抽象代数II 读书报告

汪铃　2001110014

2021 年 1 月 2 日

第一章　伽罗瓦理论

§1.1　单扩张

有理数域 $\mathbb{Q}$ 和剩余类域 $\mathbb{Z}_p$ 是我们熟知的两类域。我们还知道，$\mathbb{Q}$ 是实数域 $\mathbb{R}$ 和复数域 $\mathbb{C}$ 的子域。事实上，**任何一个域都包含同构于 $\mathbb{Q}$ 或 $\mathbb{Z}_p$ 的子域**。

定理1.1.1. 设 E 是一个域。如果 $chE = 0$，那么 E 包含一个子域 F，使得 $F \simeq \mathbb{Q}$；如果 $chE = p > 0$，那么 E 包含一个子域 F，使得 $F \simeq \mathbb{Z}_p$。

证明. 因为 E 有单位元1，任取 $n \in \mathbb{Z}$, $n1 \in E$. 记

$$S = \{n1 | n \in \mathbb{Z}\},$$

那么 S 是 E 的一个子环。建立一个映射

$$\varphi : \mathbb{Z} \longrightarrow S, \quad n \longmapsto n1,$$

则知 φ 是一个环的满同态，接下来按域的特征进行讨论即可。 □

如果一个域 F 不含真子域，那么就称 F 为**素域**。则我们知道定理1.1.1保证了**任意一个域都包含素域作为它的子域**。

如果 E 是一个域，F 是 E 的子域，那么就称 E 为域 F 的**扩域**或**扩张**，记作 E/F。根据定理1.1.1，我们知道只需要把素域的所有扩张研究清楚了，那么域的扩张也就明了了，但是呢素域的扩张并不一定比一般域的扩张简单，所以在之后的研究中我们还是研究一般域的扩张。下面我们从最简单的扩张——单扩张做起。

设 F 是 E 的一个子域，$\alpha \in E$，令

$$F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} | f(\alpha), g(\alpha) \in F[\alpha], g(\alpha) \neq 0 \right\}. \tag{1.1}$$

那么 $F(\alpha)$ 就是 E 包含 F 和 α 的最小子域，称为 F 添加元素 α 得到的**单扩张**。

设 E 是域 F 的扩张，$\alpha \in E$。如果存在 F 上的非零多项式 $f(x)$，使得 $f(\alpha) = 0$, 那么 α 叫做 F 上的**代数元**，$F(\alpha)$ 叫做 F 的一个单代数扩张。反之，如果对于 F 上任意一个非零多项式 $g(x)$，都有 $g(\alpha) \neq 0$，那么就称 α 为域 F 上的一个**超越元**，这时 $F(\alpha)$ 叫做 F 的一个单超越扩张。

例1.1.2. $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ 都是单代数扩张；$\mathbb{Q}(e)$, $\mathbb{Q}(\pi)$ 都是单超越扩张。

定理1.1.3. 设 E 是域 F 的扩张， $\alpha \in E$ 。

(i) 如果 α 是 F 上的一个超越元，那么

$$F(\alpha) \simeq F(x)\,.$$

(ii) 如果 α 是 F 上的一个代数元，那么

$$F(\alpha) = F[\alpha] \simeq F[x]/\langle p(x)\rangle\,,$$

其中 $p(x)$ 是 F 上的首1不可约多项式，并且 $p(\alpha) = 0$.

证明. 根据多项式环的泛性，知恒等映射 $id : F \longrightarrow F$ 有唯一的开拓

$$\varphi : F[x] \longrightarrow F[\alpha]\,, \quad f(x) \longmapsto f(\alpha)\,.$$

易知 φ 是一个满同态。

(i) 如果 α 是一个超越元，则知 $Ker(\varphi) = \{0\}$, φ 是环同构。因为(1.1)式定义的 $F(\alpha)$ 是 $F[x]$ 在 E 中的商域，故知 φ 可以开拓为商域的同构，则得 $F(\alpha) \simeq F(x)$.

(ii) 如果 α 是一个代数元，则有环同态基本定理知， $F[\alpha] \simeq F[x]/Ker(\varphi)$. 因为 $F[x]$ 是主理想整环，所以 $Ker(\varphi) = \langle p(x)\rangle$. 由于 $Ker(\varphi)$ 的生成元只相差一个非零常数因子，所以我们可以取 $p(x)$ 为首1多项式，于是 $p(x)$ 唯一确定。易知 $p(x)$ 不可约，故 $\langle p(x)\rangle$ 是极大理想，所以 $F[x]/\langle p(x)\rangle$ 是一个域，因而与之同构的 $F[\alpha]$ 也是一个域,再由 $F(\alpha)$ 的定义知 $F(\alpha) = F[\alpha]$. □

单代数扩张的结构比较简单，下面研究单代数扩张的结构。设 E 是域 F 的扩张， $\alpha \in E$ 是 F 上的一个代数元。那么 $F[x]$ 中使得 $f(\alpha) = 0$ 的次数最小的首1多项式

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

叫做 α 在 F 上的**极小多项式**。

引理1.1.4. 设 E 是域 F 的扩张， $\alpha \in E$ 是 F 上的一个代数元。如果 $p(x)$ 是 α 在 F 上的极小多项式， $f(x) \in F[x]$ 是 α 的零化多项式，那么有 $p(x)|f(x)$.

证明. 反证，并利用带余除法即可得到结论。 □

推论1.1.5. 设 E 是域 F 的扩张， $\alpha \in E$ 是 F 上的代数元,并设 $p(x)$ 是 α 在 F 上的极小多项式。如果 $degp(x) = n$ ，那么 $F(\alpha)$ 是域 F 上以 $\{1, \alpha, \cdots, \alpha^{n-1}\}$ 为基的一个n维向量空间。

证明. 利用带余除法并注意到 $p(x)$ 的极小性即可得到结论。 □

下面我们将说明单代数扩张总是存在的。

定理1.1.6. *对于域 F 上任意给定的不可约多项式*

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0\,,$$

存在 F 的单代数扩张 $F(\alpha)$，使得 α 在 F 上的极小多项式是 $p(x)$。

证明. 做剩余类域 $K = F[x]/\langle p(x)\rangle$. 记 $\overline{f}(x) = f(x) + \langle p(x)\rangle\,, \overline{F} = \{\overline{a}|a \in F\}$. 那么 $\varphi : \overline{F} \longrightarrow F\,, \overline{a} \longmapsto a$ 是域同构。令 $E = F \cup (K \setminus \overline{F})$. 因为 $(K \setminus \overline{F}) \cap F = \emptyset$, 根据挖补定理， φ 可以开拓为同构映射 $\widetilde{\varphi} : K \longrightarrow E$， 使得 $\widetilde{\varphi}(\overline{x}) = \overline{x}$. 因为 $\overline{x}^n + \overline{a}_{n-1}\overline{x}^{n-1} + \cdots + \overline{a}_0 = \overline{0}\,, p(\overline{x}) = \widetilde{\varphi}(\overline{x}^n + \overline{a}_{n-1}\overline{x}^{n-1} + \cdots + \overline{a}_0 = \overline{0}) = 0\,$, 所以 $p(x)$ 是 $\overline{x}$ 在 F 上的极小多项式。记 $\alpha = \overline{x}$, 那么 $E = F(\alpha)$ 是 F 的一个单代数扩张。 □

注1.1.7. *如果域 $E = F(\alpha)\,, \alpha$ 的取法不是唯一的。比如复数域 $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}(i+1)$.*

§1.2 有限扩张

设 E 是域 F 的扩张，那么 E 可以看作是 F 上的一个向量空间，数乘由域的乘法给出：

$$F \times E \longrightarrow E\,, \quad (a, x) \longmapsto ax\,.$$

E 在 F 上的维数 $dim_F E$ 叫做 E 关于 F 的**扩张次数**，记作 $[E : F]$. 如果 $[E : F] < \infty$，那么就称 E 是域 F 的**有限扩张**。如果 $[E : F] = \infty$，称 E 是域 F 的**无限扩张**。

引理1.2.1. *设域的扩张链 $F \subseteq L \subseteq E$. 如果 $L/F\,, E/L$ 都是有限扩张，那么 E/F 也是有限扩张，并且*

$$[E : F] = [E : L][L : F]\,.$$

证明. 设 $[L : F] = n\,, \alpha_1, \alpha_2, \cdots, \alpha_n$ 是向量空间 L 的 F-基；$[E : L] = m\,, \beta_1, \beta_2, \cdots, \beta_m$ 是向量空间 E 的 L-基。而容易证明向量组

$$\alpha_i\beta_j\,, \quad 1 \leqslant i \leqslant n\,, 1 \leqslant j \leqslant m\,,$$

是 E 的 F-基，所以便知结论成立。 □

推论1.2.2. 给定域扩张链 $F \subseteq F_1 \subseteq \cdots \subseteq F_{s-1} \subseteq F_s$. 如果每个域都是前一个域的有限扩张, 那么

$$[F_s : F] = [F_s : F_{s-1}] \cdots [F_1 : F] .$$

设 E 是域 F 的扩张,如果 E 的每个元都是 F 上的代数元，则称 E 是 F 的**代数扩张**。如果存在一个元是 F 上的超越元，那么称 E 是 F 的**超越扩张**。

