第一章

Galois 理论

方程是解决现实问题的重要工具, 方程的类型多种多样, 如代数方程、三角方程、微分方程等. 代数学关注的是代数方程, n 元代数方程形如

$$f(x_1, x_2, \cdots, x_n) = 0,$$

其中 $f(x_1, x_2, \cdots, x_n)$ 是一个 n 元多项式. 一元代数方程解法的讨论由来已久, 公元前 2000 年左右古巴比伦的数学家就能解一元二次方程了. 一元二次方程的一般形式是

$$ax^2 + bx + c = 0,$$

其中 $a \neq 0$. 用配方法得

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2},$$

从而它的根为

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

解一般的三次方程要困难得多, 一直挑战着数学家们, 直到 16 世纪初意大利文艺复兴时期, 这个问题才被意大利的数学家所解决. 约 1515 年, Ferro (费罗) 成功解出了形如 $ax^3 + bx = c$ 的方程.

设三次方程为

$$y^3 + a_1 y^2 + a_2 y + a_3 = 0,$$

令

$$y = x - \frac{a_1}{3},$$

可消去方程中的二次项变为形式

$$x^3 + px + q = 0. \tag{1.1}$$

假设方程 (1.1) 的三个根分别是 x_1, x_2 和 x_3, 则由 Viète (韦达) 定理得

$$\begin{aligned} x_1 + x_2 + x_3 &= 0, \\ x_1x_2 + x_2x_3 + x_1x_3 &= p, \\ x_1x_2x_3 &= -q. \end{aligned} \tag{1.2}$$

设 ω 是一个 3 次本原单位根, 即设

$$\omega = \frac{1}{2}(-1 + \sqrt{-3}),$$

则有 $\omega^2 + \omega = -1$. 令

$$u = \frac{1}{3}(x_1 + \omega x_2 + \omega^2 x_3),$$

$$v=\frac{1}{3}(x_1+\omega^2x_2+\omega x_3),$$

由式 (1.2) 得到

$$uv=-\frac{p}{3},\quad u^3+v^3=-q.$$

从而 u^3 和 v^3 是二次方程

$$z^2+qz-\frac{p^3}{27}=0 \tag{1.3}$$

的两个根. 解二次方程 (1.3) 得

$$z_{1,2}=-\frac{q}{2}\pm\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}.$$

由此

$$u=\sqrt[3]{z_1}=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}},$$
$$v=\sqrt[3]{z_2}=\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}.$$

又显然有

$$x_1=u+v,$$
$$x_2=\omega^2u+\omega v,$$
$$x_3=\omega u+\omega^2v.$$

这样我们就得到上述三次方程的根的公式.

1545 年, Cardano (卡尔达诺) 出版了 *Ars Magna* 一书, 许多历史学家认为这本著作的问世标志着近代数学的开端, 书中给出了三次方程的解法和其学生 Ferrari (费拉里) 对四次方程的解法. 这使得五次或五次以上的代数方程至少看起来可能存在着类似公式, 由此激发了许多数学家去寻找求解四次以上方程的求根公式. 但是, 在这之后的 250 年内, 寻找五次方程的求根公式都失败了.

法国数学家 Lagrange (拉格朗日) 在他的研究中指出, 对于二次、三次、四次的情形, 方程可以通过降次的方法解出. 但把同样的过程应用到五次方程时, 意外之事发生了, 结果方程没有成为想象的四次, 反倒变成了更高次! 这种方法遭遇了彻底失败. 因此 Lagrange 总结道: 用这些方法推导出五次方程的求根公式是不可能的. 意大利人 Ruffini (鲁菲尼) 声称已经证明了一般五次方程不能通过一个公式解出, 并在 1799 年公布了他的证明, 然而数学界对 Ruffini 的证明普遍持怀疑态度. 挪威天才数学家 Abel (阿贝尔) 最终证明了一般的五次方程不存在根式解, 论文发表在 1826 年出版的 *Journal für die*

Reine und Angewandte Mathematik 或称为 *Crelle's Journal* 的第一卷第一期上. 另一位天才数学家法国人 Galois (伽罗瓦) 给出了代数方程有根式解的充要条件是其 Galois 群是可解群.

本章将讨论经典的 Galois 理论, 给出 Galois 这个划时代结果的完整证明, 最后还将给出它在尺规作图这个几何问题上的应用.

1.1　域扩张的 Galois 群与 Galois 扩张

定义 1.1.1　设 E 是一个域, E 的全体自同构的集合在变换的合成下构成一个群, 称其为 E 的**自同构群**, 记为 $\mathrm{Aut}(E)$.

例 1.1.1　考虑有理数域的自同构群. 任取 $\sigma \in \mathrm{Aut}(\mathbb{Q})$, 则有 $\sigma(0) = 0$ 和 $\sigma(1) = 1$. 由

$$0 = \sigma(0) = \sigma(1 + (-1)) = \sigma(1) + \sigma(-1) = 1 + \sigma(-1)$$

得到 $\sigma(-1) = -1$. 再根据 σ 保持加法得到对任意正整数 n 有

$$\sigma(n) = \sigma(\underbrace{1 + 1 + \cdots + 1}_{n\text{ 个}}) = \underbrace{\sigma(1) + \sigma(1) + \cdots + \sigma(1)}_{n\text{ 个}} = n.$$

从而 $\sigma(-n) = \sigma(-1)\sigma(n) = -n$, 这便得到 σ 把每个整数都保持不变. 对任意非零整数 m, 由 σ 保持乘法运算得到

$$1 = \sigma(1) = \sigma\left(m \cdot \frac{1}{m}\right) = \sigma(m)\sigma\left(\frac{1}{m}\right) = m\sigma\left(\frac{1}{m}\right),$$

从而 $\sigma\left(\dfrac{1}{m}\right) = \dfrac{1}{m}$. 这样对任意有理数 $a = \dfrac{n}{m} \in \mathbb{Q}$, 其中 n, m 为整数且 $m \neq 0$, 有

$$\sigma(a) = \sigma\left(\frac{n}{m}\right) = \sigma\left(n \cdot \frac{1}{m}\right) = \sigma(n)\sigma\left(\frac{1}{m}\right) = \frac{n}{m} = a,$$

这便证出 σ 把每个有理数都保持不变, 所以 σ 为 $\mathbb{Q}$ 上的恒等变换 $\mathrm{id}_{\mathbb{Q}}$, 从而 $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}}\}$ 为单位元群.

有理数域 $\mathbb{Q}$ 没有真子域, 即为素域, 对任意素数 p, p 元域 $\mathbb{F}_p$ 也是素域, 同样容易确定出 $\mathrm{Aut}(\mathbb{F}_p)$ 也是单位元群.

下面看 $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}))$. 任取 $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}))$, 由前面的讨论知 σ 把每个有理数都保持不变. 记 $\alpha = \sqrt[3]{2}$, 则 $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\alpha)$ 中每个元素 β 形如 $f(\alpha)$, 其中 $f(x) \in \mathbb{Q}[x]$. 故

$$\sigma(\beta) = \sigma(f(\alpha)) = f(\sigma(\alpha)),$$

即 σ 被 $\sigma(\alpha)$ 所唯一确定. 由于 $\alpha^3-2=0$, 用 σ 作用得到

$$0=\sigma(0)=\sigma(\alpha^3-2)=\sigma(\alpha^3)-\sigma(2)=\sigma(\alpha)^3-2,$$

即 $\sigma(\alpha)$ 也是多项式 x^3-2 的根. 我们知道 x^3-2 的根为

$$\alpha,\ \alpha\omega,\ \alpha\omega^2,$$

其中 $\omega=\dfrac{-1+\sqrt{-3}}{2}$. 由于 $\alpha=\sqrt[3]{2}$ 是实数, 故 $\mathbb{Q}(\sqrt[3]{2})=\mathbb{Q}(\alpha)\subseteq\mathbb{R}$. 又 x^3-2 的三个根中只有 α 为实数, 所以 $\sigma(\alpha)=\alpha$. 进一步地,

$$\sigma(\beta)=f(\sigma(\alpha))=f(\alpha)=\beta.$$

从而 $\sigma=\mathrm{id}_{\mathbb{Q}(\alpha)}$, 故 $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}))$ 仍为单位元群.

例 1.1.2 设 $E=\mathbb{Q}(\sqrt{2},\sqrt{3})$, 考察 $\mathrm{Aut}(E)$. 记 $\alpha=\sqrt{2}$, $\beta=\sqrt{3}$. 显然 α 在 $\mathbb{Q}$ 上的极小多项式为 x^2-2, 所以 $[\mathbb{Q}(\alpha):\mathbb{Q}]=2$. 类似地, β 在 $\mathbb{Q}$ 上的极小多项式为 x^2-3, 由于 $\beta\notin\mathbb{Q}(\alpha)$, 故 β 在 $\mathbb{Q}(\alpha)$ 上的极小多项式仍为 x^2-3, 所以 $[E:\mathbb{Q}(\alpha)]=2$, 由此得到

$$[E:\mathbb{Q}]=[E:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]=4.$$

容易验证 $1,\alpha=\sqrt{2},\beta=\sqrt{3},\alpha\beta=\sqrt{6}$ 构成 E 在 $\mathbb{Q}$ 上的一组基.

由例 1.1.1 中讨论可知, E 的每个自同构 σ 固定 $\mathbb{Q}$, 并且被 $\sigma(\alpha)$ 和 $\sigma(\beta)$ 所唯一确定, 同时 $\sigma(\alpha)$ 是 α 在 $\mathbb{Q}$ 上的极小多项式的根, $\sigma(\beta)$ 是 β 在 $\mathbb{Q}$ 上的极小多项式的根. 由于 x^2-2 的根为 $\pm\alpha$, x^2-3 的根为 $\pm\beta$, 所以 $(\sigma(\alpha),\sigma(\beta))$ 的取值有如下四种可能:

$$(\alpha,\beta),\ (\alpha,-\beta),\ (-\alpha,\beta),\ (-\alpha,-\beta).$$

容易验证, 对如上四种可能取值的每一个, 都可以唯一给出 E 的一个自同构, 例如

$$(\sigma(\alpha),\sigma(\beta))=(\alpha,\beta)$$

给出的是 E 的恒等变换 id_E, 而

$$(\sigma(\alpha),\sigma(\beta))=(-\alpha,\beta)$$

给出的 E 的自同构为

$$\sigma(a+b\alpha+c\beta+d\alpha\beta)=a-b\alpha+c\beta-d\alpha\beta,$$

其中 $a,b,c,d\in\mathbb{Q}$. 从而 $\mathrm{Aut}(E)$ 中有 4 个元素, 但我们需要进一步看 $\mathrm{Aut}(E)$ 的群结构. 记 $\alpha,-\alpha$ 为符号 $1,2$; $\beta,-\beta$ 为符号 $3,4$, 则 $\mathrm{Aut}(E)$ 中每个元素可唯一表示成集合 $\{1,2,3,4\}$ 上的一个置换. 例如

$$(\sigma(\alpha),\sigma(\beta))=(\alpha,\beta)$$

给出恒等变换 (1),

$$(\sigma(\alpha),\sigma(\beta))=(-\alpha,\beta)$$

给出置换 (12),

$$(\sigma(\alpha),\sigma(\beta))=(\alpha,-\beta)$$

给出置换 (34),

$$(\sigma(\alpha),\sigma(\beta))=(-\alpha,-\beta)$$

给出置换 (12)(34). 由此得到 $\mathrm{Aut}(E)$ 同构于置换群

$$\{(1),(12),(34),(12)(34)\},$$

它是两个 2 阶循环群 $\langle(12)\rangle$ 和 $\langle(34)\rangle$ 的直积, 为 Klein (克莱因) 四元群.

定义 1.1.2　*设 E 是域 F 的一个扩张, E 的所有 F-自同构的集合*

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

构成 $\mathrm{Aut}(E)$ 的一个子群, 称为 E 在 F 上的 **Galois 群**.

若 E 为 F 的有限次扩张, 则存在 F 上的代数元 $\alpha_1,\alpha_2,\cdots,\alpha_r\in E$ 使得

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

对任意 $\alpha\in E$,

$$\alpha=\sum_{j_1,j_2,\cdots,j_r}c_{j_1j_2\cdots j_r}\alpha_1^{j_1}\alpha_2^{j_2}\cdots\alpha_r^{j_r},$$

其中 $c_{j_1j_2\cdots j_r}\in F$, $j_1,j_2,\cdots,j_r$ 为非负整数且表达式为有限项求和. 对任意 $\sigma\in\mathrm{Gal}(E/F)$,

$$\sigma(\alpha)=\sum_{j_1,j_2,\cdots,j_r}c_{j_1j_2\cdots j_r}\sigma(\alpha_1)^{j_1}\sigma(\alpha_2)^{j_2}\cdots\sigma(\alpha_r)^{j_r},$$

所以 σ 被 $\sigma(\alpha_1),\sigma(\alpha_2),\cdots,\sigma(\alpha_r)$ 唯一确定. 进一步地, 对任意 $1\leqslant i\leqslant r$, 设 α_i 在 F 上的极小多项式为 $p_i(x)$, 由于 σ 把 $p_i(x)$ 的系数保持不动, 故

$$p_i(\sigma(\alpha_i))=\sigma(p_i(\alpha_i))=\sigma(0)=0,$$

即 $\sigma(\alpha_i)$ 也是 $p_i(x)$ 的根, 从而 $\sigma(\alpha_i)$ 只有有限种取法, 这表明 σ 的个数有有限多, 所以 $\mathrm{Gal}(E/F)$ 为有限群.

