的代数元．那么 $|\mathrm{Gal}(F(a)/F)|$ 等于 $\min(F,a)$ 在 $F(a)$ 中的零点的个数．因此，$F(a)/F$ 是 Galois 扩张当且仅当 $\min(F,a)$ 在 $F(a)$ 中有 $n = \deg(\min(F,a))$ 个不同的零点．

Proof. 如果 $\tau \in \mathrm{Gal}(F(a)/F)$，那么 $\tau(a)$ 是 $\min(F,a)$ 的零点，又因为 $\tau(a)$ 完全决定了 τ，所以 τ 最多也只有 $n = \deg(\min(F,a))$ 个选择，即 $|\mathrm{Gal}(F(a)/F)| \leq n$．反之，若 b 是 $\min(F,a)$ 在 $F(a)$ 中的零点，我们说明确实存在 $F(a)$ 的 F-自同构将 a 送到 b．定义 $\tau : F(a) \to F(a)$ 满足 $\tau(f(a)) = f(b)$，若 $f(a) = g(a)$，记 $p(x) = \min(F,a)$，那么 $p(x) \mid f(x) - g(x)$，由于 $p(b) = 0$，所以 $f(b) = g(b)$，即 $\tau(f(a)) = \tau(g(a))$，所以 τ 是良定义的．容易验证 τ 是 F-同构．所以 $\tau \in \mathrm{Gal}(F(a)/F)$．这就表明 $\mathrm{Gal}(F(a)/F)$ 的元素一一对应到 $\min(F,a)$ 在 $F(a)$ 中的零点．又因为 $[F(a) : F] = n$，根据 推论 1.26，$F(a)/F$ 是 Galois 扩张当且仅当 $|\mathrm{Gal}(F(a)/F)| = n$，当且仅当 $\min(F,a)$ 在 $F(a)$ 中有 n 个不同的零点． □

推论 1.27 表明，阻止单扩张 $F(a)/F$ 成为 Galois 扩张可能有两个原因：

(1) $p(x) = \min(F,a)$ 在 $F(a)$ 中没有全部的根，例如 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$，此时 $\min(\mathbb{Q}, \sqrt[3]{2}) = x^3 - 2$ 在 $\mathbb{Q}(\sqrt[3]{2})$ 中只有一个零点．

(2) $p(x) = \min(F,a)$ 的所有根都在 $F(a)$ 中，但是有重根．这样的例子较为有趣，可以见 例 1.28．

上面两种情况可以推广到一般的域扩张进行研究，分别对应着第三章的正规扩张和第四章的可分扩张．实际上，通过单扩张的例子，可以直观地感受到这两种扩张同时决定着一个域扩张是否为 Galois 扩张．最后我们以一些例子结束本节．

例 1.28. 令 k 是特征 $p > 0$ 的域，$k(t)$ 为 k 上的有理函数域．考虑扩张 $k(t)/k(t^p)$．注意到 t 满足方程 $x^p - t^p \in k(t^p)[x]$，所以 $\min(k(t^p), t) \mid (x^p - t^p)$，但是 $x^p - t^p = (x-t)^p$，所以 $\min(k(t^p), t)$ 在 $k(t)$ 中只有唯一的多重零点 t，因此 $\mathrm{Gal}(k(t)/k(t^p)) = \{\mathrm{id}\}$，所以 $k(t)/k(t^p)$ 不是 Galois 扩张．

例 1.29. 记 $\omega = e^{2\pi i/3}$，考虑 $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$．由于 ω 是多项式 $x^2 + x + 1 \in \mathbb{Q}(\sqrt[3]{2})[x]$ 的根，并且 $\omega \notin \mathbb{Q}(\sqrt[3]{2})$，所以 $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})] = 2$．又因为 $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$，所以 $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6$．$\tau \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ 完全由 $\tau(\sqrt[3]{2})$ 和 $\tau(\omega)$ 确定，所以可能的取值为

$$
\begin{aligned}
&\mathrm{id} : \sqrt[3]{2} \mapsto \sqrt[3]{2},\ \omega \mapsto \omega,\\
&\tau_1 : \sqrt[3]{2} \mapsto \sqrt[3]{2},\ \omega \mapsto \omega^2,\\
&\tau_2 : \sqrt[3]{2} \mapsto \omega\sqrt[3]{2},\ \omega \mapsto \omega,\\
&\tau_3 : \sqrt[3]{2} \mapsto \omega\sqrt[3]{2},\ \omega \mapsto \omega^2,\\
&\tau_4 : \sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2},\ \omega \mapsto \omega,\\
&\tau_5 : \sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2},\ \omega \mapsto \omega^2.
\end{aligned}
$$

当然，可以逐一验证这些确实都是 $\mathbb{Q}(\sqrt[3]{2}, \omega)$ 的 $\mathbb{Q}$-自同构，所以 $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ 是 Galois 扩张．当然，检验上述映射是自同构是一个繁琐且乏味的过程，后面我们有更方便的

判断 $\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}$ 是 Galois 扩张的方法, 一旦我们知道 $\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}$ 是 Galois 扩张, 那么上述映射就必然成为自同构.

例 1.30. 这是一个非常有趣的例子. 令 k 是域, $K = k(x_1,\dots,x_n)$ 是 k 上 n 个变量的有理函数域. 对于置换 $\sigma \in S_n$, 定义 $\sigma(x_i) = x_{\sigma(i)}$. 这诱导了一个环同构, 我们仍记为 $\sigma : k[x_1,\dots,x_n] \to k[x_1,\dots,x_n]$, 满足

$$\sigma(f(x_1,\dots,x_n)) = f(x_{\sigma(1)},\dots,x_{\sigma(n)}).$$

这又诱导了分式域的同构 $\sigma : K \to K$, 满足

$$\sigma\left(\frac{f(x_1,\dots,x_n)}{g(x_1,\dots,x_n)}\right) = \frac{f(x_{\sigma(1)},\dots,x_{\sigma(n)})}{g(x_{\sigma(1)},\dots,x_{\sigma(n)})}.$$

所以我们可以将 S_n 视为 $\mathrm{Aut}(K)$ 的子群. 令 $F = \mathrm{Fix}(S_n)$, 根据 命题 1.23, K/F 是 Galois 扩张, 并且 $\mathrm{Gal}(K/F) = S_n$. 域 F 被称为**关于 $x_1,\dots,x_n$ 的对称函数域**, 这是因为 $f(x_1,\dots,x_n)/g(x_1,\dots,x_n) \in F$ 当且仅当

$$\frac{f(x_{\sigma(1)},\dots,x_{\sigma(n)})}{g(x_{\sigma(1)},\dots,x_{\sigma(n)})} = \frac{f(x_1,\dots,x_n)}{g(x_1,\dots,x_n)} \quad \forall \sigma \in S_n.$$

对于 $1 \le k \le n$, 令

$$s_k = \sum_{1\le i_1<\cdots<i_k\le n} x_{i_1}\cdots x_{i_k},$$

即

$$\begin{aligned} s_1 &= x_1 + x_2 + \cdots + x_n, \\ s_2 &= x_1x_2 + \cdots + x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n, \\ &\vdots \\ s_n &= x_1x_2\cdots x_n. \end{aligned}$$

我们将 $s_1,\dots,s_n$ 称为**基本对称多项式**. 显然 $s_1,\dots,s_n \in F$, 所以 $k(s_1,\dots,s_n) \subseteq F$. 我们将在下一节看到实际上有 $F = k(s_1,\dots,s_n)$, 也就是说每个对称函数实际上都是基本对称多项式的加减乘除构成的.

问题

1. 令 k 是域, $K = k(x)$ 是 k 上的有理函数域. 令 σ 和 τ 分别是 K 上由 $\sigma(f(x)/g(x)) = f(1/x)\big/g(1/x)$ 和 $\tau(f(x)/g(x)) = f(1-x)/g(1-x)$ 定义的自同构. 确定 $\{\sigma,\tau\}$ 的不动域 F 以及 $\mathrm{Gal}(K/F)$. 找到一个 $h \in F$ 使得 $F = k(h)$.

Proof. 首先我们寻找 σ,τ 生成的子群. 注意到 $\sigma\tau(x) = 1/(1-x)$ 且 $(\sigma\tau)^3(x) = x$, $\sigma(\sigma\tau)(x) = 1 - x = (\sigma\tau)^2\sigma(x)$, 所以 $\langle\sigma,\tau\rangle = \langle\sigma\tau,\sigma\rangle \simeq S_3$. 根据 命题 1.23, K/F 是 Galois 扩张, $\mathrm{Gal}(K/F) \simeq S_3$ 以及 $[K:F] = 6$.

$\langle\sigma,\tau\rangle$ 在 x 上作用的结果为:

$$x_1=x, x_2=\frac{1}{x}, x_3=1-x, x_4=\frac{x-1}{x}, x_5=\frac{1}{1-x}, x_6=\frac{x}{x-1}.$$

于是 $x_1,\dots,x_6$ 生成的基本对称多项式都在 $\langle\sigma,\tau\rangle$ 的作用下不动, 记 $s_1=x_1+\cdots+x_6,\dots,s_6=x_1\cdots x_6$ 是基本对称多项式, 那么 $k(s_1,\dots,s_6)\subseteq F$. 另一方面, x 是多项式 $(t-x_1)(t-x_2)\cdots(t-x_6)\in k(s_1,\dots,s_6)[t]$ 的零点, 所以 $[K:k(s_1,\dots,s_6)]\leq 6$. 所以 $[K:k(s_1,\dots,s_6)]=6$ 以及 $F=k(s_1,\dots,s_6)$.

注意到

$$s_2=-\frac{x^6-3x^5+5x^3-3x+1}{x^2(x-1)^2},$$

那么根据 例 1.5, 有 $[K:k(s_2)]=6$. 所以 $F=k(s_1,\dots,s_6)=k(s_2)$. □

2. 令 k 是域, $K=k(x)$ 是有理函数域. 如果 $u\in K$, 证明 $K=k(u)$ 当且仅当 $u=(ax+b)/(cx+d)$, 其中 $a,b,c,d\in k$ 且 $\det\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\neq 0$.

Proof. 若 $u=(ax+b)/(cx+d)$ 且 $ad-bc\neq 0$. 那么向量 $\binom{a}{b}$ 和 $\binom{c}{d}$ 线性无关, 所以 $\gcd(ax+b,cx+d)=1$, 根据 例 1.5, 有 $[K:k(u)]=1$, 所以 $K=k(u)$.

反之, 若 $K=k(u)$. 设 $u=f/g$ 且 $\gcd(f,g)=1$, 再根据 例 1.5, $[K:k(u)]=\max\{f,g\}=1$. 于是可设 $u=(ax+b)/(cx+d)$, $\gcd(ax+b,cx+d)=1$ 就表明 $ad-bc\neq 0$. □

3. 使用上一个问题证明任意 2×2 可逆矩阵 $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ 都确定了 $\mathrm{Gal}(k(x)/k)$ 的元素满足 $x\mapsto(ax+b)/(cx+d)$. 此外, 证明 $\mathrm{Gal}(k(x)/k)$ 的任意元素都由上面的公式给出. 证明从 k 上 2×2 可逆矩阵 $\mathrm{GL}_2(k)$ 到 $\mathrm{Gal}(k(x)/k)$ 的映射 $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\mapsto\varphi$, 其中 $\varphi(x)=(ax+b)/(cx+d)$,是一个群同态.确定这个群同态的核从而得到 $\mathrm{Gal}(k(x)/k)\simeq\mathrm{PGL}_2(k)$, 即 k 上的 2×2 可逆矩阵群模去数量矩阵.

1.3 正规扩张

本节我们研究 例 1.28 之前所说的阻止 $F(a)/F$ 成为 Galois 扩张的第一种情况, 即 $\min(F,a)$ 不是所有的零点都落在 $F(a)$ 中.

引理 1.31. 令 $f(x)\in F[x]$, $\alpha\in F$, 那么 α 是 f 的零点当且仅当 $(x-\alpha)\mid f$. 此外, 在 F 的任意扩域中, f 至多也只能有 $\deg f$ 个零点.

Proof. 若 $f(\alpha)=0$, 做带余除法, 存在 $q(x),r(x)\in F[x]$ 使得 $f(x)=q(x)(x-\alpha)+r(x)$, 其中 $\deg r<\deg(x-\alpha)=1$, 所以 $r(\alpha)=0$, 这表明 $r(x)=0$, 即 $(x-\alpha)\mid f(x)$. 反之显然成立.