定理1.2.3. 有限扩张都是代数扩张。

证明. 设 E 是域 F 的有限扩张， $[E : F] = n$. 任取 $c \in E, E$ 中的n+1个元素 $1, c, c^2, \cdots, c^n$ 是线性相关的，即存在不全为零的元素 $a_0, a_1, \cdots, a_n \in F$, 使得

$$a_0 + a_1 c + a_2 c^2 + \cdots + a_n c^n = 0 .$$

于是存在 F 上的非零多项式

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n ,$$

使得 $f(c) = 0$, 所以 c 是 F 上的代数元。 □

推论1.2.4. 设域的扩张链 $F \subseteq L \subseteq E$. 那么 E/F 是代数扩张当且仅当 $E/L, L/F$ 都是代数扩张。

证明. 必要性. 任取 $\alpha \in E$, 因为 α 是 F 上的代数元，所以存在 α 的零化多项式 $f(x) \in F[x] \subseteq L[x]$, 故知 α 是 L 上的代数元，所以 E/L 是代数扩张。显然 L/F 也是代数扩张。

充分性. 任取 $\alpha \in E$, 那么 α 是 L 上的代数元。设

$$p(x) = x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 ,$$

是 α 在 L 上的极小多项式，其中 $a_0, a_1, \cdots, a_{n-1} \in L$. 令 $L_0 = F(a_0, a_1, \cdots, a_{n-1})$, 因为 $a_0, a_1, \cdots, a_{n-1} \in L$ 都是 F 上的代数元，所以知 L_0/F, $L_0(\alpha)/L_0$ 都是有限扩张。则由引理1.2.1知

$$[L_0(\alpha) : F] = [L_0(\alpha) : L_0][L_0 : F] < \infty .$$

于是 $L_0(\alpha)$ 也是 F 的有限扩张，因而是代数扩张， α 是 F 上的代数元。所以 E/F 是代数扩张。 □

例1.2.5. $E=\mathbb{Q}(\sqrt{2},\sqrt{3})$ 是 $\mathbb{Q}$ 的一个有限扩张。$\sqrt{2}$ 在 $\mathbb{Q}$ 上的极小多项式为 x^2-2, 于是 $[Q(\sqrt{2}):\mathbb{Q}]=2$. 类似地, $\sqrt{3}$ 在 $\mathbb{Q}$ 上的极小多项式为 x^2-3. 因为 $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$, 所以 x^2-3 也是 $\sqrt{3}$ 在 $\mathbb{Q}(\sqrt{2})$ 上的极小多项式。最后

$$[E:\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2\times 2=4\,.$$

根据引理*1.2.1*的证明, $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ 是 E 的一组 $\mathbb{Q}$ -基。

§1.3 多项式的分裂域

根据代数基本定理，复数域上的任意一个次数大于零的多项式都可以分解为一次因式的乘积。在本节我们将证明，对于域 F 上的任意一个多项式 $f(x)$, 可以找到 F 上的一个扩张 E，使得 $f(x)$ 在 $E[x]$ 中能分解为一次因式的乘积。

定义1.3.1. 设 F 是一个域, $f(x)\in F[x]\,,\,deg(f(x))=n\geqslant 1$. F 的一个扩张 E 叫做 $f(x)$ 在 F 上的**分裂域**，如果

(i) $f(x)$ 在 $E[x]$ 中能分解为一次因式的乘积:

$$f(x)=a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)\,,$$

其中 $a\in F\,,\,\alpha_i\in E$;

(ii) $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)\,.$

定理1.3.2. 设 F 是一个域, $f(x)\in F[x]\,,\,deg(f(x))\geqslant 1$. 那么存在 $f(x)$ 在 F 上的分裂域。

证明. 对 $f(x)$ 的次数做数学归纳法。当 $deg(f(x))=1$ 时, F 是 $f(x)$ 在 F 上的分裂域。设 $deg(f(x))=n>1$ 且命题对次数为 $n-1$ 的多项式成立。假定在 $F[x]$ 中，

$$f(x)=p(x)g(x)\,,$$

其中 $p(x)$ 是 F 上的一个首1不可约多项式。根据定理1.1.6，存在一个域 $F(\alpha_1)$，使得 α_1 在 F 上的极小多项式是 $p(x)$。于是 $f(\alpha_1)=p(\alpha_1)g(\alpha_1)=0$, 因而 $f(x)$ 在 $F(\alpha_1)$ 上可以分解为

$$f(x)=(x-\alpha_1)f_1(x)\,.$$

根据归纳假设，设 $f_1(x)$ 在 $F(\alpha_1)$ 上的分裂域为 E。那么 $f_1(x)$ 可以在 $E[x]$ 中分解为一次因式的乘积，即 $f_1(x)=a(x-\alpha_2)\cdots(x-\alpha_n)$. 于是，$f(x)$ 在 $E[x]$ 中可分解为

$$f(x)=a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)\,.$$

因为

$$E = F(\alpha_1)(\alpha_2, \cdots, \alpha_n) = F(\alpha_1, \alpha_2, \cdots, \alpha_n),$$

E 是 $f(x)$ 在 F 上的分裂域。

□

推论1.3.3. 设 F 是一个域，$f(x) \in F[x]$, $deg(f(x)) = n \geqslant 1$. 如果 E 是 $f(x)$ 在 F 上的一个分裂域，那么 $[E : F] \leqslant n!$.

证明. 注意到

$$[F(\alpha_1) : F] \leqslant n, [F(\alpha_1, \alpha_2) : F(\alpha_1)] \leqslant n-1, \cdots, [E : F(\alpha_1, \cdots, \alpha_{n-1})] \leqslant 1.$$

□

下面举例说明如何求一个多项式的分裂域。

例1.3.4. 求多项式 $f(x) = (x^2 - 2)(x^2 - 3)$ 在有理数域 $\mathbb{Q}$ 上的一个分裂域。

解. 因为 $f(x)$ 在 $\mathbb{C}[x]$ 中分解为

$$f(x) = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3}),$$

所以便知 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 是 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域。 □

例1.3.5. 求多项式 $f(x) = x^3 - 2$ 在有理数域 $\mathbb{Q}$ 上的一个分裂域。

解. 因为 $f(x)$ 在 $\mathbb{C}[x]$ 中分解为

$$f(x) = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\zeta)(x - \sqrt[3]{2}\zeta^2),$$

其中 $\zeta = \frac{-1+\sqrt{3}\mathrm{i}}{2}$, 所以便知 $\mathbb{Q}(\sqrt[3]{2}, \zeta)$ 是 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域。 □

例1.3.6. 设 $f(x) = x^p - 1$, p 是一个素数。求 $f(x)$ 在理数域 $\mathbb{Q}$ 上的一个分裂域。

解. $f(x) = (x-1)p(x)$, 其中 $p(x) = x^{p-1} + x^{p-2} + \cdots + 1$ 是 $\mathbb{Q}$ 上的一个不可约多项式。记 ζ 是 $p(x)$ 的一个根，ζ 在 $\mathbb{C}$ 生成一个循环群 $\langle\zeta\rangle = \{1, \zeta, \cdots, \zeta^{p-1}\}$. 这 p 个元素恰好是 $x^p - 1$ 的全部根。所以 $\mathbb{Q}(\zeta) = \mathbb{Q}(1, \zeta, \cdots, \zeta^{p-1})$ 是 $x^p - 1$ 在 $\mathbb{Q}$ 上的分裂域，并且 $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$, $\{1, \zeta, \cdots, \zeta^{p-2}\}$ 是 $\mathbb{Q}(\zeta)$ 的 $\mathbb{Q}$ -基。

□

例1.3.7. 求 $f(x)=x^3+x+1$ 在 $\mathbb{Z}_2$ 上的一个分裂域。

解. 因为 $\mathbb{Z}_2$ 的两个元素0和1都不是 $f(x)$ 的根，所以 $f(x)$ 在 $\mathbb{Z}_2$ 上是不可约的。设 α 是 $f(x)$ 的一个根，那么 $f(\alpha^2)=\alpha^6+\alpha^2+1=(\alpha^3+\alpha+1)^2=0$，所以 α^2 也是 $f(x)$ 的一个根，并且 $\alpha^2\neq\alpha$. 令 $E=\mathbb{Z}_2(\alpha)$, 那么在 $E[x]$ 中，$(x-\alpha)(x-\alpha^2)|f(x)$，换言之 $f(x)=(x-\alpha)(x-\alpha^2)(x-\beta)$，其中 $\beta\in E$. 于是 E 是 $f(x)$ 在 $\mathbb{Z}_2$ 上的分裂域。

□

§1.4 有限域

有限域又叫做伽罗瓦域，因伽罗瓦首先提出而得名。只有有限多个元素的域叫做**有限域**。

注1.4.1. 因为特征*0*的域都是无限域，所以有限域的特征只能为素数。

引理1.4.2. 设 E 是一个有限域，$chE=p$，F 是 E 的素域。那么 E 有 p^n 个元素，其中 $n=[E:F]$.