若 E 是多项式 $f(x)\in F[x]$ 在 F 上的分裂域, 则同构延拓定理告诉我们

$$|\mathrm{Gal}(E/F)|\leqslant[E:F].$$

实际上该结论对任意的有限次扩张都成立, 这可以给出有限次扩张的 Galois 群阶的进一步刻画.

定理 1.1.1 设 E 和 L 都是 F 的扩张且 $[E:F]$ 有限, 则从 E 到 L 互不相同的 F-同态个数不超过 $[E:F]$. 特别地, $|\mathrm{Gal}(E/F)| \leqslant [E:F]$.

证明 因为 E 为 F 的有限次扩张, 所以存在 F 上的代数元 $\alpha_1, \alpha_2, \cdots, \alpha_r \in E$ 使得

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

下面对 r 做归纳.

若 $r = 0$, 即 $E = F$, 则结论显然成立, 因为从 F 到 L 的 F-同态只有恒等映射这一个, 其个数等于 $[F:F] = 1$.

设 $r \geqslant 1$ 并假设结论对 $r-1$ 成立, 下面证明结论对 r 也成立. 令

$$K = F(\alpha_1, \alpha_2, \cdots, \alpha_{r-1}),$$

则 $E = K(\alpha_r)$, 且由归纳假设从 K 到 L 互不相同的 F-同态个数不超过 $[K:F]$. 因为 $E = K(\alpha_r)$, 所以每一个 F-同态 $\varphi : K \to L$ 的延拓 $\psi : E \to L$ 被 $\psi(\alpha_r)$ 所唯一确定, 从而 φ 延拓到 ψ 的个数为 $\psi(\alpha_r)$ 不同的选取个数. 设 $g(x)$ 是 α_r 在 K 上的极小多项式, 则 $\psi(\alpha_r)$ 是 $\varphi(g)(x) \in \varphi(K)[x]$ 的根. 由于

$$\deg \varphi(g)(x) = \deg g(x) = [E:K],$$

故 $\psi(\alpha_r)$ 的可能选取个数至多为 $[E:K]$, 这表明 F-同态 $\varphi : K \to L$ 延拓为 F-同态 $\psi : E \to L$ 的个数至多为 $[E:K]$. 由于每一个 F-同态 $\psi : E \to L$ 都是某一个 F-同态 $\varphi : K \to L$ 的延拓, 由归纳假设可以得到从 E 到 L 互不相同的 F-同态个数至多为

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

□

定义 1.1.3 设 $G \leqslant \mathrm{Aut}(E)$, $\alpha \in E$, 若对任意 $\sigma \in G$, 都有 $\sigma(\alpha) = \alpha$, 则称 α 为 G 的一个**不动元**, 群 G 的不动元集合

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

构成 E 的一个子域, 称为 G 的**不动域**.

设 E 是域, 将 E 的所有子域构成的集合记为 Γ, 将 $\mathrm{Aut}(E)$ 的所有子群构成的集合记为 Ω, 则得下面两个映射:

$$\begin{aligned} \mathrm{Gal} : \Gamma &\to \Omega \\ L &\mapsto \mathrm{Gal}(E/L) \end{aligned}$$

和

$$\begin{aligned} \mathrm{Inv} : \Omega &\to \Gamma \\ H &\mapsto \mathrm{Inv}(H). \end{aligned}$$

显然这两个映射有下面的反包含性质.

命题 1.1.1　设 L_1, L_2 是域 E 的子域, H_1, H_2 是 $\mathrm{Aut}(E)$ 的子群, 则有

$$L_1 \subseteq L_2 \Rightarrow \mathrm{Gal}(E/L_1) \supseteq \mathrm{Gal}(E/L_2),$$

$$H_1 \subseteq H_2 \Rightarrow \mathrm{Inv}(H_1) \supseteq \mathrm{Inv}(H_2).$$

设 L 是 E 的子域, H 是 $\mathrm{Aut}(E)$ 的子群, 则显然有 $L \subseteq \mathrm{Inv}(\mathrm{Gal}(E/L))$ 和 $H \subseteq \mathrm{Gal}(E/\mathrm{Inv}(H))$. 进一步地, 由 $L \subseteq \mathrm{Inv}(\mathrm{Gal}(E/L))$ 有

$$\mathrm{Gal}(E/L) \supseteq \mathrm{Gal}(E/\mathrm{Inv}(\mathrm{Gal}(E/L))).$$

在 $H \subseteq \mathrm{Gal}(E/\mathrm{Inv}(H))$ 中令 $H = \mathrm{Gal}(E/L)$, 有

$$\mathrm{Gal}(E/L) \subseteq \mathrm{Gal}(E/\mathrm{Inv}(\mathrm{Gal}(E/L))),$$

故

$$\mathrm{Gal}(E/\mathrm{Inv}(\mathrm{Gal}(E/L))) = \mathrm{Gal}(E/L),$$

即 $\mathrm{Gal} \cdot \mathrm{Inv} \cdot \mathrm{Gal} = \mathrm{Gal}$. 类似地, 有

$$\mathrm{Inv}(\mathrm{Gal}(E/\mathrm{Inv}(H))) = \mathrm{Inv}(H),$$

或写成映射复合的形式 $\mathrm{Inv} \cdot \mathrm{Gal} \cdot \mathrm{Inv} = \mathrm{Inv}$.

定义 1.1.4　设 E 是域 F 的扩张, 如果 $\mathrm{Inv}(\mathrm{Gal}(E/F)) = F$, 就称 E 为 F 的一个 **Galois 扩张**.

例 1.1.3　由例 1.1.1 知

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})) = \{\mathrm{id}_{\mathbb{Q}(\sqrt[3]{2})}\},$$

所以

$$\mathrm{Inv}(\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}.$$

故 $\mathbb{Q}(\sqrt[3]{2})$ 不是 $\mathbb{Q}$ 的 Galois 扩张.

下面给出有限次扩张为 Galois 扩张的几个刻画.

定理 1.1.2　设 E 为 F 的有限次扩张, 则下列陈述等价:

(i) E 是 F 的 Galois 扩张;

(ii) E 是 F 的可分正规扩张;

(iii) E 是 F 上一个可分多项式的分裂域;

(iv) $|\mathrm{Gal}(E/F)| = [E : F]$.

证明 (i) ⇒ (ii): 设 E 是 F 的 Galois 扩张. 任取 $\alpha \in E$, 设 $p(x)$ 是 α 在 F 上的极小多项式. 任取 $\sigma \in \mathrm{Gal}(E/F)$, 则

$$p(\sigma(\alpha)) = \sigma(p(\alpha)) = 0,$$

从而 $\sigma(\alpha)$ 也是 $p(x)$ 的根. 在集合

$$\{\sigma(\alpha) \mid \sigma \in \mathrm{Gal}(E/F)\}$$

中取出所有不同的元素 $\sigma_1(\alpha) = \alpha, \sigma_2(\alpha), \cdots, \sigma_s(\alpha)$, 再令

$$h(x) = \prod_{i=1}^{s}(x - \sigma_i(\alpha)) = x^s + b_{s-1}x^{s-1} + \cdots + b_1 x + b_0.$$

任取 $\tau \in \mathrm{Gal}(E/F)$, 考虑 $\tau(h(x))$, 由于

$$\tau\sigma_1(\alpha), \tau\sigma_2(\alpha), \cdots, \tau\sigma_s(\alpha)$$

是 $\sigma_1(\alpha), \sigma_2(\alpha), \cdots, \sigma_s(\alpha)$ 的一个排列, 故 $\tau(h(x)) = h(x)$, 从而对任意 $0 \leqslant i \leqslant s-1$, 有 $\tau(b_i) = b_i$, 故

$$b_i \in \mathrm{Inv}(\mathrm{Gal}(E/F)) = F,$$

所以 $h(x) \in F[x]$. 又 $h(x)$ 的根都是 $p(x)$ 的根, 所以 $h(x) \mid p(x)$, 再由 $p(x)$ 在 $F[x]$ 中不可约得到 $h(x) = p(x)$. 于是 $p(x)$ 的根都在 E 中并且没有重根, 所以 E 是 F 的可分正规扩张.

(ii) ⇒ (iii): E 是 F 的正规扩张, 故 E 是某个多项式 $f(x) \in F[x]$ 在 F 上的分裂域, 又由 E 的可分性知 $f(x)$ 可分.

(iii) ⇒ (iv): E 是可分多项式 $f(x) \in F[x]$ 的分裂域, $\mathrm{Gal}(E/F)$ 中的元素就是 E 的 F-自同构, 由同构延拓定理的强形式有 $|\mathrm{Gal}(E/F)| = [E : F]$.

(iv) ⇒ (i): 记 $L = \mathrm{Inv}(\mathrm{Gal}(E/F))$. 由于

$$\mathrm{Gal}(E/\mathrm{Inv}(\mathrm{Gal}(E/F))) = \mathrm{Gal}(E/F),$$

我们有 $\mathrm{Gal}(E/L) = \mathrm{Gal}(E/F)$. 等式两端用 Inv 作用得到

$$\mathrm{Inv}(\mathrm{Gal}(E/L)) = \mathrm{Inv}(\mathrm{Gal}(E/F)) = L,$$

从而 E 是 L 的 Galois 扩张. 由前面的推导 (i) ⇒ (iv) 得到 $|\mathrm{Gal}(E/L)| = [E : L]$, 再由所给条件得出 $[E : F] = [E : L]$. 但是

$$F \subseteq \mathrm{Inv}(\mathrm{Gal}(E/F)) = L,$$

从而 $F = L$, 这便得到 $\mathrm{Inv}(\mathrm{Gal}(E/F)) = F$, 故 E 是 F 的 Galois 扩张. □

注意到由定理 1.1.2 容易得到若 E/F 为有限 Galois 扩张, L 是其中间域, 则 E/L 也是 Galois 扩张. 事实上, 设 E 是某可分多项式 $f(x) \in F[x]$ 在 F 上的分裂域, 则 E 也是 $f(x)$ 在 L 上的分裂域, 从而 E/L 为 Galois 扩张.

定义 1.1.5　设 E 是 F 的 Galois 扩张, L 是中间域, 对任意 $\sigma \in \mathrm{Gal}(E/F)$, 称 $\sigma(L)$ 为 L 的**共轭**.

定理 1.1.3 (Artin (阿廷) 引理)　设 E 是域, G 为 $\mathrm{Aut}(E)$ 的有限子群, $F = \mathrm{Inv}(G)$, 则

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

证明　设 $|G| = n$, 且

$$G = \{\sigma_1 = \mathrm{id}_E, \sigma_2, \cdots, \sigma_n\},$$

为证明 $[E : F] \leqslant n$, 我们只需证明 E 中任意 $n+1$ 个元素在 F 上线性相关. 设 u_1, $u_2, \cdots, u_{n+1}$ 是 E 中任意 $n+1$ 个元素. 考虑 E 上如下 $n \times (n+1)$ 矩阵:

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

记 A 的列向量组为 $\beta_1, \beta_2, \cdots, \beta_{n+1}$, 它们在 E 上线性相关, 设其秩为 $r \leqslant n$, 并设 $\beta_1, \beta_2, \cdots, \beta_r$ 线性无关, 于是存在 $a_1, a_2, \cdots, a_r \in E$ 使得

$$\beta_{r+1} = a_1\beta_1 + a_2\beta_2 + \cdots + a_r\beta_r.$$

把上式写成分量形式, 即对任意 $1 \leqslant i \leqslant n$ 有

$$\sigma_i(u_{r+1}) = a_1\sigma_i(u_1) + a_2\sigma_i(u_2) + \cdots + a_r\sigma_i(u_r). \tag{1.4}$$

对任意 $\sigma \in G$, 将 σ 作用于式 (1.4) 得到对任意 $1 \leqslant i \leqslant n$ 有

$$(\sigma\sigma_i)(u_{r+1}) = \sigma(a_1)(\sigma\sigma_i)(u_1) + \sigma(a_2)(\sigma\sigma_i)(u_2) + \cdots + \sigma(a_r)(\sigma\sigma_i)(u_r). \tag{1.5}$$

由于 $G = \{\sigma\sigma_1, \sigma\sigma_2, \cdots, \sigma\sigma_n\}$, 把式 (1.5) 写回向量形式得到

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

由 $\beta_1, \beta_2, \cdots, \beta_r$ 的线性无关性得到对任意 $\sigma \in G$ 和任意 $1 \leqslant j \leqslant r$ 有 $\sigma(a_j) = a_j$, 故

$$a_j \in \mathrm{Inv}(G) = F.$$

这时从矩阵 A 的第一行得到

$$u_{r+1} = a_1u_1 + a_2u_2 + \cdots + a_ru_r,$$

从而 $u_1, u_2, \cdots, u_{r+1}$ 在 F 上线性相关, 由此 $u_1, u_2, \cdots, u_{n+1}$ 自然在 F 上线性相关, 这便证出

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

□

下面证明 Galois 理论中一个最重要的定理, 称之为 Galois 基本定理.