对 $\deg f=n$ 归纳. 当 $n=1$ 时, 即 $f(x)=ax+b$, 其中 $a,b\in F$. 那么 $f(x)=0$ 当且仅当 $x=-b/a\in F$, 结论成立. 假设结论在 $n-1$ 的时候成立. 设 K 是 F 的任意扩域, 如果 $f(x)$ 在 K 中没有零点, 结论自然成立. 如果 $f(x)$ 在 K 中有零点 $\alpha\in K$, 根据前面的叙述, $f(x)$ 在 $K[x]$ 中分解为 $f(x)=(x-\alpha)g(x)$, 其中 $g(x)\in K[x]$. 由于

$\deg g = n-1$, 根据假设, $g(x)$ 在 K 的任意扩域中至多有 $n-1$ 个零点, 特别地, $g(x)$ 在 K 中至多有 $n-1$ 个零点, 所以 $f(x)$ 在 K 中至多有 n 个零点, 结论成立. □

定义 1.32. K/F 是域扩张, $f(x) \in F[x]$, 如果存在 $a \in F$ 和 $\alpha_1, \dots, \alpha_n \in K$ 使得

$$f(x) = a\prod_{i=1}^{n}(x-\alpha_i) \in K[x],$$

那么我们说 f 在 K 上**分裂**.

实际上, 在第一节的最开始, 我们已经证明了: 对于任意多项式 $f(x) \in F[x]$, 都可以找到 F 的一个扩域使得其至少包含 f 的一个零点. 现在我们来严格叙述这一点并且加以推广.

定理 1.33. 令 $f(x) \in F[x]$ 是 n 次多项式, 那么存在 F 的扩域 K, 使得 K 包含 f 的一个零点, 并且 $[K:F] \le n$. 进一步地, 存在 F 的扩域 L, 使得 f 在 L 上分裂, 并且 $[L:F] \le n!$.

Proof. 设 $p(x)$ 为 $f(x)$ 的不可约因子. 那么 $K = F[x]/(p(x))$ 是域, 通过将 $a \in F$ 视为 $\bar{a} = a + (p(x)) \in K$, 我们可以将 F 视为 K 的子域. 在 K 中, $\bar{x} = x + (p(x))$ 使得 $p(\bar{x}) = p(x) + (p(x)) = 0$, 所以 K 包含 p 的零点, 从而包含 f 的一个零点. 并且有 $[K:F] = \deg p \le \deg f = n$.

对 $n = \deg f$ 归纳. 在 $n = 1$ 的时候 $L = F$ 即可. 假设结论在 $n-1$ 时成立. 根据前面的叙述, 存在 F 的扩域 K, 使得 K 包含 f 的一个零点 $\alpha \in K$, 那么 $f(x) = (x-\alpha)g(x)$, 其中 $g(x) \in K[x]$. 由于 $\deg g = n-1$, 根据假设, 存在 K 的一个扩域 L, 使得 g 在 L 上分裂, 并且 $[L:K] \le (n-1)!$, 那么 f 在 L 上也分裂, 并且 $[L:F] = [L:K][K:F] \le (n-1)! \cdot n = n!$. □

定义 1.34. K/F 是域扩张, $f(x) \in F[x]$.

(1) 若 f 在 K 上分裂, 设 f 在 K 中的所有根为 $\alpha_1, \dots, \alpha_n$, 并且 $K = F(\alpha_1, \dots, \alpha_n)$, 那么我们说 K 是 f 在 F 上的**分裂域**. F 明确的情况下有时会简称为 f 的分裂域.

(2) 若 S 是 F 上的一组多项式的集合, 每个 $f \in S$ 在 K 上都分裂, 设 X 是 S 中所有多项式的零点集, 并且 $K = F(X)$, 那么我们说 K 是 S 在 F 上的**分裂域**.

若 K 是 S 在 F 上的分裂域, L 是 K 的子域且使得 S 中的多项式在 L 上都分裂, 任取 $\alpha \in K$, 那么存在 $\alpha_1, \dots, \alpha_n \in X$ 使得 $\alpha \in F(\alpha_1, \dots, \alpha_n)$, 其中 $\alpha_1, \dots, \alpha_n$ 是一些多项式 $f_1, \dots, f_m \in S$ 的零点, 由于 $f_1, \dots, f_m$ 在 L 上分裂, 所以 $\alpha_1, \dots, \alpha_n \in L$, 故 $\alpha \in L$, 所以 $L = K$. 这表明 K 实际上是使得 S 中多项式都分裂的 F 的最小扩域.

定理 1.33 实际上保证了 S 是有限集的时候分裂域的存在性.

推论 1.35. 若 $f_1, \dots, f_n \in F[x]$, 那么存在 $\{f_1, \dots, f_n\}$ 在 F 上的分裂域.

Proof. 令 $f = f_1 \cdots f_n$. 显然 $\{f_1, \dots, f_n\}$ 在 F 上的分裂域和 f 在 F 上的分裂域是相同的. 根据 定理 1.33, 存在 F 的扩域 K, 使得 f 在 K 上分裂. 令 $\alpha_1, \dots, \alpha_m$ 为 f 在 K 中的所有零点, 那么 $F(\alpha_1, \dots, \alpha_m)$ 就是 f 在 F 上的分裂域. □

例 1.36. $\mathbb{Q}(\sqrt[3]{2},\omega)$ 是 x^3-2 在 $\mathbb{Q}$ 上的分裂域, 因为

$$x^3-2=(x-\sqrt[3]{2})(x-\omega\sqrt[3]{2})(x-\omega^2\sqrt[3]{2})\in\mathbb{Q}(\sqrt[3]{2},\omega)[x],$$

并且容易验证 $\mathbb{Q}(\sqrt[3]{2},\omega)=\mathbb{Q}(\sqrt[3]{2},\omega\sqrt[3]{2},\omega^2\sqrt[3]{2})$. $\mathbb{C}$ 是 x^2+1 在 $\mathbb{R}$ 上的分裂域.

例 1.37. 考虑 $K=\mathbb{F}_2[x]/(x^2+x+1)$, 那么 K 可以视为 $\mathbb{F}_2(\alpha)$, 其中 α 是 x^2+x+1 的零点, 因为

$$x^2+x+1=(x-\alpha)(x-(\alpha+1))\in K[x],$$

所以 K 是 x^2+x+1 在 $\mathbb{F}_2$ 上的分裂域.

由 定理 1.33 立即得出下面的推论.

推论 1.38. *F 是域, $f(x)\in F[x]$ 是 n 次多项式, 如果 K 是 f 在 F 上的分裂域, 那么 $[K:F]\leq n!$.*

例 1.39. 我们继续研究 例 1.30. 记

$$f(t)=t^n-s_1t^{n-1}+\cdots+(-1)^ns_n\in k(s_1,\ldots,s_n)[t],$$

其在 $K[x]$ 中分裂为

$$f(t)=(t-x_1)\cdots(t-x_n),$$

又因为 $K=k(x_1,\ldots,x_n)$, 所以 K 是 f 在 $k(s_1,\ldots,s_n)$ 上的分裂域, 根据 推论 1.38, 所以 $[K:k(s_1,\ldots,s_n)]\leq n!$. 对于 $F=\mathrm{Fix}(S_n)$, 命题 1.23 表明 $[K:F]=|S_n|=n!$. 又因为 $k(s_1,\ldots,s_n)\subseteq F$, 所以只可能 $[K:k(s_1,\ldots,s_n)]=[K:F]=n!$. 这就证明了 $F=k(s_1,\ldots,s_n)$.

1.3.1 代数闭包

我们还没有证明无限多个多项式集合在 F 上的分裂域的存在性. 我们首先研究最极端的情况, 即 F 上所有非常数多项式在 F 上的分裂域 K, 一旦证明了 K 存在, 那么任意多项式集合的分裂域都是 K 的某个子域. 我们先假设这样的 K 存在, 若 L/K 是代数扩张, 任取 $a\in L$, 那么 a 在 F 上也是代数的, 而 $\min(F,a)$ 在 K 上分裂, 所以 $a\in L$, 所以 $L=K$. 于是我们发现, 这样的 K 如果存在, 那么其没有任意恰当的代数扩域. 我们先给出这样的域的一些等价条件.

引理 1.40. *K 是域, 那么下面的说法是等价的.*

(1) *K 的代数扩张只有 K 本身.*
(2) *K 的有限扩张只有 K 本身.*
(3) *如果 L 是 K 的扩域, 那么 K 是 K 在 L 中的代数闭包 (定义 1.10).*
(4) *任意 $f(x)\in K[x]$ 在 K 上都分裂.*
(5) *任意 $f(x)\in K[x]$ 在 K 中都有一个根.*
(6) *K 上的不可约多项式只有一次多项式.*

Proof. (1) $\Rightarrow$ (2) 有限扩张都是代数扩张.

(2) $\Rightarrow$ (3) 记 $\bar{K}$ 为 K 在 L 中的代数闭包. 任取 $a \in \bar{K}$, 那么 $K(a)/K$ 是有限扩张, 所以 $K(a) = K$, 故 $a \in K$, 所以 $K = \bar{K}$.

(3) $\Rightarrow$ (4) 任取 $f(x) \in K[x]$, 记 L 为 f 在 K 上的分裂域, 那么 L/K 是代数扩张, 所以 K 在 L 中的代数闭包就是 L, 故 $L = K$, f 在 K 上分裂.

(4) $\Rightarrow$ (5) 显然.

(5) $\Rightarrow$ (6) 设 $f(x) \in K[x]$ 是不可约多项式, 由于 f 在 K 中有零点 α, 所以 $(x-\alpha) \mid f$, f 不可约表明 $f = a(x-\alpha)$, 其中 $a \in K$, 即 f 是一次多项式.

(6) $\Rightarrow$ (1) 设 L/K 是代数扩张. 任取 $a \in L$, $\min(K, a)$ 是一次多项式, 这表明 $[K(a) : K] = 1$, 所以 $a \in K$, $L = K$. □

定义 1.41. 如果 K 满足 引理 1.40 中的任意一条, 那么我们说 K 是**代数闭域**. 如果 K/F 是代数扩张且 K 是代数闭域, 那么我们说 K 是 F 的**代数闭包**, 通常记为 $\bar{F}$.

例 1.42. 复数域 $\mathbb{C}$ 是代数闭域, 这源于**代数基本定理**, 我们将在第五节提供一种代数证明. $\mathbb{Q}$ 在 $\mathbb{C}$ 中的代数闭包记为 $\mathbb{A}$, 任取 $f(x) \in \mathbb{A}[x]$, 由于 $\mathbb{C}$ 是代数闭域, 所以 f 在 $\mathbb{C}$ 中有根 α, α 在 $\mathbb{A}$ 上是代数的, $\mathbb{A}/\mathbb{Q}$ 是代数扩张, 所以 α 在 $\mathbb{Q}$ 上是代数的, 所以 $\alpha \in \mathbb{A}$, 这表明 $\mathbb{A}$ 是代数闭域. 所以 $\mathbb{A}$ 是 $\mathbb{Q}$ 的代数闭包. 类似地可以证明: 对于域扩张 K/F, 如果 K 是代数闭域, 此时 F 在 K 中的代数闭包就是 F 的代数闭包. 此外, $\mathbb{C}$ 是 $\mathbb{R}$ 的代数闭包, 但注意 $\mathbb{C}$ 不是 $\mathbb{Q}$ 的代数闭包, 因为 $\mathbb{C}/\mathbb{Q}$ 不是代数扩张.

定理 1.43. *F 是一个域, 那么 F 有一个代数闭包.*

Proof. 对于每个首一的非常数多项式 $f \in F[x]$, 我们记 x_f 是一个未定元, 记 $X = \{x_f \mid f \in F[x]\}$. 考虑无穷多个未定元集合 X 上的多项式环 $F[X]$. 考虑所有 $f(x_f)$ 生成的理想 I. 我们首先说明 I 是 $F[X]$ 的一个恰当理想. 如果 $1 \in I$, 那么存在 $f_1, \dots, f_n \in F[x]$ 和 $g_1, \dots, g_n \in F[X]$ 使得

$$1 = g_1 f_1(x_{f_1}) + \cdots + g_n f_n(x_{f_n}).$$

$g_i \in F[X]$ 表明存在 $f_{n+1}, \dots, f_m \in F[x]$ 使得 $g_i \in F[x_{f_1}, \dots, x_{f_n}, x_{f_{n+1}}, \dots, x_{f_m}]$. 于是

$$1 = g_1(x_{f_1}, \dots, x_{f_m}) f_1(x_{f_1}) + \cdots + g_n(x_{f_1}, \dots, x_{f_m}) f_n(x_{f_n}). \tag{1.3}$$

令 K 是 $\{f_1(x), \dots, f_n(x)\}$ 在 F 上的分裂域, $1 \le i \le n$ 时, 取 x_{f_i} 为 $\alpha_i \in K$, 其中 α_i 是 $f_i(x)$ 的一个根. 令 $x_{f_{n+1}}, \dots, x_{f_m}$ 均取零, 那么 (1.3) 告诉我们在 K 中有 $0 = 1$, 这是不可能的, 所以 I 是 $F[X]$ 的一个恰当理想.