证明. 因为 E 只有有限个元素，所以是 F 的有限扩张。设 $[E:F]=n$, $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 E 的一组 F-基。那么 E 的每个元素可以唯一的表示为

$$a_1\alpha_1+a_2\alpha_2+\cdots+a_n\alpha_n\,,$$

其中 $a_i\in F$. 而 F 只有 p 个元素，每一个 a_i 有 p 种选择，所以 E 共有 p^n 个元素。 □

下面我们不加证明的列出一些有限域的相关结论。

定理1.4.3. 设 p 是一个素数，$n\in\mathbb{Z}^+$, $q=p^n$.

(i) 多项式 x^q-x 在 $\mathbb{Z}_p$ 上的分裂域是 q 元域；

(ii) 任意两个 q 元域是同构的。

定理1.4.4. *(i)* 有限域非零元素的乘法群是循环群；

(ii) 有限域 E 是素域 F 的单扩张；

(iii) 任意有限域的有限扩张都是单扩张。

命题1.4.5. 设 E 是一个 $q=p^n$ 元域，p 是一个素数。令

$$f: E \longrightarrow E, \quad \alpha \longmapsto \alpha^p .$$

那么 f 是 E 的一个自同构，称为 E 的**弗罗贝纽斯映射**。

注1.4.6. 由命题*1.4.5*知，p^n 元域的每个元素都可以开 p 次方，并且 p 次方根是唯一的。这与在复数域中熟知的，一个非零复数有 p 个两两不同的 p 次方根不一样。

§1.5 分圆域

我们在本节中讨论 x^n-1 在有理数域 $\mathbb{Q}$ 上的分裂域。

多项式 x^n-1 的任意根 ζ 叫做一个 n 次单位根。如果任取 $0<m<n$, $\zeta^m \neq 1$, 那么 ζ 就称为一个 n 次**本原单位根**。

设 ζ 是一个 n 次本原单位根，令

$$W_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\},$$

那么 W_n 关于数的乘法构成一个 n 阶循环群 $\langle\zeta\rangle$, 它是全体 n 次单位根的集合。

引理1.5.1. 设 ζ 是一个 n 次本原单位根，$0<k<n$。那么 ζ^k 也是一个 n 次本原单位根当且仅当 $(n,k)=1$. 因而存在 $\varphi(n)$ 个 n 次本原单位根，其中 $\varphi(n)$ 是欧拉函数。

证明. 注意到

$$o(\zeta^k) = \frac{n}{(k,n)} .$$

所以 ζ^k 是 W_n 中 n 阶元当且仅当 $(n,k)=1$. □

设 ζ 是一个 n 次本原单位根，令 $\varphi(n)$ 次多项式

$$\Phi_n(x) = \prod_{1\leqslant k\leqslant n,(n,k)=1} (x-\zeta^k) . \tag{1.2}$$

显然，$\Phi_1(x)=x-1$, $\Phi_2(x)=x+1$; 任取素数 p , $\Phi_p(x)=x^{p-1}+\cdots+x+1$. 他们都是 $\mathbb{Q}$ 上的不可约多项式。我们在本节的主要目标是对于任意的正整数 n ，证明 $\Phi_n(x)$ 是 $\mathbb{Q}$ 上的不可约多项式。

定理1.5.2. n 次本原单位根 ζ 在 $\mathbb{Q}$ 上的极小多项式为 $\Phi_n(x)$ 。从而 $\mathbb{Q}(\zeta)$ 是 $\Phi_n(x)$ 在 $\mathbb{Q}$ 上的分裂域，且 $[\mathbb{Q}(\zeta):\mathbb{Q}]=\varphi(n)$.

证明. 当 $n=1$ 时，结论显然成立。设 $n\geqslant 2$, ζ 在 $\mathbb{Q}$ 上的极小多项式为 $f(x)$. 那么 $f(x)|(x^n-1)$，但是当 $1\leqslant d<n$ 时， $f(x\nmid(x^d-1))$, 因为后者不是 ζ 的零化多项式。所以 $(f(x),(x^d-1))=1$， $f(x)$ 的根只能是 n 次本原单位根。

其次证明所有的 n 次本原单位根都是 $f(x)$ 的根。为此先证明一个事实：对于 $f(x)$ 的任意一个根 ζ 和一个素数 $p\nmid n$, ζ^p 也是 $f(x)$ 的根。

否则，假定 ζ^p 不是 $f(x)$ 的根。设 ζ^p 在 $\mathbb{Q}$ 上的极小多项式为 $g(x)$, 那么 $f(x)$ 与 $g(x)$ 互素。但是 $f(x),g(x)|(x^n-1)$, 所以 $f(x)g(x)|(x^n-1)$. 设 $x^n-1=f(x)g(x)h(x)$, 因为 $x^n-1\in\mathbb{Z}[x]$ 是一个本原多项式，根据高斯引理，容易证明 $f(x),g(x),h(x)\in[x]$，并且也是本原多项式。另一方面， ζ^p 是 $g(x)$ 的根，于是 ζ 是 $g(x^p)$ 的根，$f(x)|g(x^p)$. 设 $g(x^p)=f(x)l(x)$. 环同态 $\vartheta:\mathbb{Z}\to\mathbb{Z}_p$, $a\mapsto[a]$ 可以唯一拓展为环同态 $\overline{\vartheta}:\mathbb{Z}[x]\to\mathbb{Z}_p[x]$, $f(x)\mapsto\overline{f}(x)$, 其中 $\overline{\vartheta}(x)=x$. 我们得到

$$x^n-[1]=\overline{f}(x)\overline{g}(x)\overline{h}(x),\quad \overline{g}(x^p)=\overline{f}(x)\overline{l}(x).$$

因为 $[a]^p=[a]$, $\forall[a]\in\mathbb{Z}_p$, 于是 $(\overline{g}(x))^p=\overline{g}(x^p)=\overline{f}(x)\overline{l}(x)$, $(\overline{f}(x),\overline{g}(x))\neq 1$, $x^n-[1]$ 在 $\mathbb{Z}_p[x]$ 中有重根。但是在 $\mathbb{Z}_p[x]$ 中， $(x^n-[1])'$ 与 $x^n-[1]$ 互素， $x^n-[1]$ 没有重根，得到矛盾。

最后，设 $1<k<n$, $(n,k)=1$, $k=p_1p_2\cdots p_s$ 是 k 的素因子分解。那么每个 $p_i\nmid n$. 根据前面的事实， $f(\zeta^{p_1})=0$, $f(\zeta^{p_1p_2})=f((\zeta^{p_1})^{p_2})=0$; 如此继续下去，得到 $f(\zeta^k)=0$, 即任意一个 n 次本原单位根 ζ^k 都是 $f(x)$ 的根。所以 $\Phi_n(x)=f(x)$.

□

定义1.5.3. 有理数域 $\mathbb{Q}$ 上的不可约多项式 $\Phi_n(x)$ 叫做**分圆多项式**， $\Phi_n(x)$ 在 $\mathbb{Q}$ 上的分裂域叫做 n 次**分圆域**。

显然， n 次分圆域也是多项式 x^n-1 在 $\mathbb{Q}$ 上的分裂域。

对于 n 的每个正因子 d, $\Phi_d(x)$ 的根集由所有 d 次本原单位根构成，从而 $\Phi_d(x)|(x^n-1)$. 并且当 d_1, d_2 是 n 的不同正因子时， $\Phi_{d_1}(x)$ 与 $\Phi_{d_2}(x)$ 互素。反之， x^n-1 的每个根必是某个 $\Phi_d(x)$ 的根。因此我们有公式

$$x^n-1=\prod_{d|n}\Phi_d(x). \tag{1.3}$$

比较(1.3)式两端多项式的次数，得到

$$n=\sum_{d|n}\varphi(d). \tag{1.4}$$

例1.5.4. 设 p 是素数，因为 p 次单位根构成的群 W_p 是一个 p 阶循环群，除单位元外，每个元素都是 p 阶元，所以

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

于是 $x^p - 1 = \Phi_1(x)\Phi_p(x)$.