定理 1.1.4 (Galois 基本定理) 设 E 是域 F 的一个有限 Galois 扩张, $G = \mathrm{Gal}(E/F)$, 记

$$\mathcal{H} = \{H \mid H \leqslant G\}$$

和

$$\mathcal{L} = \{L \mid L \text{ 为 } E/F \text{ 的中间域, 即 } F \subseteq L \subseteq E\},$$

则

$$\begin{aligned} \mathrm{Gal} : \mathcal{L} &\to \mathcal{H} \\ L &\mapsto \mathrm{Gal}(E/L) \end{aligned}$$

和

$$\begin{aligned} \mathrm{Inv} : \mathcal{H} &\to \mathcal{L} \\ H &\mapsto \mathrm{Inv}(H) \end{aligned}$$

是映射且满足下面五条性质:

(i) Gal 和 Inv 互为逆映射, 因而都是双射.

(ii) 上述双射是反包含的, 即当子群 H_1, H_2 分别与中间域 L_1, L_2 对应时,

$$H_1 \supseteq H_2 \Leftrightarrow L_1 \subseteq L_2.$$

下面设子群 H 与中间域 L 对应, 即 $H = \mathrm{Gal}(E/L)$ 或者 $L = \mathrm{Inv}(H)$.

(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 $\sigma(L)$ 对应.

(v) $H \trianglelefteq G$ 当且仅当 L 是 F 的 Galois 扩张, 这时 $\mathrm{Gal}(L/F) \cong G/H$.

证明 对任意 $F \subseteq L \subseteq E$, 有

$$\mathrm{Gal}(E/L) \subseteq \mathrm{Gal}(E/F) = G,$$

故映射 Gal 的定义是合理的, 同理 Inv 的定义合理.

(i) 任取 $L \in \mathcal{L}$, 则 E/L 是 Galois 扩张, 所以 $\mathrm{Inv}(\mathrm{Gal}(E/L)) = L$, 故 $\mathrm{Inv} \cdot \mathrm{Gal}$ 是 $\mathcal{L}$ 上的恒等变换. 另一方面, 任取 $H \in \mathcal{H}$, 记 $L = \mathrm{Inv}(H)$, 则由

$$\mathrm{Inv}(\mathrm{Gal}(E/\mathrm{Inv}(H))) = \mathrm{Inv}(H)$$

得到 $\mathrm{Inv}(\mathrm{Gal}(E/L)) = L$, 从而 E/L 是 Galois 扩张, 所以 $|\mathrm{Gal}(E/L)| = [E : L]$. 由于

$$H \subseteq \mathrm{Gal}(E/\mathrm{Inv}(H)) = \mathrm{Gal}(E/L),$$

故

$$|H| \leqslant |\mathrm{Gal}(E/L)| = [E : L].$$

再由 Artin 引理有 $[E : L] \leqslant |H|$, 所以 $|H| = |\mathrm{Gal}(E/L)|$. 故

$$H = \mathrm{Gal}(E/L) = \mathrm{Gal}(E/\mathrm{Inv}(H)),$$

从而 $\mathrm{Gal} \cdot \mathrm{Inv}$ 是 $\mathcal{H}$ 上的恒等变换. 所以 Gal 和 Inv 互为逆映射.

(ii) 结论就是命题 1.1.1, 即

$$\begin{aligned} L_1 \subseteq L_2 &\Rightarrow \mathrm{Gal}(E/L_1) \supseteq \mathrm{Gal}(E/L_2), \\ H_1 \supseteq H_2 &\Rightarrow \mathrm{Inv}(H_1) \subseteq \mathrm{Inv}(H_2). \end{aligned}$$

(iii) (i) 中已证

$$|H| = |\mathrm{Gal}(E/L)| = [E : L].$$

另一方面,

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

(iv) 记 $L' = \sigma(L)$, $H' = \mathrm{Gal}(E/L')$. 任取 $\alpha' \in L'$, 存在 $\alpha \in L$ 使得 $\alpha' = \sigma(\alpha)$, 对任意 $\tau \in H$,

$$\sigma\tau\sigma^{-1}(\alpha') = \sigma\tau\sigma^{-1}(\sigma(\alpha)) = \sigma\tau(\alpha) = \sigma(\alpha) = \alpha',$$

所以 $\sigma H\sigma^{-1} \subseteq H'$. 另一方面, 因为 $L = \sigma^{-1}(L')$, 类似地有 $\sigma^{-1}H'\sigma \subseteq H$, 即 $H' \subseteq \sigma H\sigma^{-1}$. 于是

$$H' = \sigma H\sigma^{-1}.$$

(v) 设 L/F 是 Galois 扩张, 则 L/F 是正规的, 故对任意 $\sigma \in G$, 由《代数学（三）》中定理 6.2.4 得到 $\sigma(L) = L$. 由上面的 (iv) 有

$$\mathrm{Inv}(H) = L = \sigma(L) = \mathrm{Inv}(\sigma H\sigma^{-1}),$$

由于 Inv 是双射, 故 $H = \sigma H\sigma^{-1}$, 这便得到 $H \trianglelefteq G$. 反之, 设 $H \trianglelefteq G$, 则对任意 $\sigma \in G$, 有 $H = \sigma H\sigma^{-1}$, 所以 $\sigma(L) = L$, 仍由《代数学（三）》中定理 6.2.4 知 L/F 是正规的. 再由 E/F 可分得到 L/F 可分, 从而 L/F 是可分正规扩张, 所以 L/F 是 Galois 扩张.

进一步地, 设 L/F 是 Galois 扩张, 任取 $\sigma \in G$, 由于 $\sigma(L) = L$, 可令 $\widetilde{\sigma} = \sigma|_L$, 则 $\widetilde{\sigma} \in \mathrm{Gal}(L/F)$. 定义映射 π 为

$$\begin{aligned} \pi:\ G &\to \mathrm{Gal}(L/F) \\ \sigma &\mapsto \widetilde{\sigma}, \end{aligned}$$

容易验证 π 是一个群同态且 $\mathrm{Ker}\,\pi = \mathrm{Gal}(E/L) = H$, 所以 G/H 同构于 $\mathrm{Gal}(L/F)$ 的一个子群. 再由

$$|\mathrm{Gal}(L/F)| = [L:F] = [G:H] = |G/H|$$

得到 $\mathrm{Gal}(L/F) \cong G/H$, 或写成

$$\mathrm{Gal}(L/F) \cong \mathrm{Gal}(E/F)/\mathrm{Gal}(E/L).$$

□

定义 1.1.6 Galois 基本定理中定义的一一对应 $L \leftrightarrow \mathrm{Gal}(E/L)$ 或者 $H \leftrightarrow \mathrm{Inv}(H)$ 也称为 **Galois 对应**.

例 1.1.4 设 $F = \mathbb{F}_q$ 为 q 元域, $q = p^m$, 其中 p 为素数, m 为正整数. 设 E 是 F 的一个 n 次扩张, 则 E 为 q^n 元域, 故 E 为可分多项式 $x^{q^n} - x$ 在 F 上的分裂域, 从而 E/F 为 Galois 扩张, 所以 $|\mathrm{Gal}(E/F)| = [E:F] = n$. 对任意 $\alpha \in E$, 定义 $\sigma(\alpha) = \alpha^q$, 则容易验证 $\sigma \in \mathrm{Gal}(E/F)$. 计算得到 σ 的阶为 $o(\sigma) = n$, 所以 $\mathrm{Gal}(E/F) = \langle\sigma\rangle$ 是一个 n 阶循环群. 对 n 的每个正因子 d, $\mathrm{Gal}(E/F)$ 有唯一的 d 阶子群 $H = \langle\sigma^{\frac{n}{d}}\rangle$, 设 $L = \mathrm{Inv}(H)$, 则有

$$[L:F] = [G:H] = \frac{n}{d},$$

从而 $|\mathrm{Inv}(H)| = |L| = q^{\frac{n}{d}}$. 故每个中间域的元素个数为 q^t, 其中 $t \mid n$.

命题 1.1.2 设 F 是域, L 是 F 的一个扩张, E 是可分多项式 $f(x) \in F[x]$ 在 F 上的分裂域, K 是 $f(x)$ 在 L 上的分裂域, 那么 $\mathrm{Gal}(K/L)$ 同构于 $\mathrm{Gal}(E/F)$ 的一个子群, 记为 $\mathrm{Gal}(K/L) \lesssim \mathrm{Gal}(E/F)$.

证明 设 $f(x)$ 的全部根为 $\alpha_1, \alpha_2, \cdots, \alpha_n$, 则

$$E = F(\alpha_1, \alpha_2, \cdots, \alpha_n) \subseteq L(\alpha_1, \alpha_2, \cdots, \alpha_n) = K.$$

任取 $\sigma \in \mathrm{Gal}(K/L)$, 都有 $\sigma|_F = \mathrm{id}_F$, 又因为 E/F 正规, 由《代数学（三）》中定理 6.2.4 有 $\sigma(E) = E$. 令 $\widetilde{\sigma} = \sigma|_E$, 则 $\widetilde{\sigma} \in \mathrm{Gal}(E/F)$. 定义映射

$$\begin{aligned} \pi: \mathrm{Gal}(K/L) &\to \mathrm{Gal}(E/F) \\ \sigma &\mapsto \widetilde{\sigma}, \end{aligned}$$

则易知 π 是一个群同态. 进一步地, 若 $\widetilde{\sigma} = \mathrm{id}_E$, 则 σ 保持 E 中元素不变, 从而保持 $f(x)$ 的根不变. 又 σ 保持 L 中元素不变, 所以 σ 保持 K 中元素不变, 即 $\sigma = \mathrm{id}_K$. 故 π 为单同态, 所以 $\mathrm{Gal}(K/L)$ 同构于 $\mathrm{Gal}(E/F)$ 的一个子群. □

本节的最后, 我们给出代数基本定理的一个证明.

定理 1.1.5 (代数基本定理)　复数域 $\mathbb{C}$ 是代数封闭域.

证明　只需证明 $\mathbb{C}$ 的代数扩张只有 $\mathbb{C}$ 本身. 若否, 设 L 为 $\mathbb{C}$ 的一个代数扩张, 且 $\mathbb{C} \subsetneq L$. 因为 $\mathbb{C}$ 是实数域 $\mathbb{R}$ 的代数扩张, 所以 L 也是 $\mathbb{R}$ 的代数扩张. 选取 $\theta \in L \setminus \mathbb{C}$, 设 $f(x) \in \mathbb{R}[x]$ 为 θ 在 $\mathbb{R}$ 上的极小多项式, 而 E 是 $f(x)$ 在 $\mathbb{C}$ 上的分裂域. 因为 $\theta \in E$, 但是 $\theta \notin \mathbb{C}$, 所以有域扩张链

$$\mathbb{R} \subsetneq \mathbb{C} \subsetneq E.$$

显然 E 是 $(x^2+1)f(x) \in \mathbb{R}[x]$ 在 $\mathbb{R}$ 上的分裂域, 故 $E/\mathbb{R}$ 为 Galois 扩张. 设 Galois 群 $\mathrm{Gal}(E/\mathbb{R})$ 的阶为

$$|\mathrm{Gal}(E/\mathbb{R})| = 2^j m,$$

其中 $j \geqslant 0$, m 为奇数, 由 Sylow (西罗) 定理知 $\mathrm{Gal}(E/\mathbb{R})$ 有 2^j 阶子群 H. 令 $K = \mathrm{Inv}(H)$, 由 Galois 基本定理有 $[E:K] = |H| = 2^j$. 由于

$$[E:K][K:\mathbb{R}] = [E:\mathbb{R}] = |\mathrm{Gal}(E/\mathbb{R})| = 2^j m,$$

故 $[K:\mathbb{R}] = m$.

下面证明 $m = 1$. 事实上, 任取 $\alpha \in K$, 且 α 在 $\mathbb{R}$ 上的极小多项式为 $g(x)$, 则

$$[\mathbb{R}(\alpha):\mathbb{R}] = \deg g(x),$$

从而

$$\deg g(x) \mid [K:\mathbb{R}] = m,$$

故 $\deg g(x)$ 为奇数. 由初等微积分知奇数次实多项式一定在 $\mathbb{R}$ 中有根, 又 $g(x)$ 在 $\mathbb{R}[x]$ 中不可约, 所以 $\deg g(x) = 1$. 从而 $\alpha \in \mathbb{R}$, 即 $K = \mathbb{R}$, 故 $m = 1$. 从而 $|\mathrm{Gal}(E/\mathbb{R})| = 2^j$ 为 2 的幂.