I 是恰当理想表明其被一个极大理想 J 包含, 那么考虑域

$$L_1 = F[X]/J.$$

F 可以自然地嵌入到 L_1 中. 根据 I 的定义, 每个多项式 $f \in F[x]$ 在 L_1 中都有一个根, 即 $x_f + J$. 然后重复上面的所有操作, 可以得到域 $L_2 \supseteq L_1$ 使得 $L_1[x]$ 中的多项

式在 L_2 中都有一个根. 于是我们可以得到一个域塔:

$$F = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots,$$

其中每个 $L_i[x]$ 中的多项式在 L_{i+1} 中都有一个根. 令

$$L = \bigcup_{i \geq 0} L_i.$$

显然 L 是 F 的一个扩域. 任取多项式 $h(x) \in L[x]$, 那么存在 N 使得 $h(x) \in L_N[x]$, 从而在 $L_{N+1} \subseteq L$ 中有一个根, 根据 引理 1.40 的 (5), L 是代数闭域. 令 $\bar{F}$ 为 F 在 L 中的代数闭包, 根据 例 1.42, 此时 $\bar{F}$ 就是 F 的代数闭包. □

推论 1.44. 令 S 是 F 上某些非常数多项式的集合, 那么存在 S 在 F 上的分裂域.

Proof. 令 K 是 F 的代数闭包. 那么每个 $f(x) \in S$ 在 K 上分裂, 令 X 是所有 $f \in S$ 的零点集. 那么 $F(X) \subseteq K$ 就是 S 在 F 上的分裂域. □

1.3.2 同构延拓定理

当我们说某个多项式集合的分裂域的时候, 自然就会存在另一个问题, 有没有可能存在两个不同构的分裂域? 答案是不可能. 现在我们来证明这一点.

如果 $\sigma : F \to F'$ 是域同态, 那么自然诱导出环同态 $\sigma : F[x] \to F'[x]$, 我们仍记为 σ, 其满足 $\sigma(\sum a_i x^i) = \sum \sigma(a_i) x^i$. 如果 $f(x) = (x - a_1) \cdots (x - a_n) \in F[x]$, 那么 $\sigma(f(x)) = (x - \sigma(a_1)) \cdots (x - \sigma(a_n))$, 这一点能够帮助我们研究分裂域.

引理 1.45 (同构延拓定理 1). 令 $\sigma : F \to F'$ 是域同构, $f(x) \in F[x]$ 是不可约多项式, 如果 α 是 f 在 F 的某个扩域 K 中的根, α' 是 $\sigma(f)$ 在 F' 的某个扩域 K' 中的根, 那么存在同构 $\tau : F(\alpha) \to F'(\alpha')$ 满足 $\tau(\alpha) = \alpha'$ 以及 $\tau|_F = \sigma$.

Proof. 当然, 可以直接按照定义验证 τ 是域同构, 但是我们采用更加体现本质的方法. 记 $f'(x) = \sigma(f(x))$, 我们有同构 $\varphi : F[x]/(f(x)) \to F(\alpha)$ 以及同构 $\psi : F'[x]/(f'(x)) \to F'(\alpha')$, 所以只需要证明 $F[x]/(f(x))$ 同构于 $F'[x]/(f'(x))$. 我们已经有同构 $\sigma : F[x] \to F'[x]$, 诱导出满同态 $F[x] \to F'[x] \to F'[x]/(f'(x))$, 同态核显然为 $f(x)$, 所以存在同构 $\nu : F[x]/(f(x)) \to F'[x]/(f'(x))$, 作用为 $\nu(g(x) + (f(x))) = \sigma(g(x)) + (f'(x))$. 所以复合映射 $\tau = \psi \circ \nu \circ \varphi^{-1}$ 是 $F(\alpha)$ 到 $F'(\alpha')$ 的同构映射. 此时 $\alpha \mapsto x + (f(x)) \mapsto x + (f'(x)) \mapsto \alpha'$. 若 $a \in F$, 那么 $a \mapsto a + (f(x)) \mapsto \sigma(a) + (f'(x)) \mapsto \sigma(a)$. □

引理 1.46. 令 $\sigma : F \to F'$ 是域同构, K 是 F 的扩域, K' 是 F' 的扩域. 假设 K 是 $\{f_i\}$ 在 F 上的分裂域并且 $\tau : K \to K'$ 是使得 $\tau|_F = \sigma$ 的同态. 记 $f_i' = \sigma(f_i)$, 那么 $\tau(K)$ 是 $\{f_i'\}$ 在 F' 上的分裂域.

Proof. 由于 K 是 $\{f_i\}$ 在 F 上的的分裂域, 所以 f_i 在 K 上分裂, 即 $f_i = a \prod_j (x - \alpha_j)$, 其中 $a \in F, \alpha_j \in K$, 那么 $f_i' = \sigma(f_i) = \tau(f_i) = \tau(a) \prod_j (x - \tau(\alpha_j))$, 所以 f_i' 在 $\tau(K)$ 上分裂. 由于 $K = F(X)$, 其中 X 为 $\{f_i\}$ 的所有零点, 所以 $\tau(K) = F(\tau(X))$, $\tau(X)$ 为 $\{f_i'\}$ 的所有零点, 于是 $\tau(K)$ 为 $\{f_i'\}$ 在 F' 上的分裂域. □

定理 1.47 (同构延拓定理 2). 令 $\sigma : F \to F'$ 是域同构，$f(x) \in F[x]$，$\sigma(f) \in F'[x]$. 记 K 是 f 在 F 上的分裂域，K' 是 $\sigma(f)$ 在 F' 上的分裂域. 任取 $\alpha \in K$，若 α' 是 $\sigma(\min(F,\alpha))$ 在 K' 中的任意零点，那么存在同构 $\tau : K \to K'$ 使得 $\tau|_F = \sigma$ 以及 $\tau(\alpha) = \alpha'$.

Proof. 对 $[K : F] = n$ 归纳. $n = 1$ 时 $\tau = \sigma$ 即满足要求. 假设在 $[K : F] < n$ 的时候，都存在同构 $\tau : K \to K'$ 使得 $\tau|_F = \sigma$. 对于 n 的情况，任取 $\alpha \in K$，记 $p(x) = \min(F,\alpha)$.

如果 $\deg p > 1$，根据 引理 1.45，存在同构 $\rho : F(\alpha) \to F'(\alpha')$ 使得 $\rho|_F = \sigma$ 以及 $\rho(\alpha) = \alpha'$. 此时 $[K : F(\alpha)] < n$，并且 K 为 f 在 $F(\alpha)$ 上的分裂域，K' 为 $\sigma(f)$ 在 $F'(\alpha')$ 上的分裂域，根据假设，存在同构 $\tau : K \to K'$ 使得 $\tau|_{F(\alpha)} = \rho$，此时 $\tau|_F = \rho|_F = \sigma$，以及 $\tau(\alpha) = \rho(\alpha) = \alpha'$.

如果 $\deg p = 1$，即 $\alpha \in F$，这表明如果 $\tau|_F = \sigma$，那么必有 $\tau(\alpha) = \sigma(\alpha) = \alpha'$，所以只需要证明存在同构 $\tau : K \to K'$ 使得 $\tau|_F = \sigma$ 即可. 此时任取 $f(x)$ 的一个不可约因子 $q(x)$，然后重复上一段的操作，就可以得到同构 $\tau : K \to K'$ 使得 $\tau|_F = \sigma$. □

上面的定理十分有用，证明了有限多个多项式的分裂域的唯一性，虽然可以直接证明一般的情况，但是大多数情况下，我们使用的都是有限个多项式的情况.

定理 1.48 (同构延拓定理 3). 令 $\sigma : F \to F'$ 是域同构，令 $S = \{f_i\}$ 是 F 上的一族多项式，$S' = \{\sigma(f_i)\}$ 是 F' 上的一族多项式，K 是 S 在 F 上的分裂域，K' 是 S' 在 F' 上的分裂域. 任取 $\alpha \in K$，若 α' 是 $\sigma(\min(F,\alpha))$ 在 K' 中的任意零点，那么存在同构 $\tau : K \to K'$ 使得 $\tau|_F = \sigma$ 以及 $\tau(\alpha) = \alpha'$.

推论 1.49. 令 F 是域，S 是 $F[x]$ 中多项式的集合，那么任意两个 S 在 F 上的分裂域都是 F-同构的. 特别地，任意两个 F 的代数闭包是 F-同构的.

推论 1.50. 令 F 是域，K/F 是代数扩张，那么 K 同构于 $\bar{F}$ 的一个子域.

Proof. $\bar{K}$ 是代数闭域并且 $\bar{K}/F$ 是代数扩张，所以 $\bar{K}$ 也是 F 的代数闭包，于是存在 F-同构 $f : \bar{K} \to \bar{F}$，所以 $f(K)$ 是 $\bar{F}$ 的子域，同构于 K. □

现在我们来说明，虽然分裂域的定义依赖于一族多项式，但是实际上存在不依赖于多项式的刻画方式.

定义 1.51. K/F 是域扩张，如果 K 是 F 上某一个多项式集合在 F 上的分裂域，那么我们说 K/F 是**正规扩张**.

例 1.52. 如果 $[K : F] = 2$，那么 K/F 是正规扩张. 任取 $\alpha \in K \setminus F$，那么 $K = F(\alpha)$. 令 $p(x) = \min(F,\alpha)$，那么 p 在 K 中有一个零点 α，所以 $p(x) = (x-\alpha)q(x) \in K[x]$，所以 $q(x)$ 是一次多项式，所以 $p(x)$ 在 K 上分裂. 故 $K = F(\alpha)$ 是 $p(x)$ 在 F 上的分裂域，K/F 是正规扩张.

定理 1.53. 如果 K/F 是代数扩张，那么下面的说法是等价的.

(1) K/F 是正规扩张.

(2) 如果 $\tau : K \to \bar{K}$ 是 F-同态，那么 $\tau(K) = K$.

(3) 对于任意不可约多项式 $f(x) \in F[x]$，如果 f 在 K 中有一个根，那么 f 在 K 上分裂.

Proof. (1) $\Rightarrow$ (2) 令 $\tau : K \to \bar{K}$ 是 F-同态，设 K 是 S 在 F 上的分裂域，根据 引理 1.46，所以 $\tau(K)$ 也是 S 在 F 上的分裂域，即 $\tau(K) = F(X) = K$，其中 X 是 S 的零点集.

(2) $\Rightarrow$ (3) 若不可约多项式 $f(x) \in F[x]$ 在 K 中有一个根 α，由于 $\bar{K}$ 也是 F 的代数闭包，所以 $f(x)$ 在 $\bar{K}$ 上分裂. 令 $\beta \in \bar{K}$ 为 f 的任意一个根，那么存在 F-同构 $\sigma : F(\alpha) \to F(\beta)$，满足 $\sigma(\alpha) = \beta$. 再根据同构延拓定理 3，存在同构 $\tau : \bar{K} \to \bar{K}$ 满足 $\tau|_{F(\alpha)} = \sigma$，根据 (2)，我们有 $\tau(K) = K$，故 $\beta = \sigma(\alpha) = \tau(\alpha) \in \tau(K) = K$，所以 f 在 K 上分裂.

(3) $\Rightarrow$ (1) 对于任意的 $\alpha \in K$，$\min(F, \alpha)$ 在 K 中有根 α，从而在 K 上分裂，记 $S = \{\min(F, \alpha) \mid \alpha \in K\}$，那么 K 为 S 在 F 上的分裂域，所以 K/F 是正规扩张. □

定理 1.53 的 (3) 通常用于判定某些扩张不是正规扩张.