例1.5.5. 因为 $\Phi_2(x) = x + 1$, $\Phi_4(x) = x^2 + 1$, 所以

$$x^4 - 1 = (x - 1)(x + 1)(x^2 + 1) = \Phi_1(x)\Phi_2(x)\Phi_4(x)\,.$$

根据公式(1.3)， $x^n - 1$ 可以写成分圆多项式的乘积。反之，分圆多项式 $\Phi_n(x)$ 也可以用 $(x^d - 1)$, $d|n$, 表示出来。为此我们先定义 $\mathbb{Z}^+$ 上的**莫比乌斯函数**:

$$\mu(n) = \begin{cases} 1, & n = 1\,, \\ (-1)^r, & n = p_1p_2\cdots p_r\,,\ p_1, p_2, \cdots, p_r\text{是两两不同的素数}, \\ 0, & \text{存在素数}p\,,\ p^2|n\,. \end{cases}$$

莫比乌斯函数有下述性质：

$$\sum_{d|n}\mu(d) = \begin{cases} 1, & n = 1\,, \\ 0, & n > 1\,. \end{cases}$$

事实上，当 $n = 1$ 时，结论显然。设 $n > 1$，且 $n = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$, 其中 $p_1, p_2, \cdots, p_r$ 是两两不同的素数，$e_i \geqslant 1$. 根据 $\mu(n)$ 的定义，$\sum_{d|n}\mu(d) = \sum_{d|n'}\mu(d)$, $n' = p_1p_2\cdots p_r$. 所以

$$\sum_{d|n'}\mu(d) = 1 + \sum_{1\leqslant k_1<\cdots<k_s\leqslant r}\mu(p_{k_1}\cdots p_{k_s}) = \prod_{i=1}^{r}(1 + \mu(p_i)) = 0\,.$$

命题1.5.6.

$$\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(\frac{n}{d})}\,.$$

例1.5.7. $\Phi_{12}(x) = (x^{12}-1)(x^6-1)^{-1}(x^4-1)(x^2-1) = (x^6+1)(x^2+1)^{-1} = x^4-x^2+1$.

例1.5.8. 设 p 是一个素数，则

$$\Phi_{p^r}(x) = (x^{p^r} - 1)(x^{p^{r-1}} - 1)^{-1} = x^{(p-1)p^{r-1}} + x^{(p-2)p^{r-1}} + \cdots + x^{p^{r-1}} + 1\,.$$

§1.6 可分扩张

域的可分扩张的概念依赖于该域上的多项式在其分裂域中是否有重根。

命题1.6.1. 设 F 是一个域，$p(x)$ 是 F 上的首1不可约多项式，E 是 $p(x)$ 在 F 上的分裂域。那么 $p(x)$ 在 E 有重根当且仅当 $p'(x)=0$.

特别地，当 $chF=0$ 时，$p(x)$ 在 E 中只有单根。

证明. 设 $p(x)$ 在 E 中有一个 $k-$根 α, 那么 $p(x)=(x-\alpha)^k g(x)$, 其中 $k\geqslant 1$, $(x-\alpha)\nmid g(x)$. 这时 $p'(x)=k(x-\alpha)^{k-1}g(x)+(x-\alpha)^k g'(x)$.

如果 $p(x)$ 在 E 有重根，记作 α, 那么 $p'(\alpha)=0$. 因为 $p(x)$ 是 α 在 F 的极小多项式，所以得 $p(x)|p'(x)$, 比较次数得到 $p'(x)=0$.

如果 $p(x)$ 在 E 没有重根，那么任取 $p(x)$ 的根 α，都有 $p'(x)=g(x)+(x-\alpha)g'(x)$, 所以 $(x-\alpha)\nmid p'(x)$. 于是 $p(x)$ 与 $p'(x)$ 在 $E[x]$ 中互素，因而在 $F[x]$ 中也互素，所以 $p'(x)\neq 0$.

当 $chF=0$ 时，$p'(x)\neq 0$, 所以后一结论也成立。 □

域 F 上一个不可约多项式 $p(x)$ 叫做**可分多项式**，如果 $p(x)$ 在它的分裂域中只有单根。多项式 $f(x)\in F[x]$ 叫做**可分多项式**，如果它在 $F[x]$ 中的每个不可约因子都是可分的。否则 $p(x)$ 或 $f(x)$ 就叫做**不可分多项式**。于是，由上述命题知，当 $chF=0$ 时，F 上的多项式都是可分的。

设 E 是域 F 的任意一个代数扩张，元素 $\alpha\in E$ 叫做 F 上的一个**可分元**，如果 α 的极小多项式是一个可分多项式，否则 α 叫做 F 上的一个**不可分元**。代数扩张 E 叫做 F 的**可分扩张**，如果 E 中的每个元素都是 F 上的可分元。否则 E 叫做 F 的**不可分扩张**。

注1.6.2. 当 $chF=0$ 时，F 的任意代数扩张 E 的元素都是可分元，所以 E 是 F 的可分扩张。

现在，我们来讨论特征p的域上的不可约多项式的结构。

定理1.6.3. 设域 F 的特征 $chF=p$, $p(x)$ 是 F 上不可分的不可约多项式，E 是 $p(x)$ 在 F 上的分裂域。那么 $p(x)$ 在 $E[x]$ 中可分解为一次因式的乘积：

$$p(x)=c(x-\alpha_1)^{p^e}(x-\alpha_2)^{p^e}\cdots(x-\alpha_r)^{p^e}, \tag{1.5}$$

其中 $\alpha_1,\alpha_2\cdots,\alpha_r$ 两两不等，e 是一个正整数。令

$$h(x)=c(x-\alpha_1^{p^e})(x-\alpha_2^{p^e})\cdots(x-\alpha_r^{p^e}). \tag{1.6}$$

则 $h(x)$ 是 F 上可分的不可约多项式，并且 $p(x)=h(x^{p^e})$.

证明. 设 n 次多项式

$$p(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\,,$$

因为 $p(x)$ 是不可分的，根据命题1.6.1知 $p'(x)=0$, 于是 $ia_i=0\,,1\leqslant i\leqslant n$. 当 $p\nmid i$ 时，必有 $a_i=0$, 所以

$$p(x)=a_{pm}x^{pm}+a_{p(m-1)}x^{p(m-1)}+\cdots+a_px^p+a_0\,.$$

令 $h_1(x)=\sum\limits_{j=1}^{m}a_{pj}x^j$, 那么 $p(x)=h_1(x^p)$, 并且 $h_1(x)$ 在 F 是不可约的，否则 $h_1(x)$ 在 F 是可约会导致 $p(x)$ 可约，矛盾。

如果 $h_1(x)$ 还是不可分的，重复上述的讨论，得到 $F[x]$ 中的不可约多项式 $h_2(x)$, 使得 $h_1(x)=h_2(x^p)$, 于是 $p(x)=h_1(x^p)=h_2(x^{p^2})$.

注意到 $deg(p(x))>deg(h_1(x))>deg(h_2(x))$, 因而在有限步后，可以得到 F 上可分的不可约多项式 $h(x)$, 使得 $p(x)=h(x^{p^e})$. 因为 $h(x)$ 是可分的，所以在分裂域 E 上有分解式

$$h(x)=c\prod_{i=1}^{r}(x-\beta_i)\,,\quad p(x)=c\prod_{i=1}^{r}(x^{p^e}-\beta_i)\,,$$

其中 $\beta_1,\beta_2,\cdots,\beta_r$ 两两不等。设 $\alpha_i\in E$ 是 $x^{p^e}-\beta_i$ 的一个根，即 $\beta_i=\alpha_i^{p^e}$, 我们就得到了定理要求的(1.5)和(1.6). □

注1.6.4. 上述定理中的 $h(x)$ 和非负整数 e 都是由不可约多项式 $p(x)$ 唯一确定。

(1.6)式给出的多项式 $h(x)$ 的次数称为 $p(x)$ 的**简约次数**， p^e 称为 $p(x)$ 的**纯不可分次数**。我们有公式

$$degp(x)=p^edegh(x)\,.$$

当 $degh(x)=1$ 时，多项式 $p(x)=c(x^{p^e}-\beta)$ 叫做**纯不可分的**。这时，不可约多项式 $p(x)$ 在它的分裂域 E 中只有唯一的根 α ，叫做 F 上的**纯不可分元**； $E=F(\alpha)$ 叫做 F 上的**纯不可分扩张**。

引理1.6.5. 设域 F 的特征 $chF=p$ 多项式 $f(x)=x^p-a\in F[x]$. 如果存在 $b\in F$, 使得 $a=b^p$, 那么 $f(x)$ 在 F 上可以分解为一次因式的乘积；否则 $f(x)$ 在 F 上是不可约的。

证明. 如果存在 $b \in F$，使得 $a = b^p$, 那么 $f(x) = x^p - a = x^p - b^p = (x-b)^p$.

否则，设 E 是 $f(x)$ 在 F 上的一个分裂域， $\alpha \in E$ 是 $f(x)$ 的一个根，那么 $f(\alpha) = \alpha^p - a = 0$, $a = \alpha^p$, $f(x) = (x-\alpha)^p \in E[x]$. 如果 $f(x)$ 是 F 上可约的，那么存在次数小于p的多项式 $g(x), h(x)$, 使得 $f(x) = g(x)h(x)$. 于是 $f(x) = g(x)h(x) \in E[x]$, 根据 $f(x)$ 在 $E[x]$ 中分解的唯一性， $g(x) = (x-\alpha)^r$, $h(x) = (x-\alpha)^{p-r}$, $0 < r < p$. 于是 $g(x)$ 中 x^{r-1} 的系数 $-r\alpha \in F$. 因为 r 在 F 中可逆，得到 $\alpha \in F$. 这时 $a = \alpha^p$, 与 a 不能写成 F 中元素的p次方幂矛盾，所以 $f(x)$ 在 F 上是不可约的。 □

下面我们来定义一种具有良好可分性的域。设 F 是一个域，如果 $F[x]$ 中的每一个不可约多项式都是可分的，那么就称 F 是一个**完全域**。而注意到特征零的域一定是完全域，所以我们下面讨论特征 p 的域什么时候是完全域。为此，先考虑子集

$$F^p = \{a^p | a \in F\}.$$

易知， F^p 是 F 的一个子域。如果 $F^p = F$ ，那么都有 $F^{p^n} = F$.