由于 $\mathrm{Gal}(E/\mathbb{C}) \leqslant \mathrm{Gal}(E/\mathbb{R})$, 故 $|\mathrm{Gal}(E/\mathbb{C})| = 2^t$, 再由 $\mathbb{C} \subsetneq E$ 可知 $t \geqslant 1$. 由 Sylow 定理得到群 $\mathrm{Gal}(E/\mathbb{C})$ 有 2^{t-1} 阶子群 N, 令 $F = \mathrm{Inv}(N)$. 由 Galois 基本定理有 $[E:F] = 2^{t-1}$, 从而 $[F:\mathbb{C}] = 2$. 选取 $\eta \in F \setminus \mathbb{C}$, 并设 $h(x)$ 为 η 在 $\mathbb{C}$ 上的极小多项式, 则有 $\deg h(x) \mid 2$, 再由 $\eta \notin \mathbb{C}$ 有 $\deg h(x) = 2$. 设

$$h(x) = x^2 + ax + b,$$

其中 $a, b \in \mathbb{C}$, 由求根公式得到 $h(x)$ 在 $\mathbb{C}$ 中有根

$$\frac{-a \pm \sqrt{a^2 - 4b}}{2},$$

这与 $h(x)$ 在 $\mathbb{C}[x]$ 中不可约矛盾.

$\mathbb{C}[x]$ 中任意非常数多项式在 $\mathbb{C}$ 上的分裂域为 $\mathbb{C}$ 的代数扩张, 从而都等于 $\mathbb{C}$, 这便得到 $\mathbb{C}[x]$ 中任意非常数多项式的根都在 $\mathbb{C}$ 中, 即在 $\mathbb{C}$ 上分裂. □

习题 1.1

1. 设 $p_1, p_2, \cdots, p_m$ 是两两不同的素数, $E = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \cdots, \sqrt{p_m})$, 求 $\mathrm{Aut}(E)$.

2. 证明实数域 $\mathbb{R}$ 的自同构只有恒等自同构.

3. 设 $\mathbb{Q}$ 上多项式

$$f(x) = x^3 - 3x - 1$$

和

$$g(x) = x^3 - x - 1,$$

分别求 $f(x)$ 和 $g(x)$ 在 $\mathbb{Q}$ 上的分裂域在 $\mathbb{Q}$ 上的 Galois 群, 并求它们的子群及对应的不动域.

4. 求多项式 $x^4 - 2$ 在 $\mathbb{Q}$ 上的分裂域在 $\mathbb{Q}$ 上的 Galois 群, 再求多项式 $x^4 - 2$ 在 $\mathbb{Q}(\mathrm{i})$ 上的分裂域在 $\mathbb{Q}(\mathrm{i})$ 上的 Galois 群, 其中 $\mathrm{i} = \sqrt{-1}$.

5. 设 p 为奇素数, E 为 $x^{p^n} - 1$ 在 $\mathbb{Q}$ 上的分裂域, 证明 $\mathrm{Gal}(E/\mathbb{Q})$ 为 $p^{n-1}(p-1)$ 阶循环群.

6. 设 E/F 为有限次扩张, 证明 E/F 是 Galois 扩张当且仅当对任意 $\alpha \in E$, α 在 F 上的极小多项式为可分多项式且在 E 中分裂.

7. 给出域扩张链 $F \subseteq L \subseteq E$ 的例子使得 L/F 和 E/L 都是 Galois 扩张但是 E/F 不是 Galois 扩张.

8. 设 E 是域 F 的一个有限次扩张, $G = \mathrm{Gal}(E/F)$, 记 $\mathcal{H} = \{H \mid H \leqslant G\}$,

$$\mathcal{L} = \{L \mid L \text{ 为 } E/F \text{ 的中间域, 即 } F \subseteq L \subseteq E\},$$

定义

$$\begin{aligned} \mathrm{Gal}: \mathcal{L} &\to \mathcal{H} \\ L &\mapsto \mathrm{Gal}(E/L), \end{aligned}$$

证明映射 Gal 为满射. 进一步地, 若 E/F 不是 Galois 扩张, 则 Gal 不是单射.

9. 设 $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, 证明 $E/\mathbb{Q}$ 是 Galois 扩张, 并求出 Galois 群 $\mathrm{Gal}(E/\mathbb{Q})$ 和 E 的所有子域.

10. 设 E 是有理数域 $\mathbb{Q}$ 上某个多项式的分裂域且 $[E : \mathbb{Q}]$ 为奇数, 证明 E 是实数域 $\mathbb{R}$ 的子域.

11. 设 $f(x) = x^8 - 2 \in \mathbb{Q}[x]$, E 是 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域, 证明 $E = \mathbb{Q}(\sqrt[8]{2}, \mathrm{i})$ 并给出 $\mathrm{Gal}(E/\mathbb{Q})$ 中所有元素 (通过它们在 $\sqrt[8]{2}$ 和 i 上的作用给出).

12. 设 E 是多项式 $f(x) = x^7 - 1$ 在 $\mathbb{Q}$ 上的分裂域.

(i) 证明 $\mathrm{Gal}(E/\mathbb{Q})$ 是循环群, 并给出此群的一个生成元;

(ii) 证明 E 恰有 4 个子域, 并给出 E 的这 4 个子域;

(iii) 若多项式 $f(x)$ 换成 $x^{29}-1$, 仍用 E 表示 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域, 则这时的 Galois 群 $\mathrm{Gal}(E/\mathbb{Q})$ 是否还是循环群? E 的子域都是什么?

13. 设 $E=F(t)$ 是域 F 上以 t 为变元的有理分式域.

(i) 证明 $\sigma: E\to E$, $f(t)\mapsto f\left(\dfrac{1}{t}\right)$ 是 E 的一个自同构;

(ii) 令 $H=\langle\sigma\rangle$, $L=\mathrm{Inv}(H)$, 给出域 L 并计算扩张次数 $[E:L]$;

(iii) 求 t 在域 L 上的极小多项式;

(iv) 把 σ 换成 $\tau: f(t)\mapsto f(1-t)$, 回答以上问题 (i), (ii) 和 (iii);

(v) 令 $G=\langle\sigma,\tau\rangle$ 为由 σ 和 τ 生成的 E 的自同构群, 证明 $G\cong S_3$ 且

$$\mathrm{Inv}(G)=F(h),$$

其中 $h=\dfrac{(t^2-t+1)^3}{t^2(t-1)^2}$.

14. 设 $F=\mathbb{F}_{37}(t)$, 即域 $\mathbb{F}_{37}$ 上以 t 为变元的有理分式域,

$$f(x)=x^9-t\in F[x],$$

α 是 $f(x)$ 的一个根且令 $E=F(\alpha)$. 证明 $f(x)$ 为 F 上的可分不可约多项式, E 是 $f(x)$ 在 F 上的分裂域且 $\mathrm{Gal}(E/F)$ 为 9 阶循环群.

1.2　多项式的 Galois 群

设 $f(x)$ 是域 F 上的一个可分多项式,

$$f(x)=p_1(x)^{e_1}p_2(x)^{e_2}\cdots p_s(x)^{e_s},$$

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. 令

$$g(x)=p_1(x)p_2(x)\cdots p_s(x),$$

那么 $g(x)$ 与 $f(x)$ 有相同的根集, 从而它们有相同的分裂域, 但是 $g(x)$ 没有重根. 故下面只考虑没有重根的多项式.

定理 1.2.1　*设 $f(x)$ 是域 F 上没有重根的多项式, E 是 $f(x)$ 在 F 上的分裂域, $f(x)$ 在 $E[x]$ 中有分解式*

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

其中 $a\in F$ 为 $f(x)$ 的首项系数, 则 $\mathrm{Gal}(E/F)$ 同构于 $f(x)$ 的根集 $X=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$ 上的一个置换群 G_f.

证明 对任意 $\sigma \in \mathrm{Gal}(E/F)$, $\alpha_i \in X$, 有

$$f(\sigma(\alpha_i)) = \sigma(f(\alpha_i)) = \sigma(0) = 0,$$

因而 $\sigma(\alpha_i) \in X$. 映射 $(\sigma, \alpha_i) \mapsto \sigma(\alpha_i)$ 是 $\mathrm{Gal}(E/F)$ 在集合 X 上的一个作用, 故存在群同态

$$\pi : \mathrm{Gal}(E/F) \to S_X,$$

其中对任意 $\sigma \in \mathrm{Gal}(E/F)$ 和任意 $\alpha_i \in X$ 有

$$\pi(\sigma)(\alpha_i) = \sigma(\alpha_i).$$

又若 $\pi(\sigma) = \mathrm{id}_X$, 即对每个 $1 \leqslant i \leqslant n$, 有 $\sigma(\alpha_i) = \alpha_i$, 故由 $E = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ 得到 $\sigma = \mathrm{id}_E$, 从而 π 为单同态. 令 $G_f = \pi(\mathrm{Gal}(E/F))$, 则 $G_f \leqslant S_X$ 且 $\mathrm{Gal}(E/F) \cong G_f$. □

注 1.2.1 设 E 是 $f(x)$ 在 F 上的分裂域, 则 G_f 就是 $\mathrm{Gal}(E/F)$ 限制到 $f(x)$ 的根集 X 上所得到的群, 即

$$G_f = \{\sigma|_X \mid \sigma \in \mathrm{Gal}(E/F)\},$$

它是 $f(x)$ 的根集上的一个置换群.

定义 1.2.1 设 $f(x)$ 是域 F 上没有重根的多项式, 称 $\mathrm{Gal}(E/F)$ 限制到 $f(x)$ 的根集 X 上所得到的群 G_f 为**多项式 $f(x)$ 的 Galois 群**.

例 1.2.1 设 $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, 则 $f(x)$ 的根为 $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$ 和 $\sqrt[3]{2}\omega^2$, 从而 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域为

$$E = \mathbb{Q}(\sqrt[3]{2}, \omega),$$

其中 $\omega = \dfrac{-1 + \sqrt{-3}}{2}$. 容易计算出 $[E : \mathbb{Q}] = 6$, 故 G_f 为 6 阶群. 但是 G_f 是 3 元集上的置换群, 故 $G_f = S_3$.

更详细地说, 任取 $\sigma \in G_f$, σ 在根集上的作用取决于 $\sigma(\omega)$ 和 $\sigma(\sqrt[3]{2})$. 因为 x^2+x+1 是 ω 在 $\mathbb{Q}$ 上的极小多项式, 而 $\sigma(\omega)$ 也是 ω 在 $\mathbb{Q}$ 上的极小多项式的根, 所以 ω 的像只能是 ω 或 ω^2. 同理, 由于 $f(x)$ 是 $\sqrt[3]{2}$ 在 $\mathbb{Q}$ 上的极小多项式, $\sqrt[3]{2}$ 的像只能是 $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$ 或 $\sqrt[3]{2}\omega^2$. 于是 G_f 的元素取决于下述 6 组对应:

$$\omega \mapsto \omega, \sqrt[3]{2} \mapsto \sqrt[3]{2}; \quad \omega \mapsto \omega, \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega; \quad \omega \mapsto \omega, \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2;$$

$$\omega \mapsto \omega^2, \sqrt[3]{2} \mapsto \sqrt[3]{2}; \quad \omega \mapsto \omega^2, \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega; \quad \omega \mapsto \omega^2, \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2.$$

将 $f(x)$ 的根按照 $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$ 排序, 则第一行的 3 个置换分别为 $(1), (123), (132)$, 第二行的 3 个置换分别为 $(23), (12), (13)$, 故 $G_f = S_3$. G_f 的子群有

$$\{(1)\}, \langle(23)\rangle, \langle(13)\rangle, \langle(12)\rangle, \langle(123)\rangle \text{ 和 } G_f,$$

它们对应的中间域分别为

$$\mathbb{Q}(\sqrt[3]{2},\omega),\ \mathbb{Q}(\sqrt[3]{2}),\ \mathbb{Q}(\sqrt[3]{2}\omega),\ \mathbb{Q}(\sqrt[3]{2}\omega^2),\ \mathbb{Q}(\omega)\text{ 和 }\mathbb{Q}.$$

由于 $\langle(123)\rangle \trianglelefteq G_f$, 故 $\mathbb{Q}(\omega)/\mathbb{Q}$ 正规.

例 1.2.2　设 $f(x)=x^4+x^2-1\in\mathbb{Q}[x]$, 容易验证 $f(x)$ 在有理数域 $\mathbb{Q}$ 上不可约. 令

$$\alpha=\sqrt{\frac{\sqrt{5}-1}{2}},\ \beta=\sqrt{\frac{\sqrt{5}+1}{2}},$$

则有 $\alpha\beta=1$ 且 $f(x)$ 的 4 个根为 $\pm\alpha$, $\pm\mathrm{i}\beta$, 从而 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域为 $E=\mathbb{Q}(\alpha,\mathrm{i})$. 因为 α 在 $\mathbb{Q}$ 上的极小多项式为 $f(x)$, 又 i 在 $\mathbb{Q}(\alpha)$ 上的极小多项式为 x^2+1, 所以

$$[E:\mathbb{Q}]=[\mathbb{Q}(\alpha,\mathrm{i}):\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]=2\cdot 4=8.$$

由于 E 是 $\mathbb{Q}$ 上可分多项式的分裂域, 故 $E/\mathbb{Q}$ 为 Galois 扩张, 所以 $|G_f|=8$.