例 1.54. $F \subseteq L \subseteq K$ 是域，如果 K/F 是正规扩张，那么 K/L 是正规扩张. 设 K 是 S 在 F 上的分裂域. 那么 S 作为 $L[x]$ 中的多项式集合在 K 上自然也是分裂的. 且 $K = F(X)$ 自然推出 $K = L(X)$，所以 K 也是 S 在 L 上的分裂域，故 K/L 是正规扩张. 但是 L/F 不一定是正规扩张，例如 $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$，此时 $\mathbb{Q}(\sqrt[3]{2}, \omega)$ 是 $x^3 - 2$ 在 $\mathbb{Q}$ 上的分裂域. 注意到 $\mathbb{Q}$ 上的不可约多项式 $x^3 - 2$ 在 $\mathbb{Q}(\sqrt[3]{2})$ 只有一个根 $\sqrt[3]{2}$，所以 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 不是正规扩张.

反之，若 K/L 和 L/F 都是正规扩张，K/F 也不一定是正规扩张. 例如 $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$，$\mathbb{Q}(\sqrt{2})$ 是 $x^2 - 2$ 在 $\mathbb{Q}$ 上的分裂域，$\mathbb{Q}(\sqrt[4]{2})$ 是 $x^2 - \sqrt{2}$ 在 $\mathbb{Q}(\sqrt{2})$ 上的分裂域. 但是 $\mathbb{Q}$ 上的不可约多项式 $x^4 - 2$ 在 $\mathbb{Q}(\sqrt[4]{2})$ 中只有两个根，所以 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ 不是正规扩张.

总结起来，这表明对于 $F \subseteq L \subseteq K$：

- K/F 是正规扩张 $\Rightarrow$ K/L 是正规扩张.
- K/F 是正规扩张 $\not\Rightarrow$ L/F 是正规扩张.
- $K/L, L/F$ 是正规扩张 $\not\Rightarrow$ K/F 是正规扩张.

1.4 可分与不可分扩张

本节我们研究 例 1.28 之前所说的阻止 $F(a)/F$ 成为 Galois 扩张的第二种情况，即 $\min(F, a)$ 零点在 $F(a)$ 中有重根.

令 $f(x) \in F[x]$，f 的根 α 如果满足 $(x - \alpha)^m \mid f(x)$ 但是 $(x - \alpha)^{m+1} \nmid f(x)$，那么我们说 α 是 f 的 m 重根. 若 $m > 1$，那么我们说 α 是 f 的重根. 注意，对于 $f(x) \in F[x]$，如果 f 在 F 中有 m 重根 α，那么其在 F 的任意扩域 K 中仍然有 m 重根 α. 反之，如果 f 在扩域 K 中有 m 重根 α，并且 $\alpha \in F$，那么 f 在 F 中也有 m 重根 α. 这是由域上多项式环的唯一因子分解性质决定的.

定义 1.55. 令 F 是域，不可约多项式 $f(x) \in F[x]$ 如果在分裂域中没有重根，那么我们说 f 在 F 上是**可分的**. 如果多项式 $g(x) \in F[x]$ 的所有不可约因子在 F 上都是可分的，那么我们说 g 在 F 上是**可分的**.

根据上面的叙述, 不难验证上述定义等价于 f 在 $\bar{F}$ 中无重根.

例 1.56. $x^2-2, (x-1)^9$ 在 $\mathbb{Q}$ 上是可分的. x^2+x+1 在 $\mathbb{F}_2$ 上是可分的. 下面是一个不可分多项式的例子. 令 k 是特征 p 的域, 考虑 $k(t^p)[x]$ 中的多项式 x^p-t^p. x^p-t^p 的分裂域为 $k(t)$, 因为在 $k(t)[x]$ 中有 $x^p-t^p=(x-t)^p$. 如果 $f(x) \in k(t^p)[x]$ 是 x^p-t^p 的因子, 那么在 $k(t)[x]$ 中有 $f \mid (x-t)^p$, 所以 $f(x)=(x-t)^k \in k(t)[x]$, 但是 $1<k<p$ 时 $f(x) \notin k(t^p)[x]$, 所以只可能 $f(x)=1$ 或者 $f(x)=x^p-t^p$. 这表明 x^p-t^p 是 $k(t^p)$ 上的不可约多项式, 但是其在分裂域 $k(t)$ 中有重根 t, 所以这是不可分多项式.

更一般地, 若 $\operatorname{char} F=p$ 且 $a \in F \setminus F^p$, 那么 x^p-a 不可约并且不可分, 因为它在任意 F 的扩域中至多只有一个根: 若 $r^p-a=s^p-a$, 那么 $(r-s)^p=r^p-s^p=0$, 所以 $r=s$.

引理 1.57. 令 $f(x), g(x) \in F[x]$，那么

(1) 如果 f 在分裂域中没有重根，那么 f 在 F 上可分.
(2) 如果 $g \mid f$ 并且 f 在 F 上可分，那么 g 在 F 上可分.
(3) 如果 $f_1, \ldots, f_n$ 在 F 上可分，那么 $f_1 \cdots f_n$ 在 F 上可分.
(4) 如果 f 在 F 上可分，那么 f 在 F 的任意扩域上可分.
(5) 如果 f 在 F 的某个扩域上可分，那么 f 在 F 上可分.

Proof. (1) 对于 f 的不可约因子 p, p 的分裂域被 f 的分裂域包含, 所以 p 在分裂域中没有重根, 即 p 在 F 上可分, 所以 f 在 F 上可分.

(2) g 的不可约因子也是 f 的不可约因子, 所以 g 在 F 上可分.

(3) $f_1 \cdots f_n$ 的不可约因子必为 $f_1, \ldots, f_n$ 中某个多项式的不可约因子, 所以 $f_1 \cdots f_n$ 在 F 上可分.

(4) 令 K 是 F 的扩域. 设 p 是 $f \in K[x]$ 的不可约因子, 令 α 是 $p(x)$ 在 $\bar{K}$ 中的根, 那么在 $K[x]$ 中有 $p(x) \mid \min(F, \alpha)$, 而 $\min(F, \alpha)$ 在 F 上可分, 所以 $\min(F, \alpha)$ 在 $\bar{F}$ 中没有重根, 那么 $\min(F, \alpha)$ 在 $\bar{K}$ 中也没有重根, 所以 $p(x)$ 在 $\bar{K}$ 中没有重根, 故 p 在 K 上可分, 所以 f 在 K 上可分.

(5) 设 K 是 F 的扩域, f 在 K 上可分. 设 p 是 f 的不可约因子. 那么 p 在 F 上的分裂域 L_1 被 p 在 K 上的分裂域 L_2 包含, 所以 p 在 L_1 中无重根, 即 p 在 F 上可分, 所以 f 在 F 上可分. □

为了有效地判断多项式的可分性, 我们需要引入形式导数.

定义 1.58. 对于 $f(x)=a_0+a_1x+\cdots+a_nx^n \in F[x]$, $f(x)$ 的**形式导数**定义为 $f'(x)=a_1+2a_2x+\cdots+na_nx^{n-1}$.

在特征零的域中, 上述定义和微积分中利用极限求得的导数没有区别. 但是在特征 p 的域中, 我们需要注意: x^p 的形式导数为 $px^{p-1}=0$.

形式导数满足与微积分中导数同样的性质: 如果 $f(x), g(x) \in F[x]$, 那么

(1) $(af(x) + bg(x))' = af'(x) + bg'(x)$;

(2) $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$;

(3) $(f(g(x)))' = f'(g(x))g'(x)$.

利用形式导数, 我们可以非常方便地判断多项式是否有重根. 若 $f(x) \in F[x]$ 在 f 的分裂域 K 中有根 α, 那么在 $K[x]$ 中可设 $f(x) = (x-\alpha)^m g(x)$, 其中 $m \geq 1$ 以及 $(x-\alpha) \nmid g(x)$. 此时 $f'(x) = m(x-\alpha)^{m-1}g(x) + (x-\alpha)^m g'(x)$, 不难注意到 α 是重根当且仅当 $m \geq 2$ 当且仅当 $(x-\alpha) \mid f'(x)$ 当且仅当 f, f' 在 K 中有公共根.

引理 1.59. 令 $f(x), g(x) \in F[x]$, K 是 F 的任意扩域. 设 $F[x]$ 中 $\gcd(f,g) = d$, $K[x]$ 中 $\gcd(f,g) = d'$, 那么实际上有 $d' = d \in F[x]$.

Proof. 由于 $d \in F[x] \subseteq K[x]$ 是 f, g 的公因子, 所以 $d \mid d'$. 另一方面, $F[x]$ 中 $\gcd(f,g) = d$ 表明存在 $h_1, h_2 \in F[x]$ 使得 $fh_1 + gh_2 = d$, 所以在 $K[x]$ 中有 $d' \mid (fh_1 + gh_2) = d$, 故 $d' = d$. □

命题 1.60. 令 $f(x) \in F[x]$ 是非常数多项式, 那么 f 在分裂域中无重根当且仅当 $\gcd(f, f') = 1$.

Proof. 若 f 无重根, 令 K 为 $\{f, f'\}$ 在 F 上的分裂域, 那么 f 在 K 上可分, 所以 f, f' 在 K 中没有公共根. 令 d 是 f, f' 在 $K[x]$ 中的最大公因子. 由于 f, f' 在 K 上分裂, 所以 d 也在 K 上分裂. 若 $\deg d \geq 1$, 那么 d 的任意根都是 f, f' 的公共根, 与上面矛盾. 所以 $d = 1$. 根据 引理 1.59, 在 $F[x]$ 中也有 $\gcd(f, f') = 1$.

若 $F[x]$ 中有 $\gcd(f, f') = 1$, 同样令 K 为 $\{f, f'\}$ 在 F 上的分裂域. 根据 引理 1.59, 在 $K[x]$ 中有 $\gcd(f, f') = 1$, 这表明 f, f' 在 K 中没有公共根, 从而在 f 的分裂域中也没有公共根, 所以 f 无重根. □

命题 1.61. $f(x) \in F[x]$ 是不可约多项式.

(1) 如果 $\mathrm{char}(F) = 0$, 那么 f 在 F 上可分. 如果 $\mathrm{char}(F) = p > 0$, 那么 f 在 F 上可分当且仅当 $f'(x) \neq 0$, 当且仅当 $f(x) \notin F[x^p]$.

(2) 如果 $\mathrm{char}(F) = p$, 那么存在 $m \geq 0$ 和不可约的可分多项式 $g(x) \in F[x]$, 使得 $f(x) = g(x^{p^m})$.

Proof. (1) 因为 f 不可约, 所以 $\gcd(f, f')$ 作为 f 的因子只可能等于 1 或者 f . 如果 $\mathrm{char}(F) = 0$, 那么 $\deg f' = \deg f - 1$, 所以 $f \nmid f'$, 所以 $\gcd(f, f') = 1$, 根据 命题 1.60, f 可分. 如果 $\mathrm{char}(F) = p$, 那么 f 不可分当且仅当 $\gcd(f, f') = f$, 当且仅当 $f \mid f'$, 当且仅当 $f'(x) = 0$, 当且仅当 $f(x) \in F[x^p]$.

(2) 对于 $r \geq 0$, 注意到 $F[x^{p^r}]$ 中非常数多项式至少是 p^r 次的, 所以只可能存在有限多个 $r_1, \ldots, r_k$ 使得 $f(x) \in F[x^{p^{r_i}}]$, 由于 $f(x) \in F[x]$, 所以 $k \geq 1$. 令 $m = \max\{r_1, \ldots, r_k\}$. 设 $f(x) = g(x^{p^m})$, 那么 $g(x) \notin F[x^p]$, 否则与 m 的最大性矛盾. 由 (1), g 在 F 上可分. □

定义 1.62. K/F 是域扩张, $\alpha \in K$. 如果 $\min(F, \alpha)$ 在 F 上可分, 那么我们说 α 在 F 上可分. 如果每个 $\alpha \in K$ 都在 F 上可分, 那么我们说 K/F 是**可分扩张**.

例 1.63. 如果 $\mathrm{char}(F) = 0$, 根据 命题 1.61, F 的任意代数扩张都是可分扩张. 如果 $\mathrm{char}(F) = p$, 根据 例 1.56, 对于域 k, 扩张 $k(t)/k(t^p)$ 不是可分扩张, 因为元素 t 在 $k(t^p)$ 上不可分.