定理1.6.6. *设域 F 的特征为 p, 那么 F 是完全域当且仅当 $F^p = F$.*

证明. 设 $F^p = F$. 如果 $f(x)$ 是 F 上的任意一个不可分的不可约多项式，那么知存在可分的不可约多项式 $h(x) \in F[x]$, 使得 $f(x) = h(x^{p^e})$, $e \geqslant 1$. 设

$$h(x) = b_r x^r + b_{r-1} x^{r-1} + \cdots + b_0.$$

因为 $F^p = F$，所以存在 $a_i \in F$, 使得 $a_i^{p^e} = b_i$, $i = 0, 1, \cdots, r$. 于是

$$f(x) = h(x^{p^e}) = \sum_{i=0}^{r} a_i^{p^e} (x^i)^{p^e} = \left(\sum_{i=1}^{r} a_i x^i \right)^{p^e},$$

与 $f(x)$ 的不可约性矛盾。所以 $F(x)$ 中任意一个不可约多项式都是可分的，从而 F 是完全域。

如果 $F^p \neq F$，那么存在 $a \in F$, $a \notin F^p$, 即 a 不能写成 F 中元素的 p 次方幂。于是便知 $f(x) = x^p - a$ 是 F 上的纯不可分不可约多项式，所以 F 不是完全域。 □

推论1.6.7. *有限域是完全域。*

证明. 由弗罗贝纽斯映射可得 $F^p = F$，所以知 F 是完全域。 □

我们知道单扩张是一种最简单的扩张。设 E 是 F 的有限扩张，如果存在 $\theta \in E$，使得 $E = F(\theta)$，那么就称 θ 是 E 关于 F 的一个**本原元**。

定理1.6.8. 设 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_r)$ 是无限域 F 的一个有限扩张, 如果 $\alpha_1,\alpha_2,\cdots,\alpha_r$ 都是 F 上的可分元, 那么存在存在 $\theta\in E$, 使得 $E=F(\theta)$。

推论1.6.9. 域上的任意有限可分扩张都是单扩张。

证明. 设 E 是 F 的有限可分扩张。若 F 是有限域, 则知任意有限扩张都是单扩张。若 F 是无限域, 则有 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_r)$, 其中 $\alpha_1,\alpha_2,\cdots,\alpha_r$ 是可分元, 于是由上述定理知 E 是单扩张。 □

§1.7 正规扩张和域的嵌入

设 E 是域 F 的代数扩张。如果 $F[x]$ 中的任意一个不可约多项式在 E 有一个根, 那么它在 $E[x]$ 中可以分解成一次因式的乘积, 就称 E 是域 F 的**正规扩张**。

设 E 和 $\overline{E}$ 是域 F 的两个扩张, 如果存在域的同构 $\psi:E\longrightarrow\overline{E}$ 使得 ψ 在 F 上的限制 $\psi|_F=id$ 是恒等映射, 就称 ψ 为 $F-$同构。特别地, 如果 $\overline{E}=E$, 那么就称 ψ是 $F-$自同构。

定理1.7.1. 设 E 是域 F 的一个有限扩张, 那么下面命题等价:

(i) E 是 F 的正规扩张;

(ii) E 是 $F[x]$ 某个多项式在 F 上的分裂域;

(iii) 对于域 E 的任意代数扩张 K 和任意的 $F-$自同构 $\sigma:K\longrightarrow K$, 都有 $\sigma(E)=E$;

(iv) 存在 F 的有限正规扩张 K, 使得 $F\subseteq E\subseteq K$, 并且任取 $F-$自同构 $\sigma:K\longrightarrow K$, 都有 $\sigma(E)=E$。

命题1.7.2. 设 $F\subseteq L\subseteq L$ 是一个域的扩链。

(i) 如果 E/F 是正规的, 那么 E/L 也是正规的;

(ii) 如果 E 是 $f(x)$ 在 F 上的分裂域, 那么 E 也是 $f(x)$ 在 L 上的分裂域;

(iii) 如果 E/F 是可分的, 那么 $E/L, L/F$ 都是可分的。

设 E 是域 F 的有限扩张。称 E 的代数扩张 $\overline{E}$ 为 E 在 F 上的一个**正规闭包**, 如果

(i) $\overline{E}$ 是 F 的正规扩张；

(ii) 设 K 是 F 的正规扩张，使得 $F \subseteq E \subseteq K \subseteq \overline{E}$, 那么 $K = \overline{E}$.

推论1.7.3. 设 E 是域 F 的有限扩张。那么 E 在 F 上的正规闭包 $\overline{E}$ 存在，$\overline{E}/F$ 是有限的，并且在同构意义下是唯一的。

例1.7.4. $\mathbb{Q}(\sqrt[3]{2}, \zeta)$ 是 $x^3 - 2$ 在 $\mathbb{Q}$ 上的分裂域，因而 $\mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q}$ 是正规的，它是 $\mathbb{Q}(\sqrt[3]{2})$ 在 $\mathbb{Q}$ 上的正规闭包。另一方面，$\mathbb{Q}(\zeta)$ 在 $\mathbb{Q}$ 上的正规闭包就是它自己。

设 E 和 E' 是两个域，如果 $\varphi : E \longrightarrow E'$ 是一个环同态，那么就称 φ 是域的同态。一个有趣的事实是，E 的理想 $Ker(\varphi)$ 只能是 $\{0\}$ 或者 E 本身。前者意味着 φ 是一个单同态，后者意味着 φ 是一个满同态。

设域 $E \subseteq L \subseteq E$ 是域的一个扩张链。如果 σ 是 L 到 E 的一个嵌入，并且保持 F 的每个元都不动，就称 σ 是 L 到 E 的一个 $F-$嵌入。L 到 E 的 $F-$嵌入个数记作 $\iota(L/F, E)$.

引理1.7.5. 设 E 是域 F 的一个正规扩张，$\alpha \in E$, α 在 F 上的极小多项式为 $p(x)$. 那么

$$\iota(F(\alpha)/F, E) \leqslant deg(p(x)),$$

等号成立当且仅当 $p(x)$ 是可分的。

引理1.7.6. 设 E 是域 F 的一个有限正规扩张。如果有域的扩张链 $F \subseteq L \subseteq N \subseteq E$, 那么 $\iota(N/L, E)\iota(L/F, E) = \iota(N/F, E)$.

定理1.7.7. 设 $E = F(\alpha_1, \alpha_2, \cdots, \alpha_s)$ 是域 F 的一个有限扩张，$\overline{E}$ 是 E 在 F 上的正规闭包。那么 $\iota(E/F, \overline{E}) \leqslant [E : F]$. 特别地，下述三个条件等价：

(i) $\alpha_1, \alpha_2, \cdots, \alpha_s$ 是 F 上的可分元；

(ii) $\iota(E/F, \overline{E}) = [E : F]$;

(iii) E/F 是可分的。

推论1.7.8. 设 E 是域 F 的一个扩张，$L = \{\alpha \in E | \alpha在F上可分\}$. 那么 L 是 E/F 的一个中间域。

上述推论给出的子域 L 叫做 F 在 E 中的**可分闭包**。

§1.8 伽罗瓦扩张

设 E 是一个域，那么 E 的全体自同构的集合关于变换的合成构成一个群，称为 E 的**自同构群**，记作 $Aut(E)$.