任取 $\sigma\in G_f$, 类似于例 1.2.1 中的讨论, σ 被 $\sigma(\alpha)$ 和 $\sigma(\mathrm{i})$ 唯一确定. $\sigma(\alpha)$ 是 $f(x)$ 的根, 所以 $\sigma(\alpha)$ 有 4 种可能 $\pm\alpha$, $\pm\mathrm{i}\beta$, $\sigma(\mathrm{i})$ 是 x^2+1 的根, 所以 $\sigma(\mathrm{i})$ 有 2 种可能 $\pm\mathrm{i}$. 由此得到 G_f 中的 8 个元素 σ_i $(0\leqslant i\leqslant 7)$ 如下表, 其中 $X=\{\pm\alpha,\pm\mathrm{i}\beta\}$ 为 $f(x)$ 的根集, 把 X 中的元素 $\alpha,-\alpha,\mathrm{i}\beta,-\mathrm{i}\beta$ 分别记为 $1,2,3,4$, 表中最后一列把 G_f 中的元素写成了集合 $\{1,2,3,4\}$ 上的置换形式.

G_f	α	i	集合 $\{1,2,3,4\}$ 上的置换
σ_0	α	i	(1)
σ_1	$-\alpha$	i	(12)(34)
σ_2	$\mathrm{i}\beta$	i	(13)(24)
σ_3	$-\mathrm{i}\beta$	i	(14)(23)
σ_4	α	$-\mathrm{i}$	(34)
σ_5	$-\alpha$	$-\mathrm{i}$	(12)
σ_6	$\mathrm{i}\beta$	$-\mathrm{i}$	(1324)
σ_7	$-\mathrm{i}\beta$	$-\mathrm{i}$	(1423)

容易计算得到 $G_f=\langle\sigma_6,\sigma_5\rangle$ 且有 $\sigma_6^4=\sigma_5^2=\sigma_0$ 和 $\sigma_5\sigma_6\sigma_5=\sigma_6^{-1}$, 从而 G_f 同构于二面体群 D_4. G_f 有 10 个子群, 除单位元群 $\{\sigma_0\}$ 和自身 G_f 这 2 个平凡子群外, 还有

$$H_1=\{\sigma_0,\sigma_1\},\ H_2=\{\sigma_0,\sigma_2\},\ H_3=\{\sigma_0,\sigma_3\},\ H_4=\{\sigma_0,\sigma_4\},\ H_5=\{\sigma_0,\sigma_5\}$$

这 5 个 2 阶子群和

$$G_1=\{\sigma_0,\sigma_1,\sigma_2,\sigma_3\},\ G_2=\{\sigma_0,\sigma_1,\sigma_4,\sigma_5\},\ G_3=\{\sigma_0,\sigma_1,\sigma_6,\sigma_7\}$$

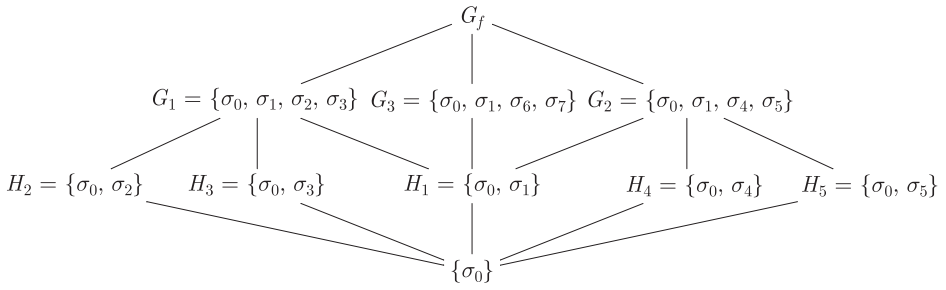
这 3 个 4 阶子群. 这些子群对应的中间域分别为 $\mathrm{Inv}(\{\sigma_0\})=E$, $\mathrm{Inv}(G_f)=\mathbb{Q}$,

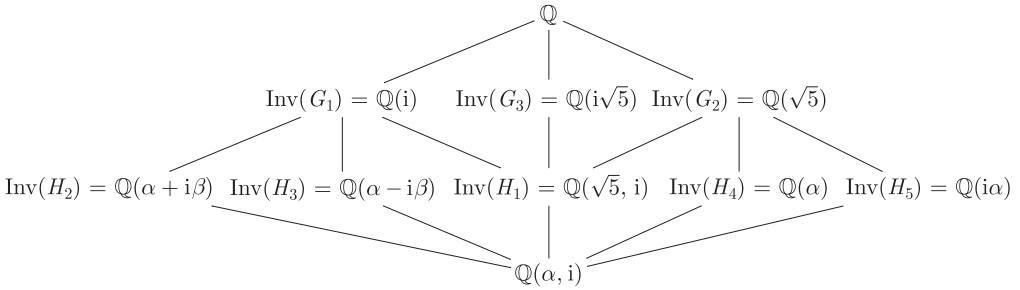
$$\mathrm{Inv}(H_1)=\mathbb{Q}(\sqrt{5},\mathrm{i}),\ \mathrm{Inv}(H_2)=\mathbb{Q}(\alpha+\mathrm{i}\beta),\ \mathrm{Inv}(H_3)=\mathbb{Q}(\alpha-\mathrm{i}\beta),$$
$$\mathrm{Inv}(H_4)=\mathbb{Q}(\alpha),\ \mathrm{Inv}(H_5)=\mathbb{Q}(\mathrm{i}\alpha)$$

和

$$\mathrm{Inv}(G_1)=\mathbb{Q}(\mathrm{i}),\ \mathrm{Inv}(G_2)=\mathbb{Q}(\sqrt{5}),\ \mathrm{Inv}(G_3)=\mathbb{Q}(\mathrm{i}\sqrt{5}).$$

G_f 的子群图以及对应的 $E/\mathbb{Q}$ 的中间域之间的关系图如下所示:





例 1.2.3 设 n 为正整数,

$$f(x)=x^n-1\in\mathbb{Q}[x],$$

则当 $n\geqslant 2$ 时 $f(x)$ 在 $\mathbb{Q}$ 上可约. 任取一个 n 次本原单位根 ζ_n, 比如取 $\zeta_n=\mathrm{e}^{\frac{2\pi\mathrm{i}}{n}}$, 则 $f(x)$ 的根集为

$$\{\zeta_n^j\mid 0\leqslant j\leqslant n-1\}.$$

从而 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域为 $E=\mathbb{Q}(\zeta_n)$.

定义 (第 n 个) **分圆多项式**为

$$\Phi_n(x)=\prod_{0\leqslant k\leqslant n-1,\gcd(n,k)=1}(x-\zeta_n^k).$$

由于 ζ_n 是 n 次本原单位根, 故 ζ_n^k 为 n 次本原单位根当且仅当 $0\leqslant k\leqslant n-1$ 且 k 与 n 互素, 所以 $\Phi_n(x)$ 是以所有 n 次本原单位根为根的首一多项式. 容易计算出 $\Phi_1(x)=x-1$,

$\Phi_2(x)=x+1$, 且由定义有

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

利用 Möbius (默比乌斯) 反演得到

$$\Phi_n(x)=\prod_{d\mid n}(x^d-1)^{\mu(\frac{n}{d})}, \tag{1.6}$$

其中 μ 为 Möbius 函数. 由式 (1.6) 得到 $\Phi_n(x)$ 是一个首一整系数多项式除以一个首一整系数多项式, 故 $\Phi_n(x)\in\mathbb{Z}[x]$ 且首一. 例如当 p 为素数时,

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

设 $p(x)$ 是 ζ_n 在 $\mathbb{Q}$ 上的极小多项式, 则显然有 $p(x)\mid x^n-1$, 而对任意 $1\leqslant m<n$, $\zeta_n^m\neq 1$, 即 ζ_n 不是 x^m-1 的根, 所以 $p(x)\nmid x^m-1$, 因此 $p(x)$ 的根只能是 n 次本原单位根. 下面证明所有的 n 次本原单位根都是 $p(x)$ 的根, 为此先证明如下论断.

论断　对于 $p(x)$ 的任一根 ζ 和任意素数 $r\nmid n$, ζ^r 也是 $p(x)$ 的根.

若否, 设 ζ^r 不是 $p(x)$ 的根, 且 ζ^r 在 $\mathbb{Q}$ 上的极小多项式为 $q(x)$, 则 $p(x)$ 与 $q(x)$ 互素. 由于 $p(x)$ 和 $q(x)$ 都整除 x^n-1, 故

$$p(x)q(x)\mid(x^n-1),$$

从而存在 $s(x)\in\mathbb{Q}[x]$ 使得

$$x^n-1=p(x)q(x)s(x). \tag{1.7}$$

由于 $x^n-1\in\mathbb{Z}[x]$ 是一个首一本原多项式, 且 $p(x)$ 和 $q(x)$ 均首一, 故 $s(x)$ 也首一. 由《代数学（三）》中定理 5.5.3 和定理 5.5.4 可得 $p(x),q(x),s(x)\in\mathbb{Z}[x]$. 另一方面, 由于 ζ^r 是 $q(x)$ 的根, 故 ζ 是 $q(x^r)$ 的根, 所以 $p(x)\mid q(x^r)$, 故存在 $\ell(x)\in\mathbb{Q}[x]$ 使得

$$q(x^r)=p(x)\ell(x). \tag{1.8}$$

同理由于 $q(x^r),p(x)\in\mathbb{Z}[x]$ 且首一, 故有 $\ell(x)\in\mathbb{Z}[x]$ 且首一. 自然同态 $\mathbb{Z}\to\mathbb{Z}_r$ 诱导了多项式环 $\mathbb{Z}[x]$ 上系数模 r 的同态 $\varphi:\mathbb{Z}[x]\to\mathbb{Z}_r[x]$, 并记 $\varphi(g(x))=\overline{g}(x)\in\mathbb{Z}_r[x]$. 将同态 φ 作用到式 (1.7) 和 (1.8) 上得到

$$x^n-\overline{1}=\overline{p}(x)\overline{q}(x)\overline{s}(x),\quad \overline{q}(x^r)=\overline{p}(x)\overline{\ell}(x).$$

由于 $\mathbb{Z}_r$ 为 r 元域, 其中每个元素的 r 次方等于自身, 故

$$\overline{q}(x^r)=\overline{q}(x)^r,$$

所以 $\overline{p}(x)$ 与 $\overline{q}(x)$ 不互素, 从而 $x^n-\overline{1}$ 在 $\mathbb{Z}_r$ 的扩域中有重根. 但是在 $\mathbb{Z}_r[x]$ 中

$$(x^n-\overline{1})'=nx^{n-1}$$

与 $x^n-\overline{1}$ 互素, 矛盾. 故论断得证.

对任意正整数 $1\leqslant k<n$ 且 $\gcd(k,n)=1$, 设

$$k=p_1p_2\cdots p_s$$

为 k 的素因子分解式. 由于 k 与 n 互素, 显然对任意 $1\leqslant i\leqslant s$, 有 $p_i\nmid n$. 由于 ζ_n 是 $p(x)$ 的根, 由前面已证明的论断有 $\zeta_n^{p_1}$ 是 $p(x)$ 的根, 接着

$$\zeta_n^{p_1p_2}=(\zeta_n^{p_1})^{p_2}$$

是 $p(x)$ 的根, 一直下去, $\zeta_n^k=\zeta_n^{p_1p_2\cdots p_s}$ 是 $p(x)$ 的根, 所以任意 n 次本原单位根都是 $p(x)$ 的根, 故 $\Phi_n(x)\mid p(x)$. 又由于 ζ_n 是 $\Phi_n(x)$ 的根, 故 $p(x)\mid\Phi_n(x)$, 所以 $p(x)=\Phi_n(x)$. 故 $\Phi_n(x)$ 在 $\mathbb{Q}$ 上不可约, 且

$$[E:\mathbb{Q}]=\deg\Phi_n(x)=\phi(n).$$

E 是 x^n-1 在 $\mathbb{Q}$ 上的分裂域, 也是 $\Phi_n(x)$ 在 $\mathbb{Q}$ 上的分裂域, 称其为 n 次**分圆域**. 显然 $E/\mathbb{Q}$ 为 Galois 扩张, 从而 $|\mathrm{Gal}(E/\mathbb{Q})|=\phi(n)$.

任取 $\sigma\in G_f=G_{\Phi_n}$, σ 在根集上的作用取决于 $\sigma(\zeta_n)$, 又 $\sigma(\zeta_n)$ 只能取某个 ζ_n^k, 其中 $0\leqslant k\leqslant n-1$ 且 $\gcd(k,n)=1$. 对固定的 k, 记 $\sigma_k(\zeta_n)=\zeta_n^k$, 所以

$$G_{\Phi_n}=\{\sigma_k\mid 0\leqslant k\leqslant n-1,\ \text{且 }\gcd(k,n)=1\}.$$

定义 G_{Φ_n} 到整数模 n 的乘法群 $U(n)$ 的映射 π 为 $\pi(\sigma_k)=\overline{k}$, 容易验证 π 为群同构, 所以

$$G_f=G_{\Phi_n}\cong U(n).$$

由于 $\mathrm{Gal}(E/\mathbb{Q})$ 为交换群, 每个子群都正规, 故对 $E/\mathbb{Q}$ 的任意中间域 L, $L/\mathbb{Q}$ 也是 Galois 扩张.