现在我们可以说明 Galois 的代数扩张等价于正规可分扩张, 这是我们判断一个代数扩张是否为 Galois 扩张的一个最普遍的方法.

定理 1.64. *K/F 是代数扩张, 那么下面的说法是等价的.*

(1) *K/F 是 Galois 扩张.*

(2) *K/F 是正规可分扩张.*

(3) *K 是 F 上某一族可分多项式集合的分裂域.*

Proof. (1) $\Rightarrow$ (2) 若 K/F 是 Galois 扩张. 任取 $\alpha \in K$, 设 $\min(F,\alpha)$ 在 K 中的所有不同的根为 $\alpha_1 = \alpha, \ldots, \alpha_n$. 令 $f(x) = \prod(x - \alpha_i) = x^n + \beta_{n-1}x^{n-1} + \cdots + \beta_0 \in K[x]$. 任取 $\sigma \in \mathrm{Gal}(K/F)$, 由于 σ 是 $\alpha_1, \ldots, \alpha_n$ 的一个置换, 所以 $\sigma(f) = f$. 根据 σ 的任意性, 有 $\beta_i \in \mathrm{Fix}(\mathrm{Gal}(K/F)) = F$, 所以 $f(x) \in F[x]$. 因为 $f(\alpha) = 0$, 所以 $\min(F,\alpha) \mid f(x)$. 另一方面, 在 $K[x]$ 中有 $f(x) \mid \min(F,\alpha)$, 所以 $f(x) = \min(F,\alpha)$. 这表明 $\min(F,\alpha)$ 无重根且在 K 上分裂, 所以 K/F 是可分扩张, 同时 K 是 $\{\min(F,\alpha) \mid \alpha \in K\}$ 在 F 上的分裂域. 故 K/F 为正规可分扩张.

(2) $\Rightarrow$ (3) 若 K/F 为正规可分扩张.那么 K 是可分多项式集合 $\{\min(F,\alpha) \mid \alpha \in K\}$ 在 F 上的分裂域.

(3) $\Rightarrow$ (1) 首先假设 $[K : F] < \infty$. 对 $n = [K : F]$ 归纳. 若 $n = 1$, 那么 $K = F$, 此时 K/F 当然是 Galois 扩张. 现在假设 $n > 1$ 且结论对所有小于 n 的扩张成立. 若 K 是可分多项式集合 $\{f_i(x)\}$ 的分裂域且 $[K : F] = n$. $n > 1$ 表明存在某个 f_i 的根 α 不在 F 中, 令 $L = F(\alpha)$, 那么 $[L : F] > 1$, 所以 $[K : L] < n$. 此时 K 是 $\{f_i\}$ 在 L 上的分裂域, 根据归纳假设, K/L 是 Galois 扩张. 令 $H = \mathrm{Gal}(K/L)$ 是 $\mathrm{Gal}(K/F)$ 的子群, $\alpha_1, \ldots, \alpha_r \in L$ 是 $\min(F,\alpha)$ 的不同的根. 由于 α 在 F 上可分, 所以 $[L : F] = r$. 根据同构延拓定理, 存在 $\tau_i \in \mathrm{Gal}(K/F)$ 使得 $\tau_i(\alpha) = \alpha_i$. 注意到陪集 $\tau_i H$ 互不相同, 因为若 $\tau_i^{-1}\tau_j \in H$, 那么 $\tau_i^{-1}\tau_j(\alpha) = \alpha$, 即 $\alpha_i = \tau_i(\alpha) = \tau_j(\alpha) = \alpha_j$. 令 $G = \mathrm{Gal}(K/F)$, 我们有

$$|G| = [G : H]|H| \geq r|H| = [L : F][K : L] = [K : F],$$

又因为总是有 $|G| \leq [K : F]$, 所以 $|G| = [K : F]$, 即 K/F 是 Galois 扩张.

现在假设 K/F 是任意代数扩张. □

推论 1.65. *令 L/F 是有限扩张.*

(1) *L/F 可分当且仅当 L 被 F 的某个 Galois 扩张包含.*

(2) *如果 $L = F(\alpha_1, \ldots, \alpha_n)$, 其中 α_i 在 F 上可分, 那么 L/F 可分.*

Proof. (1) 若 $L \subseteq K$ 且 K/F 是 Galois 扩张, 那么 K/F 可分, 所以 L/F 可分. 反之, 若 L/F 可分, 因为 $[L : F] < \infty$, 所以可以假设 $L = F(\alpha_1, \ldots, \alpha_n)$, 其中每个 α_i 都在 F 上可分. 令 K 是 $\{\min(F,\alpha_i)\}$ 在 F 上的分裂域, 那么 K/F 正规可分, 所以是 Galois 扩张, 所以 L 被 Galois 扩张 K 包含.

(2) 和 (1) 的证明一致. □

那些所有代数扩张都可分的域是性质良好的, 我们现在来确定哪些域有这样的属性.

定义 1.66. 对于域 F, 如果 F 的每个代数扩张都是可分扩张, 那么说 F 是完全域.

例 1.67. 根据 命题 1.61, 特征零的域都是完全域. 任意代数闭域都是完全域, 因为它的代数扩张只有本身.

下面的定理刻画了素特征的完全域. 我们在 例 1.56 中已经发现, 如果 $a \in F \setminus F^p$, 那么 $x^p - a$ 是不可分的不可约多项式. 因此, 若 F 是完全域, 那么必须有 $F^p = F$. 我们现在证明这其实是一个充分必要条件.

定理 1.68. 令 F 是特征 p 的域, 那么 F 是完全域当且仅当 $F^p = F$.

Proof. 假设 F 是完全域, 若 $F^p \neq F$, 取 $a \in F^p \setminus F$, 令 K 是 $x^p - a$ 在 F 上的分裂域, 那么 $a^{1/p} \in K$ 不可分, 因为 $\min(F, a^{1/p}) = x^p - a$ 有重根, 这与 F 是完全域矛盾, 所以 $F^p = F$.

反之, 若 $F^p = F$. 令 K/F 是代数扩张, 任取 $\alpha \in K$, $p(x) = \min(F, \alpha)$. 根据 命题 1.61, 存在 $g(x) \in F[x]$ 使得 $p(x) = g(x^{p^m})$, 其中 g 不可约且可分. 如果 $g(x) = a_0 + a_1 x + \cdots + x^r$, 由于 $a_i \in F = F^p$, 所以存在 $b_i \in F$ 使得 $a_i = b_i^p$, 所以

$$p(x) = b_0^p + b_1^p x^{p^m} + \cdots + x^{rp^m} = \left(b_0 + b_1 x^{p^{m-1}} + \cdots + x^{rp^{m-1}}\right)^p,$$

而 p 不可约, 所以 $m = 0$, 即 $p = g$ 在 F 上可分. 这就表明 K/F 是可分扩张. □

例 1.69. 任意有限域都是完全域. 设 F 是有限域, $\varphi : F \to F$ 为 $\varphi(a) = a^p$, 那么 φ 是单射, F 是有限集表明 φ 是满射, 所以 $F = F^p$, 即 F 是完全域.

1.4.1 纯不可分扩张

现在我们讨论与可分性完全相反的概念. 这种情况只与素特征相关, 因为特征 0 的任意代数扩张都是可分扩张. 如果 F 是特征 $p > 0$ 的域, $a \in F$, 那么 $x^p - a$ 在任意分裂域中只有一个根. 这是因为如果 α 是一个根, 那么 $\alpha^p = a$, 即 $x^p - a = (x - \alpha)^p$.

定义 1.70. 令 K/F 是代数扩张, 如果 $\alpha \in K$ 使得 $\min(F, \alpha)$ 只有一个零点, 那么我们说 α 在 F 上**纯不可分**. 如果 K 的每个元素在 F 上都纯不可分, 那么我们说 K/F 是纯不可分扩张.

引理 1.71. 令 F 是特征 p 的域. 如果 α 在 F 上是代数的, 那么 α 纯不可分当且仅当存在某个 n 使得 $\alpha^{p^n} \in F$. 此时存在 m 使得 $\min(F, \alpha) = (x - \alpha)^{p^m}$.

Proof. 根据 命题 1.61, 存在不可约的可分多项式 $g(x) \in F[x]$ 使得 $\min(F, \alpha) = g(x^{p^n})$. 若 $g(x)$ 在分裂域中分裂为 $g(x) = (x - a_1) \cdots (x - a_r)$, 其中 $a_1, \ldots, a_r$ 互不相同. 于是 $\min(F, \alpha)$ 的零点为 $x^{p^n} = a_i$ 的所有解. α 纯不可分当且仅当 $\min(F, \alpha)$ 只有 α 一个零点, 所以 $r = 1$ 并且 $\alpha^{p^n} = a_1$, 此时 $\min(F, \alpha) = x^{p^n} - a_1 \in F[x]$, 故 $\alpha^{p^n} = a_1 \in F$.

反之, 若 $\alpha^{p^n} \in F$, 那么 α 是多项式 $x^{p^n} - \alpha^{p^n} \in F[x]$ 的零点, 所以 $\min(F,\alpha) \mid (x-\alpha)^{p^n}$, 所以 $\min(F,\alpha)$ 只有 α 一个零点, 即 α 纯不可分. □

引理 1.72. 令 K/F 是代数扩张.

(1) 如果 $\alpha \in K$ 在 F 上同时可分以及纯不可分, 那么 $\alpha \in F$.

(2) 如果 K/F 纯不可分, 那么 K/F 是正规扩张并且 $\mathrm{Gal}(K/F) = \{\mathrm{id}\}$. 此外, 如果 $[K:F] < \infty$, $\mathrm{char}(F) = p$, 那么 $[K:F] = p^n$.

(3) 如果 $K = F(X)$, 其中每个 $\alpha \in X$ 都在 F 上纯不可分, 那么 K/F 纯不可分.

(4) 如果 $F \subseteq L \subseteq K$ 是域, 那么 K/F 纯不可分当且仅当 K/L 和 L/F 都纯不可分.

Proof. (1) α 同时可分和纯不可分表明 $\min(F,\alpha)$ 无重根且只有 α 一个零点, 所以 $\min(F,\alpha) = x - \alpha$, 即 $\alpha \in F$.

(2) 任取 $\alpha \in K$, 根据 引理 1.71, α 纯不可分表明 $\min(F,\alpha) = (x-\alpha)^{p^m}$, 所以 $\min(F,\alpha)$ 在 K 上分裂, 故 K/F 是正规扩张. 任取 $\sigma \in \mathrm{Gal}(K/F)$, 那么对于任意 $\alpha \in K$ $\sigma(\alpha)$ 是 $\min(F,\alpha)$ 的根, 所以 $\sigma(\alpha) = \alpha$, 即 $\sigma = \mathrm{id}$, 即 $\mathrm{Gal}(K/F) = \{\mathrm{id}\}$. 若 $[K:F] < \infty$, 设 $K = F(\alpha_1, \dots, \alpha_n)$. 由于 $[F(\alpha_1,\dots,\alpha_i) : F(\alpha_1,\dots,\alpha_{i-1})]$ 都是 p 的幂次, 所以 $[K:F]$ 是 p 的幂次.

(3) 任取 $a \in K$, 那么存在 $\alpha_1, \dots, \alpha_n \in X$ 使得 $a \in F(\alpha_1,\dots,\alpha_n)$. 对于每个 α_i, 存在 m_i 使得 $\alpha_i^{p^{m_i}} \in F$, 那么 a 作为 $\alpha_1,\dots,\alpha_n$ 的多项式, 自然有 $a^{p^m} \in F$, 所以 a 在 F 上纯不可分.

(4) 若 K/F 纯不可分. 任取 $\alpha \in K$, 那么 $\alpha^{p^n} \in F \subseteq L$, 所以 α 在 L 上纯不可分. L/F 纯不可分也是显然的. 反之, 若 $K/L, L/F$ 纯不可分. 任取 $\alpha \in K$, 那么 $\alpha^{p^n} \in L$, 进而 $(\alpha^{p^n})^{p^m} \in F$, 即 $\alpha^{p^{m+n}} \in F$, 所以 α 在 F 上纯不可分. □

例 1.73. 域扩张可能是既不可分又不是纯不可分的. 例如, 若 $F = \mathbb{F}_2(x)$, $K = F(x^{1/6})$. 那么 $K = \mathbb{F}_2(x^{1/6}) = \mathbb{F}_2(\sqrt{x}, \sqrt[3]{x})$. 此时 $\sqrt{x}$ 在 F 上纯不可分, $\sqrt[3]{x}$ 在 F 上可分. 故 $F(\sqrt{x})/F$ 是纯不可分扩张, $F(\sqrt[3]{x})/F$ 是可分扩张, 这表明 K/F 既不是纯不可分扩张又不是可分扩张.