如果 E 是域 F 的一个扩张， E 的 $F-$自同构的集合

$$Gal(E/F) = \{\sigma \in Aut(E) | \sigma|_F = id\}$$

构成 $Aut(E)$ 的一个子群，就称为 E 在 F 上的**伽罗瓦群**。

设 G 是域 E 的自同构群 $Aut(E)$ 的任意一个子群，元素 $\alpha \in E$. 如果任取 $\sigma \in G$, 都有 $\sigma(\alpha) = \alpha$，就称 α 为 G 的一个**不动元**。群 G 的不动元的集合

$$Inv(G) = \{\alpha \in E | \sigma(\alpha) = \alpha, \forall\, \sigma \in G\}$$

构成 E 的一个子域，叫做 G 的**不动域**。

现在设 E 是一个域，我们将 E 的子域的集合记作：

$$\Gamma = \{域 L | L \subseteq E\};$$

将 $Aut(E)$ 子群的集合记作：

$$\Omega = \{H | H \leqslant Aut(E)\}.$$

那么可以得到下述两个映射：

$$Gal : \Gamma \longrightarrow \Omega, \quad L \longmapsto Gal(E/L);$$

$$Inv : \Omega \longrightarrow \Gamma, \quad H \longmapsto Inv(H).$$

命题1.8.1. 设 L_1, L_2, L 分别是 E 的子域， $H_1.H_2, H$ 分别是 $Aut(E)$ 的子群。那么

$$\begin{cases} L_1 \subseteq L_2 \Longrightarrow Gal(E/L_1) \supseteq Gal(E/L_2), \\ H_1 \subseteq H_2 Inv(H_1) \Longrightarrow \supseteq Inv(H_2). \end{cases}$$

$$\begin{cases} L \subseteq Inv(Gal(E/L)), \\ H \subseteq Gal(E/Inv(H)). \end{cases}$$

$$\begin{cases} Gal(E/Inv(Gal(E/L))) = Gal(E/L), \\ Inv(Gal(E/Inv(H))) = Inv(H). \end{cases}$$

证明. 直接验证即可，在此不再赘述。 □

设 E 是域 F 的有限扩张，如果 $Inv(Gal(E/F)) = F$，那么称 E 为 F 的一个有限**伽罗瓦扩张**。

定理1.8.2. *设 E 是域 F 的一个有限扩张，那么下述条件等价。*

(i) E/F *是伽罗瓦扩张；*

(ii) E/F *是正规可分扩张；*

(iii) E *是* F *上某个可分多项式的分裂域；*

(iv) $|Gal(E/F)| = [E : F]$.

证明. (i) $\Longrightarrow$ (ii) 设 E/F 是伽罗瓦扩张。任取 $\alpha \in E$，设 $p(x)$ 是 α 在 F 上的极小多项式。任取 $\sigma \in Gal(E/F)\,, p(\sigma(\alpha)) = \sigma(p(\alpha)) = 0\,,$ 因而 $\sigma(\alpha)$ 也是 $p(x)$ 的根。在 $\{\sigma(\alpha)|\sigma \in Gal(E/F)\}$ 中取出所有不同的元素 $\sigma_1(\alpha) = \sigma(\alpha), \sigma_2(\alpha), \cdots, \sigma_s(\alpha)$. 令

$$h(x) = \prod_{i=1}^{s}(x - \sigma_i(\alpha)) = x^s + b_1x^{s-1} + \cdots + b_s\,,$$

任取 $\sigma \in Gal(E/F)\,, \sigma\sigma_1(\alpha), \sigma\sigma_2(\alpha), \cdots, \sigma\sigma_s(\alpha)$ 是 $\sigma_1(\alpha), \sigma_2(\alpha), \cdots, \sigma_s(\alpha)$ 的一个排列，所以 $\sigma(b_i) = b_i \in F\,,$ 于是 $h(x) \in F[x]$. 因为 $h(x)$ 的根都是 $p(x)$ 的根，所以有 $h(x)|p(x)\,,$ 但 $p(x)$ 是不可约的，所以得到 $h(x) = p(x)$. 于是 $p(x)$ 的全部根都在 E 中，且没有重根，所以 E/F 是正规可分扩张。

(ii) $\Longrightarrow$ (iii) 由 E/F 是正规扩张，可知 E 是某个多项式 $f(x)$ 在 F 上的分裂域。又因为 E/F 是可分的，所以 $f(x)$ 的每一个不可约因子都是可分的，故 $f(x)$ 是不可分的。

(iii) $\Longrightarrow$ (iv) 设 E 是 F 上可分多项式 $f(x)$ 在 F 上的分裂域，$\alpha_1, \alpha_2, \cdots, \alpha_s$ 是 $f(x)$ 的全部根。那么 $E = F(\alpha_1, \alpha_2, \cdots, \alpha_s)\,,$ 并且每个 α_i 在 F 都是可分的。又注意到 E/F 正规，E 在 F 上的正规闭包 $\overline{E} = E\,,$ 所以可得 $\iota(E/F, E) = [E : F]\,;$ 又根据定义，$\iota(E/F, E) = |Gal(E/F)|\,,$ 所以得到(iv)中的等式。

(iv) $\Longrightarrow$ (i) 记 $L = Inv(Gal(E/F))$. 由命题1.8.1知, $Gal(E/Inv(Gal(E/F))) = Gal(E/F)$，得

$$Gal(E/L) = Gal(E/F)\,.$$

在等式两端作用Inv，得到 $Inv(Gal(E/L)) = L\,,$ 所以 E 是 L 的伽罗瓦扩张。下面证明 $L = F$. 事实上，因为 E 是 L 的伽罗瓦扩张，由前面已证的(i)推出(iv)成立，可以得到

$|Gal(E/L)| = [E:L]$, 从而有 $|Gal(E/F)| = [E:L]$. 又由条件知 $|Gal(E/F)| = [E:F]$, 所以 $[E:F] = [E:L]$. 但是 $F \subseteq Inv(Gal(E/F)) = L$, 从而 $F = L$, E/F 是伽罗瓦扩张。

□

例1.8.3. 设 p 是素数, $F = \mathbb{Z}_p(t^p - t)$, 其中 t 是 $\mathbb{Z}_p$ 上的一个未定元, $E = F(t)$. 则 E 是 F 上的一个 p 次伽罗瓦扩张, 并且伽罗瓦群 $Gal(E/F) \simeq (\mathbb{Z}_p, +)$.

§1.9 伽罗瓦基本定理

我们在本节中证明伽罗瓦理论的基本定理, 先证明一个引理。

引理1.9.1 (阿廷, E.Artin). 设 E 是一个域, G 是 E 的自同构群的一个子群, $F = Inv(G)$ 是 G 的不动域, 那么

$$[E:F] \leqslant |G|.$$

证明. 设 $G = \{id = \sigma_1, \sigma_2, \cdots, \sigma_n\}$, $u_1, u_2, \cdots, u_{n+1}$ 为 E 中的任意 $n+1$ 个非零元素, 用 σ_i 作用于 u_j 得到一个 $n \times (n+1)$ 阶矩阵

$$\mathbf{A} = \begin{pmatrix} \sigma_1(u_1) & \sigma_1(u_2) & \cdots & \sigma_1(u_{n+1}) \\ \sigma_2(u_1) & \sigma_2(u_2) & \cdots & \sigma_2(u_{n+1}) \\ \vdots & \vdots & & \vdots \\ \sigma_n(u_1) & \sigma_n(u_2) & \cdots & \sigma_n(u_{n+1}) \end{pmatrix}.$$

记$\mathbf{A}$ 的列向量依次为 $\beta_1, \beta_2, \cdots, \beta_{n+1}$, 则它们在 E 上线性相关, 设秩为r.适当调序后, 不妨假设 $\beta_1, \beta_2, \cdots, \beta_r$ 线性无关。于是

$$\beta_{r+1} = a_1\beta_1 + a_2\beta_2 + \cdots + a_r\beta_r, \ a_i \in E, \tag{1.7}$$

写成分量形式得到

$$\sigma_i(u_{r+1}) = a_1\sigma_i(u_1) + a_2\sigma_i(u_2) + \cdots + a_r\sigma_(u_r), \ i = 1, 2, \cdots, n. \tag{1.8}$$

任取 $\sigma \in G$, 将 σ 作用于(1.8)式得到

$$(\sigma\sigma_i)(u_{r+1}) = \sigma(a_1)(\sigma\sigma_i)(u_1) + \sigma(a_2)(\sigma\sigma_i)(u_2) + \cdots + \sigma(a_r)(\sigma\sigma_i)(u_r), \ i = 1, 2, \cdots, n.$$

因为 $\sigma\sigma_1, \sigma\sigma_2, \cdots, \sigma\sigma_n$ 是 $\sigma_1, \sigma_2, \cdots, \sigma_n$ 的一个排列, 所以将行向量

$$(\sigma\sigma_i(u_1), \sigma\sigma_i(u_2), \cdots, \sigma\sigma_i(u_{n+1}))$$

适当调序后，再恢复到矩阵**A**中列向量的写法，得到

$$\beta_{r+1} = \sigma(a_1)\beta_1 + \sigma(a_2)\beta_2 + \cdots + \sigma(a_r)\beta_r \,. \tag{1.9}$$

比较(1.7)(1.9)式，由 $\beta_1, \beta_2, \cdots, \beta_r$ 的线性无关性得到

$$\sigma(a_j) = a_j \,, \forall \sigma \in G \,, 1 \leqslant j \leqslant r \,,$$

从而 $a_j \in Inv(G) = F$, $j = 1, 2, \cdots, r$. 在(1.8)式中取 $\sigma_i = \sigma_1 = id$, 得到

$$u_{r+1} = a_1 u_1 + a_2 u_2 + \cdots + a_r u_r \,.$$

所以 $u_1, u_2, \cdots, u_{r+1}$ 在 F 上线性相关，从而 $u_1, u_2, \cdots, u_{n+1}$ 在 F 也上线性相关，所以得到 $[E : F] \leqslant |G|$. □

设 E 是 F 的伽罗瓦扩张，L 是一个中间域。任取 $\sigma \in Gal(E/F)$，称 $\sigma(L)$ 为 L 的**共轭子域**。

定理1.9.2 (伽罗瓦基本定理). *设 E 是 F 的一个伽罗瓦扩张。$G = Gal(E/F)$. 记 $\mathcal{H} = \{H | H \leqslant G\}$, $\mathcal{L} = \{L | F \subseteq L \subseteq E\}$ 是 F 与 E 的中间域集。那么存在两个映射*

$$Gal : \mathcal{L} \longrightarrow \mathcal{H}, \quad L \longmapsto Gal(E/L) \,, Inv : \mathcal{H} \longrightarrow \mathcal{L}, \quad H \longmapsto Inv(H) \,,$$

满足下述五条性质：

(i) Gal和Inv 互为逆映射，因而都是一一映射；

(ii) 上述一一映射是反包含的；

(iii) $[E : L] = |H|$, $[L : F] = [G : H]$;

(iv) 任取 $\sigma \in G$, H 的共轭子群 $\sigma H \sigma^{-1}$ 与 L 的共轭子域对应；

(v) $H \trianglelefteq G$ 当且仅当 L 是 F 的伽罗瓦扩张，这时 $Gal(L/F) \simeq G/H$.