例 1.2.4 设 $f(x)=x^3+x+1\in\mathbb{F}_2[x]$, 由于 $0,1$ 都不是 $f(x)$ 的根, 故 $f(x)$ 在 $\mathbb{F}_2$ 上不可约. 设 α 是 $f(x)$ 的一个根, 则 α 在 $\mathbb{F}_2$ 上的极小多项式为 $f(x)$. 由《代数学（三）》中定理 6.4.2 得到 $f(x)$ 的所有根为

$$\alpha,\ \alpha^2\ \text{和}\ \alpha^4=\alpha^2+\alpha,$$

所以 $f(x)$ 在 $\mathbb{F}_2$ 上的分裂域为 $E=\mathbb{F}_2(\alpha)$. 显然 $[E:\mathbb{F}_2]=3$, 故 G_f 为 3 阶群, 它一定为循环群. 任取 $\sigma\in G_f$, σ 在根集上的作用取决于 $\sigma(\alpha)$, 又 $\sigma(\alpha)$ 为 $f(x)$ 的根, 故 $\sigma(\alpha)$ 只能是 α, α^2 或 $\alpha^2+\alpha$. 将对应的同构分别记为 σ_0, σ_1, σ_2, 则 $\sigma_0=\mathrm{id}_E$, $\sigma_2=\sigma_1^2$, 所以

$$G_f=\langle\sigma_1\rangle.$$

因为 G_f 没有真子群, 所以 $\mathbb{F}_2$ 与 E 之间没有真中间域. (事实上, $f(x)$ 的分裂域 E 为 8 元域 $\mathbb{F}_8$.)

例 1.2.5　设 p 为素数, t 是域 $\mathbb{F}_p$ 上的未定元, $F=\mathbb{F}_p(t)$,

$$f(x)=x^p-x-t\in F[x],$$

下面求 $f(x)$ 在 F 上的 Galois 群.

记

$$\mathbb{F}_p=\{0,1,\cdots,p-1\},$$

注意到对任意 $c\in\mathbb{F}_p$ 有 $c^p=c$, 设 α 是多项式 $f(x)=x^p-x-t$ 的一个根, 则 $f(x)$ 的所有根为

$$\alpha,\alpha+1,\cdots,\alpha+p-1.$$

因此 $f(x)$ 无重根, 从而 $f(x)$ 可分, 且 $f(x)$ 在 F 上的分裂域为 $E=F(\alpha)$, 故 E/F 为 Galois 扩张. 由于 $t=\alpha^p-\alpha$, 故 $E=\mathbb{F}_p(t,\alpha)=\mathbb{F}_p(\alpha)$. 设 σ 为 $\mathbb{F}_p$ 上的恒等变换 $\mathrm{id}_{\mathbb{F}_p}$ 由 $\alpha\mapsto\alpha+1$ 所延拓的 E 的自同构, 即 $\sigma\in\mathrm{Aut}(E),\sigma(\alpha)=\alpha+1$, 且 $\sigma|_{\mathbb{F}_p}=\mathrm{id}_{\mathbb{F}_p}$, 则

$$\sigma(t)=\sigma(\alpha^p-\alpha)=\sigma(\alpha)^p-\sigma(\alpha)=(\alpha+1)^p-(\alpha+1)=t,$$

故 $\sigma\in\mathrm{Gal}(E/F)$, 从而 $\langle\sigma\rangle\leqslant\mathrm{Gal}(E/F)$. 注意到 $o(\sigma)=p$, 所以

$$p=|\langle\sigma\rangle|\leqslant|\mathrm{Gal}(E/F)|=[E:F]\leqslant p,$$

于是 $\mathrm{Gal}(E/F)$ 为 p 阶循环群. 进一步地, 还可以得到 $f(x)$ 在 F 上不可约, 否则 α 在 F 上的极小多项式 $p(x)$ 的次数小于 p, 与 $[E:F]=p$ 矛盾.

定义 1.2.2　设 E 是域 F 的 Galois 扩张, 如果 $\mathrm{Gal}(E/F)$ 为交换群, 就称 E/F 是**交换扩张**或 **Abel 扩张**; 若 $\mathrm{Gal}(E/F)$ 为循环群, 则称 E/F 是**循环扩张**.

注 1.2.2　由例 1.2.3 知 $\mathbb{Q}(\zeta_n)$ 是 $\mathbb{Q}$ 上的 Abel 扩张. 进一步地, 若 F 是 $\mathbb{Q}$ 的扩域, 则由

$$\mathrm{Gal}(F(\zeta_n)/F)\lesssim\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

得到 $F(\zeta_n)$ 是 F 上的 Abel 扩张. 另外, 例 1.2.5 给出的扩张是循环扩张.

命题 1.2.1　设 F 是域 $\mathbb{Q}(\zeta_n)$ 的扩域, 其中 ζ_n 是一个 n 次本原单位根. 令 $a\in F^*$, E 是

$$f(x)=x^n-a\in F[x]$$

在 F 上的分裂域, 那么 $\mathrm{Gal}(E/F)$ 为循环群, 其阶为 n 的因子. 特别地, 如果 $f(x)$ 在 F 上不可约, 那么 $\mathrm{Gal}(E/F)$ 为 n 阶循环群.

证明 设 $\theta=\sqrt[n]{a}$, 则 $f(x)$ 的根为

$$\theta,\zeta_n\theta,\zeta_n^2\theta,\cdots,\zeta_n^{n-1}\theta,$$

故 $E=F(\theta)$. 任取 $\sigma\in\mathrm{Gal}(E/F)$, 则 $\sigma(\theta)$ 仍为 $f(x)$ 的根, 故存在某个 $0\leqslant i\leqslant n-1$, 使得 $\sigma(\theta)=\zeta_n^i\theta$. 记这样的同构 σ 为 σ_i, 从而 $\sigma_i=\sigma_j$ 当且仅当 $\zeta_n^i=\zeta_n^j$, 再由 ζ_n 为 n 次本原单位根且 $0\leqslant i,j\leqslant n-1$ 得到 $\sigma_i=\sigma_j$ 当且仅当 $i=j$. 定义映射 $\pi:\mathrm{Gal}(E/F)\to\mathbb{Z}_n$ 为 $\pi(\sigma_i)=\bar{i}$, 则 π 为单射. 再由

$$\sigma_i\sigma_j(\theta)=\sigma_i(\zeta_n^j\theta)=\sigma_i(\zeta_n^j)\sigma_i(\theta)=\zeta_n^j\zeta_n^i\theta=\zeta_n^{i+j}\theta$$

得到 π 为群的单同态, 故 $\mathrm{Gal}(E/F)$ 同构于加法群 $\mathbb{Z}_n$ 的一个子群. 从而 $\mathrm{Gal}(E/F)$ 为循环群, 且阶为 n 的因子. 进一步地, 若 $f(x)$ 在 F 上不可约, 则 θ 在 F 上的极小多项式为 $f(x)$, 从而

$$|\mathrm{Gal}(E/F)|=[F(\theta):F]=n.$$

□

定理 1.2.2 设 $f(x)$ 是域 F 上没有重根的多项式, 则 $f(x)$ 在 F 上不可约当且仅当 G_f 在 $f(x)$ 的根集上的作用传递.

证明 不失一般性, 设 $f(x)\in F[x]$ 首一且 $\deg f(x)=n$. 设 E 是 $f(x)$ 在 F 上的分裂域且 $f(x)$ 在 $E[x]$ 中有分解式

$$f(x)=\prod_{i=1}^{n}(x-\alpha_i),$$

记 $f(x)$ 的根集为 $X=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$. 对任意 $1\leqslant i\leqslant n$, 设 α_i 在 F 上的极小多项式为 $p_i(x)$, 则显然有 $p_i(x)\mid f(x)$.

若 G_f 在 X 上的作用传递, 则对任意 α_i, 存在 $\sigma\in G_f$ 使得 $\sigma(\alpha_1)=\alpha_i$. 注意到 $\sigma\in G_f$, α_1 为 $p_1(x)$ 的根, 所以 $\alpha_i=\sigma(\alpha_1)$ 也是 $p_1(x)$ 的根, 因而 $(x-\alpha_i)\mid p_1(x)$. 于是 $f(x)\mid p_1(x)$, 从而 $f(x)=p_1(x)$ 是 F 上的不可约多项式.

反之, 若 $f(x)$ 在 F 上不可约, 则对所有 $1\leqslant i\leqslant n$, 均有 $p_i(x)=f(x)$. 任取 $\alpha_i\in X$, $1\leqslant i\leqslant n$, 存在一个 F-同构 $\tau:F(\alpha_1)\to F(\alpha_i)$ 使得 $\tau(\alpha_1)=\alpha_i$. 注意到此时 E 也是 $f(x)$ 在 $F(\alpha_i)$ 上的分裂域, 故 τ 可以延拓成 E 的 F-自同构 σ, 即存在 $\sigma\in\mathrm{Gal}(E/F)$ 使得 $\sigma|_{F(\alpha_1)}=\tau$, 由此得到 $\sigma(\alpha_1)=\tau(\alpha_1)=\alpha_i$, 于是 G_f 在 X 上的作用传递. □

注 1.2.3 设 $f(x)$ 是 F 上的可分不可约多项式, $\deg f(x)=n$, 由定理 1.2.2 知 G_f 在 $f(x)$ 的根集

$$X=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$$

上的作用传递, 故 $n=|X|=[G_f:(G_f)_{\alpha_1}]$, 从而 $|G_f|$ 可被 $f(x)$ 的次数 n 整除.

设 $f(x)\in F[x]$, $\deg f(x)=n\geqslant 1$, $f(x)$ 在其分裂域中的根为 $\alpha_1,\alpha_2,\cdots,\alpha_n$. 定义 $f(x)$ 的**判别式**为

$$D_f=a^{2n-2}\prod_{1\leqslant i<j\leqslant n}(\alpha_j-\alpha_i)^2,$$

其中 a 为 $f(x)$ 的首项系数. 显然, D_f 是 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 的对称多项式, 从而是 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 的初等对称多项式的多项式, 由 Viète 定理易知 $D_f\in F$. 又显然 $f(x)$ 没有重根当且仅当 $D_f\neq 0$.

定理 1.2.3　*设域 F 的特征不为 2, $f(x)\in F[x]$, $\deg f(x)=n\geqslant 1$, 且 $f(x)$ 没有重根, 则 G_f 中的每个元素都是 $f(x)$ 的根集 $X=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$ 上的偶置换当且仅当 D_f 为 F 中的平方元.*

证明　设 E 是 $f(x)$ 在 F 上的分裂域, 从而 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$. 记

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

则 $\delta\in E$ 且 $a^{2(n-1)}\delta^2=D_f$. 由于 $a\in F$, 故 D_f 为域 F 中的平方元当且仅当 $\delta\in F$.

任取 $\sigma\in G_f$, 用 $\operatorname{sgn}(\sigma)$ 表示置换 σ 的符号, 即 $\operatorname{sgn}(\sigma)=\pm 1$ 且 $\operatorname{sgn}(\sigma)=1$ 当且仅当 σ 为偶置换. 由于 $\sigma(X)=X$, 容易验证

$$\sigma(\delta)=\prod_{1\leqslant i<j\leqslant n}(\sigma(\alpha_j)-\sigma(\alpha_i))=\operatorname{sgn}(\sigma)\prod_{1\leqslant i<j\leqslant n}(\alpha_j-\alpha_i)=\operatorname{sgn}(\sigma)\cdot\delta.$$

因为域 F 的特征不为 2, 又 $\delta\neq 0$, 所以 $\delta\neq-\delta$, 从而 σ 为偶置换当且仅当 $\sigma(\delta)=\delta$. 由于 E/F 为 Galois 扩张, 故对所有 $\sigma\in G_f$ 都有 $\sigma(\delta)=\delta$ 当且仅当

$$\delta\in\operatorname{Inv}(\operatorname{Gal}(E/F))=F.$$

□

例 1.2.6　设域 F 的特征不为 2, $f(x)$ 是域 F 上无重根的 3 次不可约多项式, 则有 $3\mid|G_f|$, 从而 $G_f\cong A_3$ 或者 S_3. 进一步地, 若 $D_f\in F^{*2}$, 则 $G_f\cong A_3$, 反之 $G_f\cong S_3$.

设 $f(x)=x^3+ax+b$, 容易算出

$$D_f=-4a^3-27b^2.$$

例如对 $\mathbb{Q}$ 上的不可约多项式 $f(x)=x^3-2$, 其判别式 $D_f=-108$ 不是有理数的平方, 故 $G_f\cong S_3$, 这正是例 1.2.1 的结论. 再看

$$f(x)=x^3-3x-1\in\mathbb{Q}[x],$$

它在 $\mathbb{Q}$ 上不可约且 $D_f = 81$ 为有理数的平方, 所以它的 Galois 群 $G_f \cong A_3$.

注意到

$$f(x) = x^3 - 2x + 1 \in \mathbb{Q}[x]$$

的判别式 $D_f = 5$, 但它的 Galois 群 G_f 不是 S_3, 因为该多项式在 $\mathbb{Q}[x]$ 中可约, 所以 G_f 在它的 3 个根构成的集合上的作用不是传递的, 故不可能为 S_3.