定义 1.74. 令 K/F 是域扩张. 那么 F 在 K 中的**可分闭包**定义为集合

$$\{a \in K \mid a \text{ is separable over } F\}.$$

F 在 K 中的**纯不可分闭包**定义为集合

$$\{a \in K \mid a \text{ is purely inseparable over } F\}.$$

命题 1.75. K/F 是域扩张. 设 S, I 分别是 F 在 K 中的可分闭包与纯不可分闭包. 那么 S, I 是 F 的扩域且 S/F 可分, I/F 纯不可分, 以及 $S \cap I = F$. 如果 K/F 是代数扩张, 那么 K/S 是纯不可分扩张.

Proof. 任取 $a, b \in S$, 根据 推论 1.65, $F(a,b)/F$ 是可分扩张, 所以 S 是域. 任取 $c, d \in I$, 那么 $c^{p^n}, d^{p^m} \in F$, 于是 $(c \pm d)^{p^{n+m}} \in F$, 以及 $(cd)^{p^{n+m}}, (c/d)^{p^{n+m}} \in F$, 所以 $c \pm d, cd, c/d \in I$, 所以 I 也是域. 根据定义, S/F 可分, I/F 纯不可分. 根据 引理 1.72, 有 $S \cap I = F$.

若 K/F 是代数扩张. 任取 $\alpha \in K$, 设 $\min(F,\alpha) = g(x^{p^m})$, 其中 g 是不可约的可分多项式. 由于 α^{p^m} 是 g 的零点, 所以 $g(x)$ 是 α^{p^m} 在 F 上的最小多项式, 所以 α^{p^m} 在 F 上可分, 故 $\alpha^{p^m} \in S$, 所以 α 在 S 上纯不可分. □

如果 K/F 是代数扩张, 那么我们可以把 K/F 分为可分扩张 S/F 以及一个纯不可分扩张 K/S. 可分闭包是一个处理可分性问题的非常棒的工具. 例如, 我们证明可分性是可以传递的.

命题 1.76. 如果 $F \subseteq L \subseteq K$ 是域且 $L/F, K/L$ 是可分扩张, 那么 K/F 可分.

Proof. 记 S 是 F 在 K 中的可分闭包. 那么 $L \subseteq S \subseteq K$. K/L 可分表明 K/S 可分, 同时 K/S 又纯不可分, 所以 $S = K$, 即 K/F 可分. □

命题 1.75 告诉我们 K/S 纯不可分. 一个自然的问题是 K/I 是否可分. 一般情况下这是不对的, 但是在 K/F 是正规扩张的情况下是正确的.

定理 1.77. K/F 是正规扩张, S, I 分别是 F 在 K 中的可分闭包与纯不可分闭包. 那么 S/F 是 Galois 扩张, $I = \mathrm{Fix}(\mathrm{Gal}(K/F))$, 并且 $\mathrm{Gal}(S/F) \simeq \mathrm{Gal}(K/I)$. 因此, K/I 是 Galois 扩张. 此外, 还有 $K = SI$.

K/F 是域扩张. 设 S, I 分别是 F 在 K 中的可分闭包与纯不可分闭包. 我们可以定义 K/F 的**可分次数** $[K:F]_s$ 为 $[S:F]$, 以及**不可分次数** $[K:F]_i$ 为 $[K:S]$. 那么我们有 $[K:F] = [K:F]_i[K:F]_s$. 定理 1.77 还告诉我们在 K/F 正规的时候, 有 $[K:I] = [S:F]$, 因此有 $[K:S] = [I:F]$. 需要注意一般情况下并没有 $[K:S] = [I:F]$! 将不可分次数定义为 $[K:S]$ 而不是 $[I:F]$ 是因为 $[K:S]$ 通常可以更好的衡量 K/F 距离可分扩张有多远. 下面的例子表明在 K/F 不可分的时候也有可能有 $I = F$.

1.5 Galois 理论基本定理

定理 1.78 (Galois 理论基本定理). 令 K/F 是有限 Galois 扩张, $G = \mathrm{Gal}(K/F)$, 那么在 K/F 的中间域和 G 的子群之间存在一一对应, 由 $L \mapsto \mathrm{Gal}(K/L)$ 和 $H \mapsto \mathrm{Fix}(H)$ 给出. 如果 $L \leftrightarrow H$, 那么 $[K:L] = |H|$ 并且 $[L:F] = [G:H]$. 此外, H 是 G 的正规子群当且仅当 L/F 是 Galois 扩张, 此时 $\mathrm{Gal}(L/F) \simeq G/H$.

$$
\begin{array}{ccc}
K & \longleftrightarrow & \mathrm{Gal}(K/K) = 0 \\
\cup\!| & & \wedge \\
L & \longleftrightarrow & \mathrm{Gal}(K/L) = H \\
\cup\!| & & \wedge \\
F & \longleftrightarrow & \mathrm{Gal}(K/F) = G
\end{array}
$$

定理 1.79 (本原元定理). 有限扩张 K/F 是单扩张当且仅当只存在有限多个中间域 L 使得 $F \subseteq L \subseteq K$.

Proof. 我们仅对无限域的情况做证明, 有限域的情况留到下一节中. 由于 $[K:F]<\infty$, 所以设 $K=F(\alpha_1,\dots,\alpha_n)$. 对 n 归纳, 当 $n=1$ 时结论显然成立. 假设 $n-1$ 时成立, 对于 $n>1$ 的时候, 根据假设, 有 $\beta\in K$ 使得 $F(\beta)=F(\alpha_1,\dots,\alpha_{n-1})$, 所以 $K=F(\alpha_n,\beta)$. 任取 $a\in F$, 考虑 $M_a=F(\alpha_n+a\beta)$, 显然 $F\subseteq M_a\subseteq K$. 由于 F 有无限个元素, 所以一定存在 $a\neq b$ 使得 $M_a=M_b$. 注意到

$$\beta=\frac{(\alpha_n+a\beta)-(\alpha_n+b\beta)}{a-b}\in M_a,$$

所以 $\alpha_n=(\alpha_n+a\beta)-a\beta\in M_a$, 所以 $K=M_a$, 即 K 是 F 的单扩张.

反之, 假设存在某个 $\alpha\in K$ 使得 $K=F(\alpha)$. 设 M 使得 $F\subseteq M\subseteq K$, 那么 $K=M(\alpha)$. 记 $q(x)=\min(M,\alpha)\in M[x]$, 设 $q(x)=a_0+a_1x+\cdots+x^r$, 考虑 $M_0=F(a_0,\dots,a_{r-1})$, 那么 $M_0\subseteq M$ 且 $q(x)\in M_0[x]$. 因为 $\min(M_0,\alpha)\mid q(x)$, 所以

$$[K:M]=q\geq\deg(\min(M_0,\alpha))=[K:M_0]=[K:M][M:M_0],$$

所以 $M=M_0$, 这表明 M 完全由多项式 q 确定. 记 $p(x)=\min(F,\alpha)$, 那么 $q\mid p$, 所以这样的 q 只有有限多个, 即 K/F 只有有限多个中间域. □

推论 1.80. 若 K/F 是有限可分扩张, 那么 K/F 是单扩张.

Proof. 设 $K=F(\alpha_1,\dots,\alpha_n)$, 令 N 为 $\{\min(F,\alpha_i)\}$ 在 F 上的分裂域, 根据 定理 1.64, N/F 是 Galois 扩张. 此时 $F\subseteq K\subseteq N$. 根据基本定理, N/F 的中间域和有限群 $\mathrm{Gal}(N/F)$ 的子群一一对应, 所以 N/F 只有有限多个中间域, 即 K/F 只有有限多个中间域, 所以 K/F 是单扩张. □

推论 1.81. 如果 K/F 是有限扩张且 $\mathrm{char}(F)=0$, 那么 K/F 是单扩张.

Proof. 特征零的域都是完全域. □

2

典型的 Galois 扩张

2.1 有限域

如果 F 是特征 p 的有限域, 那么 F 包含 $\mathbb{F}_p$, 所以 F 可以视为 $\mathbb{F}_p$-向量空间, F 有限表明维数是有限维的, 即可以假设 $[F:\mathbb{F}_p]=n$. 根据线性代数的基本知识, 我们知道 F 同构于 $\mathbb{F}_p^n$, 所以 $|F|=p^n$. 为了研究有限域, 我们首先研究 $F^\times$ 的群结构, 实际上有限域的乘法群的群结构决定了有限域的很多性质.

首先证明一个群论的结论.

引理 2.1. 设 G 是 n 阶有限群, 如果对于任意正整数 m, 方程 $x^m=e$ 在 G 中最多只有 m 个解, 那么 G 是循环群.

Proof. 记集合

$$A_d=\{g\in G\mid \operatorname{ord}(g)=d\},\quad S_d=\{g\in G\mid g^d=e\}.$$

显然 $A_d\subseteq S_d$. 若 $d\nmid n$, 那么 $A_d=\varnothing$. 若 $d\mid n$ 且 $A_d\neq\varnothing$, 设 $a\in A_d$, 那么 $\langle a\rangle\subseteq S_d$. 根据条件, 我们有 $|S_d|\leq d=|\langle a\rangle|$, 所以 $S_d=\langle a\rangle$. 于是 $A_d\subseteq\langle a\rangle$. $\langle a\rangle$ 的生成元有 $\varphi(d)$ 个, 所以 $|A_d|=\varphi(d)$. 这表明 $d\mid n$ 的时候, 要么 $|A_d|=0$, 要么 $|A_d|=\varphi(d)$.

又因为 $G=\bigcup_{d\mid n}A_d$, 所以

$$n=|G|=\sum_{d\mid n}|A_d|\leq\sum_{d\mid n}\varphi(d)=n,$$

所以 $d\mid n$ 的时候必须有 $|A_d|=\varphi(d)$. 这表明 $|A_n|\neq 0$, 即 G 中存在 n 阶元. □

推论 2.2. 若 F 是有限域, 那么 $F^\times$ 是循环群.

Proof. 对于任意正整数 m, 方程 $x^m=1$ 在 F 中最多只有 m 个解, 所以在 $F^\times$ 中最多也只有 m 个解, 所以 $F^\times$ 是循环群. □

例 2.3. $\mathbb{F}_p^\times$ 的生成元被称为**模 p 的原根**. 例如, $\mathbb{F}_5^\times=\{1,2,3,4\}=\langle 2\rangle$, 即 2 是模 5 的原根. 又比如 3 是模 7 的原根. 一般来说, 没有一种简单的方式去寻找模 p 的原根.

定理 1.79 证明了无限域情况下的本原元定理, 下面我们证明有限域情况下的. 注意到如果 K/F 是有限域的扩张, 那么 K/F 显然只有有限个中间域, 因此本原元定理的假设始终成立. 下面的推论完成了有限域情况下的本原元定理.

推论 2.4. 如果 K/F 是有限域的扩张，那么 K 是 F 的单扩张.

Proof. 设 $K^\times = \langle \alpha \rangle$，那么 K 的任意非零元都是 α 的幂次，所以 $K = F(\alpha)$. □

定理 2.5 (有限域的结构定理). 令 F 的特征 p 的有限域，设 $|F| = p^n$. 那么 F 是可分多项式 $x^{p^n} - x$ 在 $\mathbb{F}_p$ 上的分裂域，所以 $F/\mathbb{F}_p$ 是 Galois 扩张. 此外，如果定义 $\sigma : F \to F$ 为 $\sigma(a) = a^p$，那么 σ 生成 $\mathrm{Gal}(F/\mathbb{F}_p)$，故 Galois 群 $\mathrm{Gal}(F/\mathbb{F}_p)$ 是循环群. 这个自同构 σ 被称为 **Frobenius 自同构**.

Proof. 根据导数判别法，$x^{p^n} - x$ 是可分多项式. 由于 $|F^\times| = p^n - 1$，所以任意 $a \in F^\times$ 满足 $a^{p^n-1} = 1$，也即 $a^{p^n} - a = 0$，显然 0 也满足这个方程，所以 F 的元素均为 $x^{p^n} - x$ 的零点. 又因为 $x^{p^n} - x$ 至多只有 p^n 个零点，所以 F 的元素恰为 $x^{p^n} - x$ 的全部零点，故 F 是 $x^{p^n} - x$ 的分裂域. 根据 定理 1.64，$F/\mathbb{F}_p$ 是 Galois 扩张.