证明. (i) 任取 $L \in \mathcal{L}$. 由 E 是 F 的伽罗瓦扩张知 E/F 是有限正规可分扩张，于是 E/L 也是有限正规可分扩张，从而 E/L 是伽罗瓦扩张，所以 $Inv(Gal(E/L)) = L$, 我们得到 $Inv \cdot Gal = id_{\mathcal{L}}$.

任取 $H \in \mathcal{H}$, 记 $L = Inv(H)$, 于是知 E/L 是伽罗瓦扩张，再由 $H \subseteq Gal(E/L)$ 得 $|H| \leqslant |Gal(E/L)| = [E : L]$. 另一方面，由引理1.9.1得 $[E : L] \leqslant |H|$. 所以

$$|H| = |Gal(E/L)| = [E : L] \,, \tag{1.10}$$

$H = Gal(E/L) = Gal(E/Inv(H))$, 得到 $Gal \cdot Inv = id_{\mathcal{H}}$.

(ii) 前一节已经证明。

(iii) 根据公式(1.10)， $|H| = [E : L]$. 另一方面，

$$[G : H] = |G|/|H| = [E : F]/[E : L] = [L : F].$$

(iv) 记 $L' = \sigma(L)$, $H' = Gal(E/L')$, 我们来证明 $H' = \sigma H \sigma^{-1}$. 事实上，任取 $\alpha' \in L'$, 存在 $\alpha \in L$, 使得 $\alpha' = \sigma(\alpha)$,

$$\sigma\tau\sigma^{-1}(\alpha') = \sigma\tau\sigma^{-1}(\sigma(\alpha)) = \sigma\tau(\alpha) = \sigma(\alpha) = \alpha', \quad \forall \tau \in H,$$

所以 $\sigma H \sigma^{-1} \subseteq H'$. 因为 $L = \sigma^{-1}(L')$, 类似可证 $\sigma^{-1} H' \sigma \subseteq H$, 即 $H' \subseteq \sigma H \sigma^{-1}$, 于是 $H' = \sigma H \sigma^{-1}$.

(v)构造同构映射即可证明 □

定理1.9.2中定义的一一对应叫做**伽罗瓦对应**.

§1.10 多项式的伽罗瓦群

我们知道一个域的伽罗瓦扩张是某个可分多项式的分裂域，我们将在本节证明这个扩张的伽罗瓦群同构于该多项式根集的某个置换群，并通过一系列例子计算伽罗瓦定理给出的中间域与子群之间的对应。

设 $f(x)$ 是域 F 上的一个可分多项式，则 $f(x) = p_1(x)^{e_1} p_2(x)^{e_2} \cdots p_s(x)^{e_s}$, 其中 $p_1(x), p_2(x), \cdots, p_s(x)$ 是 F 上互不相伴的可分不可约多项式。设 $g(x) = p_1(x) p_2(x) \cdots p_s(x)$, 那么 $g(x)$ 与 $f(x)$ 由相同的根集， $g(x)$ 没有重根，而且它们的分裂域相同。

定理1.10.1. *设 $f(x)$ 是域 F 上没有重根的首1多项式， E 是 $f(x)$ 在 F 上的分裂域， $f(x)$ 在 $E[x]$ 中有分解式 $\prod_{i=1}^{n}(x - \alpha_i)$. 那么Gal(E/F)同构于根集 $X = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ 的一个置换群，记作 G_f.*

证明. 任取 $\sigma \in Gal(E/F), \alpha_i \in X$, 都有 $f(\sigma(\alpha_i)) = \sigma(f(\alpha_i)) = 0$, 因而 $\sigma(\alpha_i) \in X$. 映射

$$Gal(E/F) \times X \longrightarrow X, \quad (\sigma, \alpha_i) \longmapsto \sigma(\alpha_i)$$

是 $Gal(E/F)$ 在集合X上的一个作用，因而 $Gal(E/F)$ 的每个元素 σ 诱导出一个置换 $\overline{\sigma} : X \longrightarrow X, \alpha_i \longmapsto \sigma(\alpha_i)$. 令

$$G_f = \{\overline{\sigma} | \sigma \in Gal(E/F)\}.$$

于是知 $\psi : Gal(E/F) \longrightarrow G_f$, $\sigma \longmapsto \overline{\sigma}$ 是群的满同态。当 $\overline{\sigma} = \overline{\tau}$ 时，有 $\sigma(\alpha_i) = \tau(\alpha_i)$, 于是 $\sigma = \tau, \psi$ 是单同态。所以 ψ 是一个同构，$Gal(E/F) \simeq G_f$. □

上述定理定义的 G_f 叫做多项式 $f(x)$ 在 F 上**伽罗瓦群**。下面我们举例说明多项式伽罗瓦群的计算方法。

例1.10.2. 设 $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. 于是知 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域 $E = \mathbb{Q}(\sqrt[3]{2}, \zeta)$, 其中 $\zeta = \frac{-1+\sqrt{-3}}{2}$. 于是 $[E : \mathbb{Q}] = 6$, $|G_f| = 6$. 任取 $\sigma \in G_f$, σ 在 $f(x)$ 的根集上的作用取决于 $\sigma(\sqrt[3]{2})$ 和 $\sigma(\zeta)$. 因为 $x^2 + x + 1$ 是 ζ 在 $\mathbb{Q}$ 上的极小多项式，ζ 的像只能是 ζ 或者 ζ^2. 而 $f(x)$ 是 $\sqrt[3]{2}$ 在 $\mathbb{Q}(\zeta)$ 上的极小多项式，$\sqrt[3]{2}$ 的像只能是 $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta$, $\sqrt[3]{2}\zeta^2$. 于是 G_f 的元素取决于下述六组对应：

$$\zeta \longmapsto \zeta, \sqrt[3]{2} \longmapsto \sqrt[3]{2}; \zeta \longmapsto \zeta, \sqrt[3]{2} \longmapsto \sqrt[3]{2}\zeta; \zeta \longmapsto \zeta, \sqrt[3]{2} \longmapsto \sqrt[3]{2}\zeta^2;$$

$$\zeta \longmapsto \zeta^2, \sqrt[3]{2} \longmapsto \sqrt[3]{2}; \zeta \longmapsto \zeta^2, \sqrt[3]{2} \longmapsto \sqrt[3]{2}\zeta; \zeta \longmapsto \zeta^2, \sqrt[3]{2} \longmapsto \sqrt[3]{2}\zeta^2.$$

将 $f(x)$ 的根按照 $\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2$ 排序，则知 $G_f = S_3$.