下面讨论 4 次无重根多项式的 Galois 群. 依然设 $\operatorname{char} F \neq 2$, 设 $f(x) \in F[x]$, 若 $f(x)$ 在 F 上可约, 则问题可转化为次数 $\leqslant 3$ 的情形, 下面设 $f(x)$ 不可约. 不失一般性, 可设 $f(x)$ 首一且其 3 次项系数为零, 故记

$$f(x) = x^4 + ax^2 + bx + c.$$

由于 F 的特征不为 2, 故

$$f'(x) = 4x^3 + 2ax + b \neq 0,$$

又 $f(x)$ 不可约, 所以 $f(x)$ 没有重根. 设 $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ 为 $f(x)$ 的根, $E = F(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ 是 $f(x)$ 在 F 上的分裂域. 对任意 $\sigma \in G_f$, 记 $\sigma(\alpha_i) = \alpha_{\sigma(i)}$, 这样就把 σ 看成是集合 $\{1, 2, 3, 4\}$ 上的置换. 由于 $G_f \leqslant S_4$, 又 $4 \mid |G_f|$, 故 $|G_f| = 24, 12, 8$ 或者 4. G_f 是 S_4 的传递子群, 所以 G_f 只可能是 S_4, A_4, S_4 的 Sylow 2-子群, 即 8 阶二面体群

$$D_4 = \langle (1234), (12)(34) \rangle,$$

4 阶循环群 $\mathbb{Z}_4 = \langle (1234) \rangle$ 或者 Klein 四元群

$$V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}.$$

令

$$\alpha = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4),$$

$$\beta = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4),$$

$$\gamma = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3),$$

则容易计算出

$$\beta - \alpha = (\alpha_3 - \alpha_2)(\alpha_4 - \alpha_1),$$

$$\gamma - \alpha = (\alpha_3 - \alpha_1)(\alpha_4 - \alpha_2),$$

$$\gamma - \beta = (\alpha_2 - \alpha_1)(\alpha_4 - \alpha_3),$$

所以 α, β, γ 两两不同. 设以 α, β, γ 为根的多项式为

$$g(x) = (x - \alpha)(x - \beta)(x - \gamma) = x^3 + px^2 + qx + r.$$

利用 Viète 定理经过计算可得

$$p = -(\alpha+\beta+\gamma) = -2a,$$

$$q = \alpha\beta+\beta\gamma+\gamma\alpha = a^2-4c,$$

$$r = -\alpha\beta\gamma = b^2,$$

所以 $g(x)\in F[x]$, 还容易计算得到 $D_g = D_f$, 称 $g(x)$ 为 $f(x)$ 的**预解式**. 令

$$L = F(\alpha,\beta,\gamma)\subseteq E,$$

则 L 是无重根多项式 $g(x)$ 在 F 上的分裂域, 从而 L/F 为 Galois 扩张. 进一步地, 容易验证 V_4 中的元素同时固定 α,β 和 γ. 熟知 S_4 有 5 个共轭类, 代表元可以分别取为

$$(1),\ (12)(34),\ (12),\ (123),\ (1234),$$

而 V_4 是前两个共轭类的并. 显然 (12) 对换 β 和 γ, (123) 把 α,β,γ 映为 γ,α,β, (1234) 对换 α 和 γ, 它们都不能同时固定 α,β 和 γ. 而对后 3 个共轭类中任一置换 π, 设 $\pi=\sigma\tau\sigma^{-1}$, 其中 $\tau=(12),(123)$ 或者 (1234), $\sigma\in S_4$, 显然 π 把 3 元组 $(\sigma(\alpha),\sigma(\beta),\sigma(\gamma))$ 映为 $(\sigma(\tau(\alpha)),\sigma(\tau(\beta)),\sigma(\tau(\gamma)))$. 由于 $\tau(\alpha,\beta,\gamma)\neq(\alpha,\beta,\gamma)$, 又 σ 为 $\{\alpha,\beta,\gamma\}$ 上的置换, 故 π 不能同时固定 α,β 和 γ. 这便证出 S_4 的后 3 个共轭类中的元素都不能同时固定 α,β 和 γ, 从而只有 V_4 中的 4 个置换同时使 α,β,γ 都保持不动, 所以 $\mathrm{Gal}(E/L)\cong G_f\cap V_4$. 由 Galois 基本定理,

$$G_f/(G_f\cap V_4)\cong \mathrm{Gal}(L/F)\cong G_g.$$

下面记

$$m = |G_g| = [L:F],$$

并分成下面 5 种情形分别讨论.

情形 1: 若 $g(x)$ 在 F 上不可约且 $D_f = D_g\notin F^{*2}$, 则 $G_g\cong S_3$. 故 $m=6$ 且 $6\mid|G_f|$, 从而 $|G_f|=24$ 或者 12. 又 S_4 只有唯一的一个 12 阶子群 A_4, 包含了所有的偶置换, 所以 G_f 包含了所有的偶置换. 再由 $D_f\notin F^{*2}$ 知 G_f 中有奇置换, 故 $G_f\cong S_4$.

情形 2: 若 $g(x)$ 在 F 上不可约且 $D_f = D_g\in F^{*2}$, 则 $G_g\cong A_3$. 故 $m=3$, 且 $3\mid|G_f|$, 又 $4\mid|G_f|$, 所以 $12\mid|G_f|$. 但由 $D_f\in F^{*2}$ 知 G_f 中无奇置换, 所以 $G_f\cong A_4$.

情形 3: 若 $g(x)$ 在 $F[x]$ 中有一个 2 次不可约因式, 则 $m=|G_g|=2$, 故

$$[G_f : G_f\cap V_4] = 2.$$

进一步地, 若 $f(x)$ 在 L 上不可约, 由于 E 也是 $f(x)$ 在 L 上的分裂域, 从而 $f(x)$ 的次数 4 整除 Galois 群 $\mathrm{Gal}(E/L)$ 的阶, 故 $[E:L]=|\mathrm{Gal}(E/L)|\geqslant 4$. 由

$$4 = |V_4|\geqslant |G_f\cap V_4| = [E:L]\geqslant 4$$

可以得到 $|G_f \cap V_4| = 4$, 故 $|G_f| = 8$. 因此 G_f 为 S_4 的 Sylow 2-子群, 它们彼此共轭, 都同构于二面体群 D_4.

情形 4: 若 $g(x)$ 在 $F[x]$ 中有一个 2 次不可约因式且 $f(x)$ 在 L 上可约, 这时仍然有 $m = 2$ 和

$$[G_f : G_f \cap V_4] = 2.$$

下面证明 $|G_f \cap V_4| < 4$. 事实上, 若 $|G_f \cap V_4| = 4$, 则 $G_f \cap V_4 = V_4$, 从而 $\mathrm{Gal}(E/L) \cong V_4$. 但是 V_4 在 $f(x)$ 的根集上传递, 所以 $f(x)$ 在 L 上不可约, 矛盾. 从而由 $|G_f \cap V_4| < 4$ 就得到 $|G_f| < 8$, 再由 $4 \mid |G_f|$ 得到 $|G_f| = 4$. S_4 的 4 阶传递子群有 $\langle(1234)\rangle$ 和 V_4 这两种类型, 其中只有群 $\langle(1234)\rangle$ 中有奇置换. 设 $g(x)$ 的三个根中 α, β 是 F 上 2 次不可约多项式 $h(x)$ 的根, 而 $\gamma \in F$, 这时

$$D_g = (\gamma - \alpha)^2(\gamma - \beta)^2(\beta - \alpha)^2 = h(\gamma)^2 D_h.$$

注意到 $h(\gamma) \in F$, 又 $h(x)$ 在 F 上不可约, 故 $h(x)$ 在 F 中无根, 因此其判别式 $D_h \notin F^{*2}$. 所以 $D_f = D_g \notin F^{*2}$, 于是 G_f 中有奇置换, 从而 $G_f \cong \langle(1234)\rangle \cong \mathbb{Z}_4$.

情形 5: 若 $g(x)$ 在 F 上分解为一次因式的乘积, 则有 $\alpha, \beta, \gamma \in F$, 从而 $L = F$. 这时 $G_f = G_f \cap V_4$, 即 $G_f \subseteq V_4$, 又 $4 \mid |G_f|$, 故 $G_f \cong V_4$.

综合上面的讨论, 我们有如下定理.

定理 1.2.4 *设域 F 的特征不为 2, $f(x)$ 是 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 $f(x)$ 的预解式, L 是 $g(x)$ 在 F 上的分裂域, $m = [L : F]$.*

(i) *若 $g(x)$ 在 F 上不可约且 $D_f \notin F^{*2}$, 则 $m = 6$, $G_f \cong S_4$.*

(ii) *若 $g(x)$ 在 F 上不可约且 $D_f \in F^{*2}$, 则 $m = 3$, $G_f \cong A_4$.*

(iii) *若 $g(x)$ 在 $F[x]$ 中有一个 2 次不可约因式, 且 $f(x)$ 在 L 上不可约, 则 $m = 2$, $G_f \cong D_4$.*

(iv) *若 $g(x)$ 在 $F[x]$ 中有一个 2 次不可约因式, 且 $f(x)$ 在 L 上可约, 则 $m = 2$, $G_f \cong \mathbb{Z}_4$.*

(v) *若 $g(x)$ 在 $F[x]$ 中分解为一次因式的乘积, 则 $m = 1$, $G_f \cong V_4$.*

4 次不可约多项式的 Galois 群的分类已经有点复杂了, 次数更高的不可约多项式的 Galois 群的分类问题则更加困难, 而下面所说的 Galois 反问题至今仍未解决.

Galois 反问题: 对于有限群 G, 是否存在有理数域 $\mathbb{Q}$ 上的 Galois 扩张 E 使得

$$\mathrm{Gal}(E/\mathbb{Q}) \cong G\,?$$

下面我们构造一个 n 次多项式, 使其 Galois 群为对称群 S_n. 为此设 $x_1, x_2, \cdots, x_n$ 是域 K 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, 则 $s_1, s_2, \cdots, s_n$ 也是域 K 上的无关未定元.

定理 1.2.5　设 $x_1, x_2, \cdots, x_n$ 是域 K 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 $F = K(s_1, s_2, \cdots, s_n)$ 以及

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

则 $f(x)$ 在域 F 上的 Galois 群 G_f 同构于 n 元对称群 S_n.

证明　设 E 是 $f(x)$ 在 F 上的分裂域, 则

$$E = K(s_1, s_2, \cdots, s_n)(x_1, x_2, \cdots, x_n) = K(x_1, x_2, \cdots, x_n),$$

所以 E 中元素可写为形式 $\dfrac{a}{b}$, 其中 a, b 都是域 K 上 $x_1, x_2, \cdots, x_n$ 的多项式且 $b \neq 0$. 对任意 $\sigma \in S_n$, 定义 $\sigma : E \to E$ 为

$$\sigma\left(\frac{a}{b}\right) = \frac{\sigma(a)}{\sigma(b)},$$

其中对 $a = a(x_1, x_2, \cdots, x_n) \in K[x_1, x_2, \cdots, x_n]$,

$$\sigma(a) = \sigma(a(x_1, x_2, \cdots, x_n)) = a(x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(n)}).$$

则 $\sigma \in \mathrm{Aut}(E)$ 且对任意 $1 \leqslant i \leqslant n$ 有 $\sigma(s_i) = s_i$, 故 $\sigma \in \mathrm{Gal}(E/F)$, 从而

$$|G_f| = |\mathrm{Gal}(E/F)| \geqslant n!.$$

又 G_f 是 n 元集 $X = \{x_1, x_2, \cdots, x_n\}$ 上的对称群, 所以 $G_f \cong S_n$. □

注 1.2.4　定理 1.2.5 中的 $F = K(s_1, s_2, \cdots, s_n)$ 是多项式环 $K[s_1, s_2, \cdots, s_n]$ 的分式域, 它是域 K 的超越扩张. 另外由于 G_f 在 X 上的作用传递, 故 $f(x)$ 在 F 上不可约.

设 p 为素数, 下面给出有理数域 $\mathbb{Q}$ 上以对称群 S_p 为 Galois 群的 p 次多项式.

定理 1.2.6　设 p 为素数, $f(x)$ 是 $\mathbb{Q}$ 上的 p 次不可约多项式, 如果 $f(x)$ 在 $\mathbb{C}$ 中恰有 2 个非实数复根, 那么 $G_f \cong S_p$.