不难验证 σ 是一个 $\mathbb{F}_p$-单同态. F 有限表明 σ 是满射，所以是 $\mathbb{F}_p$-自同构，所以 $\sigma \in \mathrm{Gal}(F/\mathbb{F}_p)$. 注意到 $\mathrm{Fix}(\langle\sigma\rangle) = \{a \in F \mid a^p = a\} \supseteq \mathbb{F}_p$，且 $x^p - x$ 最多只有 p 个零点，所以 $\mathbb{F}_p = \mathrm{Fix}(\langle\sigma\rangle)$. 所以 $\mathrm{Gal}(F/\mathbb{F}_p) = \mathrm{Gal}(F/\mathrm{Fix}(\langle\sigma\rangle)) = \langle\sigma\rangle$. □

推论 2.6. 任意两个相同大小的有限域是同构的.

Proof. p^n 阶有限域是 $x^{p^n} - x$ 在 $\mathbb{F}_p$ 上的分裂域，所以它们是同构的. □

实际上 定理 2.5 可以刻画任意有限域的扩张，而不必从 $\mathbb{F}_p$ 开始.

推论 2.7. 如果 K/F 是有限域的域扩张，那么 K/F 是具有循环 Galois 群的 Galois 扩张. 此外，如果 $\mathrm{char}(F) = p$ 以及 $|F| = p^n$，那么 $\mathrm{Gal}(K/F)$ 由自同构 τ 生成，其中 $\tau(a) = a^{p^n}$.

Proof. 设 $[K : \mathbb{F}_p] = m$，那么 K 是 $x^{p^m} - x$ 在 $\mathbb{F}_p$ 上的分裂域，从而也是 $x^{p^m} - x$ 在 F 上的分裂域，所以 K/F 是 Galois 扩张. 由于 $\mathrm{Gal}(K/F)$ 是 $\mathrm{Gal}(K/\mathbb{F}_p)$ 的子群，所以 $\mathrm{Gal}(K/F)$ 是循环群. 记 σ 是 Frobenius 自同构，设 $s = |\mathrm{Gal}(K/F)| = [K : F]$，那么 $m = ns$，所以 $\mathrm{Gal}(K/F)$ 的生成元是 σ^n，满足 $\sigma^n(a) = a^{p^n}$. □

我们已经描述了有限域作为 $\mathbb{F}_p$ 的扩域时的结构，并且知道 $\mathbb{F}_p$ 的任意有限扩张都有 p^n 个元素. 但是，我们还没有确定是否对于每个 n，都存在 p^n 个元素的有限域. 利用基本定理和有限域的结构定理，我们现在证明对于每个 n，确实存在唯一的 p^n 个元素的有限域.

定理 2.8. 令 N 是 $\mathbb{F}_p$ 的代数闭包. 对于每个正整数 n，存在唯一的 p^n 个元素的 N 的子域. 如果 K, L 分别是 p^m, p^n 阶子域，那么 $K \subseteq L$ 当且仅当 $m \mid n$. 此时，L/K 是 Galois 扩张，并且 $\mathrm{Gal}(L/K) = \langle\tau\rangle$，其中 $\tau(a) = a^{p^m}$.

Proof. 对于每个正整数 n，多项式 $x^{p^n} - x$ 在 N 中有 p^n 个根，这些根的集合构成一个域，即 p^n 个元素的子域. 根据 定理 2.5，N 的任意 p^n 阶子域都由 $x^{p^n} - x$ 的所有根组成，所以是唯一的.

若 K, L 分别是 p^m, p^n 阶子域. 假设 $K \subseteq L$，那么 $\mathbb{F}_p \subseteq K \subseteq L$，所以

$$n = [L : \mathbb{F}_p] = [L : K][K : \mathbb{F}_p] = [L : K]m,$$

所以 $m \mid n$. 反之, 若 $m \mid n$, 任取 $a \in K$, 那么 $a^{p^m} = a$, 从而 $a^{p^n} = a$, 所以 $a \in L$, 即 $K \subseteq L$. 根据 推论 2.7, L/K 是 Galois 扩张, 并且 $\mathrm{Gal}(L/K)$ 由 $\tau(a) = a^{p^m}$ 生成. □

推论 2.9. 令 F 是有限域, $f(x)$ 是 F 上的 n 次首一不可约多项式.

(1) 如果 a 是 f 在 F 的任意扩域中的根, 那么 $F(a)$ 是 f 在 F 上的分裂域. 因此, 如果 K 是 f 在 F 上的分裂域, 那么 $[K : F] = n$.

(2) 如果 $|F| = q$, 那么 f 的根的集合为 $\{a^{q^r} \mid r \geq 1\}$.

Proof. 令 K 是 f 在 F 上的分裂域. 若 $a \in K$ 是 f 的根, 考虑 $F(a)$, 此时 $[F(a) : F] = n$, 所以 $|F(a)| = q^n$. 由于 $F(a)/F$ 是 Galois 扩张, 所以 $f = \min(F, a)$ 在 $F(a)$ 中分裂, 所以 $K \subseteq F(a)$, 故 $F(a) = K$ 是 f 在 F 上的分裂域以及 $[K : F] = n$.

由于 $\mathrm{Gal}(K/F) = \langle \tau \rangle$, 对于 $x \in K$ 有 $\tau(x) = x^q$. 由于 $a \in K$ 是 f 的根, 所以对于任意 $r \geq 1$, $a^{q^r} = \tau^r(a)$ 都是 f 的根. 再根据同构延拓定理, 对于 f 的任意根 a', 都存在某个 r 使得 $\tau^r(a) = a'$, 故 f 的根的集合恰为 $\{a^{q^r} \mid r \geq 1\}$. □

例 2.10. 考虑 $K = \mathbb{F}_2(\alpha)$, 其中 α 是 $f(x) = x^3 + x^2 + 1$ 的根. 多项式 f 在 $\mathbb{F}_2$ 中没有零点, 直接计算可知 f 是不可约多项式, 所以 $[K : \mathbb{F}_2] = 3$. 现在我们知道 K 是 f 在 $\mathbb{F}_2$ 上的分裂域, 并且 f 的所有根为 $\alpha, \alpha^2, \alpha^4$. 我们可以验证这一点. 因为 $\alpha^3 + \alpha^2 + 1 = 0$, 所以

$$\alpha^6 + \alpha^4 + 1 = (\alpha^3 + \alpha^2)^2 + 1 = 0,$$
$$\alpha^{12} + \alpha^8 + 1 = (\alpha^3 + \alpha^2)^4 + 1 = 0.$$

注意到 $\alpha^4 = (\alpha^2 + 1)\alpha = \alpha^2 + \alpha + 1$, 所以 $\{1, \alpha, \alpha^2\}$ 构成 $K/\mathbb{F}_2$ 的一组基, 这就表明 $\mathbb{F}_2(\alpha)$ 确实是 f 在 $\mathbb{F}_2$ 上的分裂域.

例 2.11. 令 $f(x) = x^2 + 1$, 如果 p 是奇素数, 我们证明 f 在 $\mathbb{F}_p$ 上可约当且仅当 $p \equiv 1 \pmod 4$. 设 $a \in \mathbb{F}_p$ 是 f 的零点, 那么 $a^4 = 1$, 即 a 是 $\mathbb{F}_p^\times$ 的 4 阶元, 所以 $4 \mid p - 1$, 即 $p \equiv 1 \pmod 4$. 反之, 若 $p \equiv 1 \pmod 4$, 由于 $\mathbb{F}_p^\times$ 是 $p - 1$ 阶循环群, 所以存在 4 阶元 a, 那么 $a^2 \neq 1$, 这只可能 $a^2 = -1$, 所以 a 是 f 的零点.

2.2 分圆扩张

一个域的 n 次单位根指的是满足 $\omega^n = 1$ 的元素 ω, 为了强调 n, 有时我们写作 ω_n. 例如, 复数 $\zeta_n = e^{2\pi i/n}$ 是一个 n 次单位根. 本节我们研究域扩张 $F(\omega)/F$. 这个扩张在 Galois 理论的应用中扮演着重要角色, 尤其是在多项式方程的可解性问题上.

定义 2.12. 如果 $\omega \in F$ 满足 $\omega^n = 1$, 那么说 ω 是 n 次单位根. 如果 ζ_n 是乘法群 $F^\times$ 的 n 阶元, 那么说 ζ_n 是 n 次本原单位根. 对于任意单位根 ω, 域扩张 $F(\omega)/F$ 被称为分圆扩张.

我们首先指出关于单位根的两个事实. 第一点, 如果 $\zeta_n \in F$ 是本原单位根, 那么 $\mathrm{char}(F) \nmid n$. 这是因为如果特征 $p \mid n$, 设 $n = pm$, 那么 $(\zeta_n^m - 1)^p = \zeta_n^n - 1 = 0$, 所以

$\zeta_n^m = 1$, 这与 ζ_n 是本原单位根矛盾. 第二点, 如果 ω_n 是单位根, 那么 ω_n 在 $F^\times$ 中的阶整除 n, 并且设 ω_n 的阶是 $m \mid n$, 那么 ω_n 实际上是 m 次本原单位根.

注意到域 F 的 n 次单位根就是 $x^n - 1$ 的根的集合, 不难验证所有的 n 次单位根构成一个群, 其作为 $F^\times$ 的有限子群, 是一个循环群, 此时这个循环群的生成元就是一个 n 次本原单位根.

命题 2.13. 设 $\mathrm{char}(F) \nmid n$, K 是 $x^n - 1$ 在 F 上的分裂域, 那么 K/F 是 Galois 扩张并且 $K = F(\zeta_n)$, $\mathrm{Gal}(K/F)$ 同构于 $(\mathbb{Z}/n\mathbb{Z})^\times$ 的一个子群. 因此, $\mathrm{Gal}(K/F)$ 是 Abelian 群并且 $[K : F] \mid \varphi(n)$.

Proof. 根据导数判别法, $x^n - 1$ 是可分多项式, 所以 K/F 是 Galois 扩张. 由于 ζ_n 是本原单位根, 所以 $x^n - 1$ 的任意根都是 ζ_n 的幂次, 所以 $K = F(\zeta_n)$.

任取 $\sigma \in \mathrm{Gal}(K/F)$, σ 由 $\sigma(\zeta_n)$ 完全确定. σ 是自同构表明 σ 把 ζ_n 送到另一个本原单位根, 故 $\sigma(\zeta_n) = \zeta_n^t$, 其中 $(t, n) = 1$. 定义 $\theta : \mathrm{Gal}(K/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$ 为 $\sigma \mapsto t$. 设 $\sigma(\zeta_n) = \zeta_n^t$ 以及 $\tau(\zeta_n) = \zeta_n^s$, 那么 $\sigma\tau(\zeta_n) = \zeta_n^{st}$, 这表明 θ 是群同态. 若 $\theta(\sigma) = 0$, 那么 $\sigma(\zeta_n) = \zeta_n$, 所以 θ 是单同态, 这就表明 $\mathrm{Gal}(K/F)$ 同构于 $(\mathbb{Z}/n\mathbb{Z})^\times$ 的一个子群. □

例 2.14. 设 $n \geq 3$, 那么 $\mathbb{R}(\zeta_n) = \mathbb{C}$, 因为 $\mathbb{R}(\zeta_n) \subseteq \mathbb{C}$ 并且 $[\mathbb{C} : \mathbb{R}] = 2$, 所以 $\zeta_n \notin \mathbb{R}$ 就表明 $\mathbb{R}(\zeta_n) = \mathbb{C}$.

例 2.15. 考虑 $\mathbb{F}_2(\zeta_7)$. 计算可得 $x^7 - 1$ 有分解

$$x^7 - 1 = (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1),$$

所以 $\min(\mathbb{F}_2, \zeta_7) = x^3 + x + 1$ 或者 $\min(\mathbb{F}_2, \zeta_7) = x^3 + x^2 + 1$, 即 $[\mathbb{F}_2(\zeta_7) : \mathbb{F}_2] = 3$. 这表明 $\mathbb{F}_2$ 上的 7 次本原单位根有 6 个, 其中 3 个是多项式 $x^3 + x + 1$ 的根, 另外 3 个是多项式 $x^3 + x^2 + 1$ 的根, 所以造成扩张次数是 3 而不是 $\varphi(7) = 6$. 我们将看到, 这与 $\mathbb{Q}$ 上的情况大不相同, 即 $\mathbb{Q}$ 上的分圆扩张的次数 $[\mathbb{Q}(\zeta_n), \mathbb{Q}]$ 一定等于 $\varphi(n)$.