例1.10.3. 设 $f(x) = x^4 - 2 \in \mathbb{Q}[x]$, 那么 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域 $E = \mathbb{Q}(\sqrt[4]{2}, i)$, 其中 $[E : \mathbb{Q}] = 8$, 于是 $|G_f| = 8$. 任取 $\sigma \in G_f, \sigma$ 在 $f(x)$ 的根集上的作用取决于 $\sigma(\sqrt[4]{2})$ 和 $\sigma(i)$. 因为 $x^2 + 1$ 是i在 $\mathbb{Q}$ 上的极小多项式，i的像只能是i或-i。又因为 $x^4 - 2$ 是 $\sqrt[4]{2}$ 在 $\mathbb{Q}[i]$ 上的极小多项式，$\sqrt[4]{2}$ 的像只能是 $\pm\sqrt[4]{2}$ 或 $\pm\sqrt[4]{2}i$. 令

$$\rho_1 : E \longrightarrow E, 使得 \rho_1(\sqrt[4]{2}) = \sqrt[4]{2}i, \rho_1(i) = i;$$

$$\tau_0 : E \longrightarrow E, 使得 \tau_0(\sqrt[4]{2}) = \sqrt[4]{2}, \tau_0(i) = -i,$$

那么 $G_f = \{id, \rho_1, \rho_2, \rho_3, \tau_0, \tau_1, \tau_2, \tau_3\}$, 其中 $\rho_i = \rho_1^i, \tau_i = \rho_i\tau_0, i = 0, 1, 2, 3$. 所以知 G_f 是由 ρ_1 和 τ_0 生成的二面体群。

为了讨论方程的可解性，我们在本节的最后给出两种特殊的域扩张及其伽罗瓦群。设 ζ 是一个 n 次本原单位根， n 次分圆域 $\mathbb{Q}(\zeta)$ 是多项式 $x^n - 1$ 在 $\mathbb{Q}$ 上的分裂域，因而是一个伽罗瓦扩张。

命题1.10.4. *(i)* $Gal(\mathbb{Q}(\zeta) : \mathbb{Q}) \simeq U(\mathbb{Z}_n)$,其中 $U(\mathbb{Z}_n)$ 是 $\mathbb{Z}_n$ 中单位的乘法群；

(ii) 如果域 F 是 $\mathbb{Q}$ 的扩张，那么 $Gal(F(\zeta)/F)$ 同构于 $U(\mathbb{Z}_n)$ 的一个子群。

设 E 是域 F 的伽罗瓦扩张。如果 $Gal(E/F)$ 是交换群，那么就称 E/F 是**阿贝尔扩张**；如果 $Gal(E/F)$ 是循环群，那么就称 E/F 是**循环扩张**。

命题1.10.5. 设 F 是 $\mathbb{Q}(\zeta)$ 的一个扩张，其中 ζ 是一个n次本原单位根。令 $a \in F, E$ 是 $x^n - a$ 在 F 上的分裂域。那么 E 在 F 上的伽罗瓦群G是一个循环群，它的阶整除n。特别地，如果 $x^n - a$ 在 F 上是不可约的，那么 $|G| = n$.

§1.11 n 次一般方程的伽罗瓦群

引理1.11.1. 设 $f(x) \in F[x]$, E 是 $f(x)$ 在域 F 上的分裂域，并且 $f(x) = \prod_{i=1}^{n}(x = \alpha_i) \in E[x]$ 没有重根。那么 $f(x)$ 在 F 上是不可约的当且仅当 G_f 在 $X = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ 上的作用是可迁的。

定理1.11.2. 设 $x_1, x_2, \cdots, x_n$ 是域 F 上的无关未定元， $s_1, s_2, \cdots, s_n$ 是关于 $x_1, x_2, \cdots, x_n$ 的初等对称多项式。令

$$f(x) = \prod_{i=1}^{n}(x - x_i) \in F(s_1, s_2, \cdots, s_n)[x],$$

那么 $f(x)$ 在域 $F(s_1, s_2, \cdots, s_n)$ 上的伽罗瓦群 G_f 与 S_n 同构，并且 $f(x)$ 也是域 $F(s_1, s_2, \cdots, s_n)$ 上的不可约多项式。

下面我们讨论域 F 上2，3，4次方程伽罗瓦群的分类，为了保证不可约多项式没有重根，假定 $chF \neq 2, 3$.

设 $f(x)$ 是域 F 上的 n 次首1多项式，并且没有重根，E 是 $f(x)$ 在 F 上的分裂域， $f(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n) \in E[x], E/F$ 是伽罗瓦扩张。定义

$$\Delta = \prod_{1 \leqslant i < j \leqslant n}(\alpha_j - \alpha_i).$$

引理1.11.3. 多项式 $f(x)$ 定义如上。记 $H = G_f \cap A_n$, 则 $Inv(H) = F(\Delta)$. 特别地， $G_f \subseteq A_n$ 当且仅当 $\Delta \in F$.

将 Δ^2 记作 $D(f)$, 称为方程 $f(x) = 0$ 的根的判别式。

例1.11.4. 令 $f(x) = x^2 - a_1 x + a_2 \in F[x]$. 2次方程 $f(x) = 0$ 的判别式我们非常熟悉， $D(f) = a_1^2 - 4a_2$. 当 $D(f) \in F^2$ 时，方程 $f(x) = 0$ 在 F 中可解， $G_f = \{(1)\}$; $D(f) \notin F^2$ 时，方程 $f(x) = 0$ 在 F 中不可解， $G_f = S_2$。

令 $f(x) = x^3 - a_1 x^2 + a_2 x - a_3$, 那么3次方程 $f(x) = 0$ 的判别式

$$D(f) = -4a_1^4 a_2 + a_1^3 a_3 + 18a_1 a_2 a_3 - 4a_2^3 - 27a_3^3.$$

特别地，我们可以做一个线性替换 $x = y + \frac{a_1}{3}$, 使得2次项系数为0，记 $f(x) = x^3 + px + q$, 那么

$$D(f) = -4p^3 - 27q^2.$$

命题1.11.5. *设 $f(x)$ 是域 F 上的 3 次不可约多项式，那么当 $D(f) \in F^2$ 时，$G_f = A_3$; 当 $D(f) \notin F^2$ 时，$G_f = S_3$.*

当方程是4次的时候，G_f 的情况就会复杂很多，下面列出一个结论。

命题1.11.6. *设 $f(x)$ 是域 F 上的 4 次不可约多项式, E 是 $f(x)$ 在 F 上的分裂域.令 $g(x)$ 为 $f(x)$ 的3 次预解式， L 是 $g(x)$ 在 F 上的分裂域， $m = [L : F]$.*

(i) 如果 $g(x)$ 在 F 上不可约，并且 $D(g) \notin F^2$, 那么 $m = 6, G_f \simeq S_4$;

(ii) 如果 $g(x)$ 在 F 上不可约，并且 $D(g) \in F^2$, 那么 $m = 3, G_f \simeq A_4$;

(iii) 如果 $g(x)$ 在 $F[x]$ 中有一个2 次不可约因式，并且 $f(x)$ 在 L 上不可约，那么 $m = 2, G_f \simeq D_4$;

(iv) 如果 $g(x)$ 在 $F[x]$ 中有一个2 次不可约因式，并且 $f(x)$ 在 L 上可约，那么 $m = 2, G_f \simeq \mathbb{Z}_4$;

(v) 如果 $g(x)$ 在 $F[x]$ 中可以分解为一次因式的乘积，那么 $m = 1, G_f \simeq K_4$.

§1.12 方程的根式解

用四则运算和开方运算求解多项式方程是古代数学的一个核心问题，两千多年前，人们已经会解线性方程和二次方程，在文艺复兴时代的意大利，数学家发现了3，4 次方程的公式解。5次方程的公式解困扰了数学界300余年，直到19世纪初，阿贝尔才证明了5次方程没有公式解。随后，天才数学家伽罗瓦给出了多项式方程可用根式解的充分必要条件。在本节中假定ch F=0.

首先给出多项式方程根式可解的定义。如果 $E = F(\alpha)$ 是域 F 的一个单扩张，使得 $\alpha^n \in F$, 那么 E 叫做 F 的一个**单根式扩张**。

如果 E 是 F 的有限扩张，并且存在一个中间域的链

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_s = E\,,$$

使得对于 $i = 1, 2, \cdots, s$, 每一个 F_i 都是 F_{i-1} 的单根式扩张，即 $F_i = F(\alpha_i)\,, \alpha_i^{n_i} \in F_{i-1}$, 那么 E 叫做 F 的**根式扩张**。如果存在 F 的一个根式扩张，包含 $f(x)$ 在 F 上的一个分裂域，那么就称方程 $f(x) = 0$ 在 F 上**根式可解**或可用根式解.

定理1.12.1. 设 F 是一个域，$chF=0$, $f(x)\in F[x]$. 如果多项式方程 $f(x)=0$ 可用根式解，那么 $f(x)$ 在 F 上的伽罗瓦群 G_f 是可解群。

反过来，便有

定理1.12.2. 设 F 是一个域，$chF=0$, $f(x)\in F[x]$. 如果 $f(x)$ 在 F 上的伽罗瓦群 G_f 是可解群，那么方程 $f(x)=0$ 可用根式解。

推论1.12.3. 设 $x_1,x_2,\cdots,x_n$ 是域 F 上的无关未定元，$s_1,s_2,\cdots,s_n$ 是 $x_1,x_2,\cdots,x_n$ 的初等对称多项式，$f(x)=\prod_{i=1}^{n}(x-x_i)\in F(s_1,s_2,\cdots,s_n)[x]$.

(i) 当 $n\leqslant 4$ 时，方程 $f(x)=0$ 在 $F(s_1,s_2,\cdots,s_n)[x]$ 可用根式解；

(ii) 当 $n\geqslant 5$ 时，方程 $f(x)=0$ 在 $F(s_1,s_2,\cdots,s_n)[x]$ 不可用根式解.

注1.12.4. 尺规作图是初等几何的基本问题之一。例如三等分任意角、倍立方和化圆为方，是古代长期未能解决的三大几何作图难题，现在伽罗瓦理论可以给出最终的解答。限于篇幅原因，我们在此处就不再展开讨论了。

参考文献

[1] 张英伯, 王恺顺, 代数学基础（下册）, 北京师范大学出版社, 2013.