现在我们研究 $\mathbb{Q}$ 的分圆扩张, 令 ζ_n 是 $\mathbb{C}$ 中的 n 次本原单位根, 那么 $\zeta_n = e^{2k\pi i/n}$, 其中 $(k, n) = 1$.

定义 2.16. 定义 n 次分圆多项式 $\Phi_n(x) = \prod(x - \zeta_n) \in \mathbb{C}[x]$, 其中乘积取遍所有的 n 次本原单位根.

例如:

$$\begin{aligned}
\Phi_1(x) &= x - 1, \\
\Phi_2(x) &= x + 1, \\
\Phi_4(x) &= (x - i)(x + i) = x^2 + 1.
\end{aligned}$$

此外, 如果 p 是素数, 那么 p 次本原单位根恰为所有的 $e^{2k\pi i/p}$ $(1 \leq k \leq p - 1)$, 所以

$$\Phi_p(x) = \frac{x^n - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

引理 2.17. 我们有 $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$. 此外, $\Phi_n(x) \in \mathbb{Z}[x]$.

Proof. 由于 $x^n-1=\prod(x-\omega_n)$, 乘积取遍所有的 n 次单位根. 对于每个 $d\mid n$, 把 d 次本原单位根的乘积合在一起, 即得 $x^n-1=\prod_{d\mid n}\Phi_d(x)$.

对 n 归纳. 显然 $\Phi_1(x)\in\mathbb{Z}[x]$. 假设在 $d<n$ 的时候有 $\Phi_d(x)\in\mathbb{Z}[x]$, 那么

$$x^n-1=\left(\prod_{d\mid n,d<n}\Phi_d(x)\right)\Phi_n(x),$$

由于 x^n-1 和 $\prod_{d\mid n,d<n}\Phi_d(x)$ 都在 $\mathbb{Z}[x]$ 中, 根据带余除法, 就有 $\Phi_n(x)\in\mathbb{Z}[x]$. □

定理 2.18. $\Phi_n(x)$ 在 $\mathbb{Q}$ 上不可约.

推论 2.19. 如果 $K=\mathbb{Q}(\zeta_n)$ 是 x^n-1 在 $\mathbb{Q}$ 上的分裂域, 那么 $[K:\mathbb{Q}]=\varphi(n)$ 且 $\mathrm{Gal}(K/\mathbb{Q})\simeq(\mathbb{Z}/n\mathbb{Z})^\times$. 此外, $\mathrm{Gal}(K/\mathbb{Q})=\{\sigma_i\mid(i,n)=1\}$, 其中 σ_i 满足 $\sigma_i(\zeta_n)=\zeta_n^i$.

Proof. $\Phi_n(x)$ 不可约就表明 $\min(\mathbb{Q},\zeta_n)=\Phi_n(x)$, 所以 $[K:\mathbb{Q}]=\deg\Phi_n(x)=\varphi(n)$. 所以 $\mathrm{Gal}(K/\mathbb{Q})$ 有 $\varphi(n)$ 个元素, 从而必须有 $\mathrm{Gal}(K/\mathbb{Q})\simeq(\mathbb{Z}/n\mathbb{Z})^\times$. □

例 2.20. 我们研究 $\mathbb{Q}(\zeta_7)/\mathbb{Q}$. 此时 $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})\simeq\mathbb{F}_7^\times$ 是循环群. 记 $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})=\{\sigma_1,\dots,\sigma_6\}$, 由于 $\mathbb{F}_7^\times=\langle 3\rangle$, 所以 $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})=\langle\sigma_3\rangle$, 满足 $\sigma_3(\zeta_7)=\zeta_7^3$. 于是 $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$ 的所有子群为

$$0,\ \langle\sigma_3^3\rangle,\ \langle\sigma_3^2\rangle,\ \langle\sigma_3\rangle.$$

我们寻找对应的中间域. 记 $L=\mathrm{Fix}(\sigma_3^3)=\mathrm{Fix}(\sigma_6)$, 那么 $[\mathbb{Q}(\zeta_7):L]=|\langle\sigma_6\rangle|=2$ 以及 $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/L)=\langle\sigma_6\rangle$, 这意味着 $\min(L,\zeta_7)$ 是 2 次多项式并且有根 $\zeta_7,\zeta_7^6=\sigma_6(\zeta_7)$, 所以

$$\min(L,\zeta_7)=(x-\zeta_7)(x-\zeta_7^6)=x^2-(\zeta_7+\zeta_7^6)x+1,$$

所以 $\zeta_7+\zeta_7^6\in L$. 如果令 $\zeta_7=e^{2\pi i/7}$, 那么 $\zeta_7+\zeta_7^6=2\cos(2\pi/7)$. 因此 $\mathbb{Q}(\cos(2\pi/7))\subseteq L$. 此时 $\min(L,\zeta_7)$ 也是 $\mathbb{Q}(\cos(2\pi/7))$ 上的多项式, 所以 $[\mathbb{Q}(\zeta_7):\mathbb{Q}(\cos 2\pi/7)]$ 最多是 2 次的, 这就表明 $L=\mathbb{Q}(\cos 2\pi/7)$.

记 $K=\mathrm{Fix}(\sigma_3^2)=\mathrm{Fix}(\sigma_2)$, 那么 $[\mathbb{Q}(\zeta_7):K]=|\langle\sigma_2\rangle|=3$ 以及 $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/K)=\langle\sigma_2\rangle$. 于是

$$\min(K,\zeta_7)=(x-\zeta_7)(x-\zeta_7^2)(x-\zeta_7^4),$$

所以常数项 $\zeta_7+\zeta_7^2+\zeta_7^4\in K$. 此时 $[K:\mathbb{Q}]=2$, 我们只需要说明 $\zeta_7+\zeta_7^2+\zeta_7^4\notin\mathbb{Q}$ 即可表明 $K=\mathbb{Q}(\zeta_7+\zeta_7^2+\zeta_7^4)$. 注意到

$$\sigma_6(\zeta_7+\zeta_7^2+\zeta_7^4)=\zeta_7^6+\zeta_7^5+\zeta_7^3,$$

如果 $\zeta_7+\zeta_7^2+\zeta_7^4\in\mathbb{Q}$, 那么 $\sigma_6(\zeta_7+\zeta_7^2+\zeta_7^4)=\zeta_7+\zeta_7^2+\zeta_7^4$, 即 ζ_7 适合一个 6 次多项式 $x^6+x^5-x^4+x^3-x^2-x$, 同时 ζ_7 适合不可约多项式 $\Phi_7(x)=x^6+\cdots+x+1$, 显然 $\Phi_7(x)$ 不整除这个 6 次多项式, 产生矛盾. 这就表明 $K=\mathbb{Q}(\zeta_7+\zeta_7^2+\zeta_7^4)$.

因此, $\mathbb{Q}(\zeta_7)/\mathbb{Q}$ 的所有中间域为

$$\mathbb{Q}(\zeta_7),\ \mathbb{Q}(\cos(2\pi/7)),\ \mathbb{Q}(\zeta_7+\zeta_7^2+\zeta_7^4),\ \mathbb{Q}.$$

例 2.21. 考虑 $\mathbb{Q}(\zeta_8)/\mathbb{Q}$. 此时 $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) = \{\sigma_1, \sigma_3, \sigma_5, \sigma_7\}$, 其中除开 σ_1 都是 2 阶元. 那么它的所有子群为

$$0,\ \langle\sigma_3\rangle,\ \langle\sigma_5\rangle,\ \langle\sigma_7\rangle,\ \mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}).$$

中间三个子群对应的中间域在 $\mathbb{Q}$ 上都是 2 次的. 令 $\zeta_8 = e^{\pi i/4} = (1+i)/\sqrt{2}$, 注意到 $\sigma_5(\zeta_8^2) = \zeta_8^2 = i$, 所以 $\mathrm{Fix}(\sigma_5) \supseteq \mathbb{Q}(\zeta_8^2) = \mathbb{Q}(i)$. 又因为 $[\mathrm{Fix}(\sigma_5) : \mathbb{Q}] = 2$ 且 $\mathbb{Q}(i) \neq \mathbb{Q}$, 所以 $\mathrm{Fix}(\sigma_5) = \mathbb{Q}(i)$.

剩下两个中间域的计算和上例相同. 记 $L = \mathrm{Fix}(\sigma_3)$, 那么 $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/L) = \{\sigma_1, \sigma_3\}$, 所以 $\min(L, \zeta_8) = (x-\zeta_8)(x-\zeta_8^3) \in L[x]$, 所以 $\zeta_8 + \zeta_8^3 \in L$, 故 $\mathbb{Q}(\zeta_8+\zeta_8^3) \subseteq L$. 同时 $\zeta_8 + \zeta_8^3 = \sqrt{2}i \notin \mathbb{Q}$, 所以 $\mathrm{Fix}(\sigma_3) = \mathbb{Q}(\zeta_8 + \zeta_8^3) = \mathbb{Q}(\sqrt{-2})$. 同理不难得到 $\mathrm{Fix}(\sigma_7) = \mathbb{Q}(\zeta_8 + \zeta_8^7) = \mathbb{Q}(\sqrt{2})$.

于是 $\mathbb{Q}(\zeta_8)/\mathbb{Q}$ 的所有中间域为

$$\mathbb{Q}(\zeta_8),\ \mathbb{Q}(\sqrt{-2}),\ \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}.$$

2.3 范数与迹

注意到在 例 2.20 和 例 2.21 中, 我们使用形如 $\sum_{\sigma\in H}\sigma(\zeta_n)$ 的元素来生成分圆扩张的中间域 $\mathrm{Fix}(H)$. 我们将看到这个和 $\sum_{\sigma\in H}\sigma(\zeta_n)$ 就是 ζ_n 在扩张 $\mathbb{Q}(\zeta_n)/\mathrm{Fix}(H)$ 下的迹.

令 K 是 F 的扩域且 $[K:F] = n$. 如果 $a \in K$, 记 L_a 为映射 $L_a : K \to K$, 满足 $L_a(b) = ab$. 容易验证 L_a 是 F-线性映射. L_a 作为有限维向量空间之间的线性映射, 其可以表示为一个矩阵, 从而可以计算矩阵的行列式和迹.

定义 2.22. 令 K 是 F 的扩域, 对于 $a \in K$, 定义 a 的范数 $N_{K/F}$ 和 $T_{K/F}$ 分别为

$$\mathrm{N}_{K/F}(a) = \det(L_a),\ \mathrm{Tr}_{K/F}(a) = \mathrm{Tr}(L_a).$$

根据这个定义, 显然 $\mathrm{N}_{K/F}(a), \mathrm{Tr}_{K/F}(a) \in F$.

例 2.23. 设 F 是域, 对于 $d \in F \setminus F^2$, 令 $K = F(\sqrt{d})$, 那么 K 的一组基为 $\{1, \sqrt{d}\}$. 如果 $\alpha = a + b\sqrt{d}$, 其中 $a, b \in F$, 我们来计算 α 的范数和迹. 由于 $L_\alpha(1) = \alpha = a + b\sqrt{d}$, 以及 $L_\alpha(\sqrt{d}) = \alpha\sqrt{d} = bd + a\sqrt{d}$, 所以 L_α 的表示矩阵为

$$\begin{pmatrix} a & bd \\ b & a \end{pmatrix},$$

所以 $\mathrm{N}_{K/F}(\alpha) = a^2 - b^2 d$ 以及 $\mathrm{Tr}_{K/F}(\alpha) = 2a$.

例 2.24. 对于域扩张 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, 计算 $\sqrt[3]{2}$ 的范数与迹. 由于 $\mathbb{Q}(\sqrt[3]{2})$ 有基 $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$, 所以 $L_{\sqrt[3]{2}}$ 的表示矩阵为

$$\begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

所以 $\mathrm{N}_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(\sqrt[3]{2}) = 2$ 以及 $\mathrm{Tr}_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(\sqrt[3]{2}) = 0$.

例 2.25. 令 F 是特征 $p > 0$ 的域, K/F 是次数为 p 的纯不可分扩张.