证明　不妨设 $f(x)$ 首一且在复数域 $\mathbb{C}$ 上有分解

$$f(x) = \prod_{i=1}^{p}(x - \alpha_i) \in \mathbb{C}[x],$$

其中 α_1, α_2 是 $f(x)$ 的非实数复根, $\alpha_3, \cdots, \alpha_p$ 是 $f(x)$ 的实数根. 因为 $f(x)$ 是 $\mathbb{Q}$ 上的 p 次不可约多项式, 所以 $p \mid |G_f|$, 由 Sylow 定理知 G_f 中有 p 阶元 ρ. 设 τ 是 $\mathbb{C}$ 中的共轭变换, 则

$$\tau(\alpha_1) = \alpha_2, \quad \tau(\alpha_2) = \alpha_1,$$

且对 $3 \leqslant i \leqslant p$ 有 $\tau(\alpha_i) = \alpha_i$, 故 τ 为 G_f 中的对换. 由于 $\rho, \tau \in G_f$, 故

$$S_p = \langle \rho, \tau \rangle \leqslant G_f,$$

再由 G_f 是 p 元集 $\{\alpha_1, \alpha_2, \cdots, \alpha_p\}$ 上的置换群得到 $G_f \cong S_p$. □

例 1.2.7 设 $q > 11$ 为素数,

$$f(x) = x^5 - qx + q \in \mathbb{Q}[x],$$

由 Eisenstein (艾森斯坦) 判别法知 $f(x)$ 在 $\mathbb{Q}$ 上不可约. 又

$$f'(x) = 5x^4 - q,$$

实多项式 $f(x)$ 有两个极值点 $\pm\sqrt[4]{\dfrac{q}{5}}$, 因为

$$\lim_{x \to -\infty} f(x) = -\infty, f\left(-\sqrt[4]{\frac{q}{5}}\right) > 0, f\left(\sqrt[4]{\frac{q}{5}}\right) < 0, \lim_{x \to +\infty} f(x) = +\infty,$$

所以 $f(x)$ 有 3 个实根. 从而 $f(x)$ 有 2 个非实数复根, 由定理 1.2.6 得 $G_f \cong S_5$.

类似地, 有理数域 $\mathbb{Q}$ 上的不可约多项式

$$g(x) = x^5 - 4x - 1$$

的 Galois 群 $G_g \cong S_5$. 但是 $\mathbb{Q}$ 上的不可约多项式

$$h(x) = x^5 - x - 1$$

只有 1 个实根, 因此定理 1.2.6 不适用于对它的 Galois 群的讨论.

多项式的 Galois 群是它的根集上的置换群, 而对于不可约多项式 $f(x)$, 通过它的 Galois 群和一个根, 也可以得到 $f(x)$ 的所有根.

定理 1.2.7 *设 $f(x) \in F[x]$ 是不可约多项式, E 是 $f(x)$ 在 F 上的分裂域, α 是 $f(x)$ 在 E 中的一个根, 则 $f(x)$ 的所有根都形如 $\sigma(\alpha)$, 其中 $\sigma \in \mathrm{Gal}(E/F)$.*

证明 对任意 $\sigma \in \mathrm{Gal}(E/F)$, 由

$$f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$$

知 $\sigma(\alpha)$ 是 $f(x)$ 的根. 另一方面, 设 β 是 $f(x)$ 的一个根, 由 $f(x)$ 不可约知存在一个 F-同构 $\tau : F(\alpha) \to F(\beta)$ 使得 $\tau(\alpha) = \beta$. 又 E 是 $f(x)$ 分别在 $F(\alpha)$ 和 $F(\beta)$ 上的分裂域, 故 τ 可以延拓成 E 的 F-自同构 σ 且 $\sigma|_{F(\alpha)} = \tau$. 从而存在 $\sigma \in \mathrm{Gal}(E/F)$ 使得 $\sigma(\alpha) = \tau(\alpha) = \beta$. □

注 1.2.5 在定理 1.2.7 中即使多项式 $f(x)$ 可分也可能会出现 $\sigma_1 \neq \sigma_2 \in \mathrm{Gal}(E/F)$, 但是 $\sigma_1(\alpha) = \sigma_2(\alpha)$ 的情形. 例如 $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ 是可分多项式, 它有 3 个根, 但是它的 Galois 群的阶为 6.

例 1.2.8　设 $F=\mathbb{F}_q$ 为 q 元域, $f(x)$ 为 F 上的一个 n 次首一不可约多项式,

$$E=F[x]/(f(x)),$$

则 E 中元素 $\overline{x}$ 是 $f(x)$ 的一个根. 记 $\alpha=\overline{x}$, 则 α 在 F 上的极小多项式为 $f(x)$ 且 $E=F(\alpha)$. 由例 1.1.4 知 $\mathrm{Gal}(E/F)=\langle\sigma\rangle$, 其中对任意 $\beta\in E$ 有 $\sigma(\beta)=\beta^q$, 所以由定理 1.2.7 得到 $f(x)$ 的全部根为

$$\alpha,\ \alpha^q,\ \alpha^{q^2},\cdots,\alpha^{q^{n-1}}.$$

这就是《代数学（三）》中的定理 6.4.2.

习题 1.2

1. 设

$$f(x)=x^4-2x^2+3\in\mathbb{Q}[x],$$

求出 $f(x)$ 的 Galois 群 G_f, 并确定 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域的所有子域.

2. 设

$$f(x)=x^6-4\in\mathbb{Q}[x],$$

求出 $f(x)$ 的 Galois 群 G_f, 并确定 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域的所有子域.

3. 设 E 是域 F 的 Galois 扩张, $\mathrm{Gal}(E/F)\cong S_3$, 证明 E 是 F 上一个 3 次不可约多项式的分裂域.

4. 求 $\mathbb{Q}(\mathrm{e}^{\frac{2\pi\mathrm{i}}{15}})$ 的子域个数.

5. 设 p 为素数, 求 p^{40} 元有限域的子域个数.

6. 计算 $\Phi_{20}(x)$ 并把 $x^{20}-1$ 分解为 $\mathbb{Q}[x]$ 中不可约多项式的乘积.

7. 设 p 为素数且 $p\neq 2,3$,

$$f(x)=x^3+ax+b$$

为 $\mathbb{Z}_p[x]$ 中不可约多项式, 证明此多项式的判别式为 $\mathbb{Z}_p$ 中的平方元.

8. 证明任一有限群都是某个域上多项式的 Galois 群.

9. 设 G 为有限交换群, 证明存在 $\mathbb{Q}$ 上的 Galois 扩张 E 使得 $\mathrm{Gal}(E/\mathbb{Q})\cong G$.

10. 设复数 $\alpha=\sqrt{(2+\sqrt{2})(-3+\sqrt{3})}$, $E=\mathbb{Q}(\alpha)$,

(i) 证明 $\mathbb{Q}(\alpha^2)=\mathbb{Q}(\sqrt{2},\sqrt{3})\subsetneq\mathbb{Q}(\alpha)$, 并由此证明 $[\mathbb{Q}(\alpha):\mathbb{Q}]=8$;

(ii) 令 $\alpha_1,\alpha_2,\cdots,\alpha_8$ 是 8 个复数 $\pm\sqrt{(2\pm\sqrt{2})(-3\pm\sqrt{3})}$, 令

$$f(x)=\prod_{j=1}^{8}(x-\alpha_j),$$

证明 $f(x)\in\mathbb{Q}[x]$ 且 $f(x)$ 为 α 在 $\mathbb{Q}$ 上的极小多项式;

(iii) 令 $\beta=\sqrt{(2-\sqrt{2})(-3+\sqrt{3})}$, φ 为 $\mathbb{Q}(\alpha)$ 的自同构使得 $\varphi(\alpha)=\beta$, 证明

$$\varphi(\sqrt{2})=-\sqrt{2},\ \ \varphi(\sqrt{3})=\sqrt{3},\ \ \varphi(\alpha\beta)=-\alpha\beta,\ \ \varphi(\beta)=-\alpha,$$

并由此证明 φ 的阶为 4;

(iv) 类似地令 $\gamma=\sqrt{(2+\sqrt{2})(-3-\sqrt{3})}$, $\delta=\sqrt{(2-\sqrt{2})(-3-\sqrt{3})}$, ψ 和 η 为 $\mathbb{Q}(\alpha)$ 的自同构使得 $\psi(\alpha)=\gamma$, $\eta(\alpha)=\delta$, 证明 ψ 和 η 的阶都是 4 且 $\eta=\psi\varphi$;

(v) 证明 $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ 有 6 个 4 阶元, 1 个 2 阶元和 1 个 1 阶元 (单位元), 并由此得到 $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ 同构于四元数群;

(vi) 求 $\mathbb{Q}(\alpha)$ 的所有子域.

11. 给出一般 4 次方程的求根公式.

1.3 方程的根式解

本节讨论代数方程是否有根式解这个问题.

定义 1.3.1 设 $E=F(\alpha)$ 是域 F 的一个单扩张, 如果存在正整数 n 使得 $\alpha^n\in F$, 就称 E 为 F 的一个**单根式扩张**.

例 1.3.1 设 n 为正整数, ζ_n 是一个 n 次本原单位根. 由例 1.2.3 知 $E=\mathbb{Q}(\zeta_n)$ 是 $f(x)=x^n-1$ 在 $\mathbb{Q}$ 上的分裂域, 也是分圆多项式 $\Phi_n(x)$ 在 $\mathbb{Q}$ 上的分裂域. 由于 $\zeta_n^n=1\in\mathbb{Q}$, 故 $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ 是单根式扩张.

设 F 为 $\mathbb{Q}(\zeta_n)$ 的扩域, $a\in F^*$, 由命题 1.2.1 知多项式 x^n-a 在 F 上的分裂域为 $E=F(\theta)$, 其中 $\theta=\sqrt[n]{a}$. 由于 $\theta^n=a\in F$, 故 $F(\theta)/F$ 也是单根式扩张.

注 1.3.1 对于单根式扩张 $F(\alpha)/F$, 由于有正整数 n 使得 $\alpha^n\in F$, 故 α 是多项式

$$x^n-\alpha^n\in F[x]$$

的根, 从而 α 为 F 上的代数元. 因此 $F(\alpha)/F$ 一定是单代数扩张, 自然也是有限次扩张.

定义 1.3.2 设 E/F 是有限次扩张, 若存在一个域的扩张链

$$F=F_0\subseteq F_1\subseteq\cdots\subseteq F_{s-1}\subseteq F_s=E, \tag{1.9}$$

使得对于每个 $1\leqslant i\leqslant s$, F_i 是 F_{i-1} 的单根式扩张, 即存在 $\alpha_i\in F_i$ 和正整数 n_i 使得

$$F_i=F_{i-1}(\alpha_i)$$

且 $\alpha_i^{n_i} \in F_{i-1}$, 则称 E 为 F 的一个**根式扩张**, 而如上域的扩张链 (1.9) 叫做根式扩张 E/F 的一个**根式扩张链**.

设多项式 $f(x) \in F[x]$, 如果 $f(x)$ 的每一个根都可以用对 $f(x)$ 的系数施行有限次加、减、乘、除和开方运算的式子表达出来, 就称方程 $f(x) = 0$ **根式可解**或者**有根式解**. 因为加、减、乘、除四则运算可以在任意域中进行, 而对 F 的一个元素 a 开 n 次方, 相当于求一个元素 α 使得 $\alpha^n = a$, 即有一个单根式扩张 $F(\alpha)/F$. 于是施行有限次加、减、乘、除和开方运算就是存在一个根式扩张链 (1.9) 使得 $f(x)$ 的每个根都在 E 中, 这表明若方程 $f(x) = 0$ 根式可解, 则 $f(x)$ 的根都在 F 的某个根式扩张 E 中. 反之, 如果存在 F 的一个根式扩张 E/F 使得 $f(x)$ 的每个根都在 E 中, 那么这时有一个根式扩张链 (1.9), 从而 $f(x)$ 的每一个根可以由 $f(x)$ 的系数施行有限次加、减、乘、除和开方运算表达出来. 由此可给出如下定义.

定义 1.3.3　设 F 是域, $f(x) \in F[x]$, 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, 那么就称代数方程 $f(x) = 0$ (或多项式 $f(x)$) 在 F 上**根式可解**或**有根式解**.

例 1.3.2　由例 1.3.1 知对任意正整数 n, 多项式 $f(x) = x^n - 1$ 和分圆多项式 $\Phi_n(x)$ 在有理数域 $\mathbb{Q}$ 上根式可解. 进一步地, 设 ζ_n 是一个 n 次本原单位根, F 为 $\mathbb{Q}(\zeta_n)$ 的扩域, $a \in F^*$, 则 $x^n - a$ 在 F 上根式可解.

下面我们讨论一般多项式的根式可解性, 先证明如下引理.

引理 1.3.1　设 E 是 F 的有限可分扩张, $\widetilde{E}$ 是 E/F 的正规闭包. 如果 E/F 是根式扩张, 那么 $\widetilde{E}/F$ 也是根式扩张.

证明　设 E/F 的一个根式扩张链为 (1.9)

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{s-1} \subseteq F_s = E,$$

其中 $F_i = F_{i-1}(\alpha_i)$, $\alpha_i^{n_i} \in F_{i-1}$, $1 \leqslant i \leqslant s$, 从而

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

由于 E/F 为有限次扩张, 故为代数扩张. 设 α_i 在 F 上的极小多项式为 $p_i(x)$, 令

$$f(x) = \prod_{i=1}^{s} p_i(x),$$

由《代数学（三）》中定理 6.2.5 的证明知 E/F 的正规闭包 $\widetilde{E}$ 为 $f(x)$ 在 F 上的分裂域. 由 E/F 的可分性知 $f(x)$ 可分, 所以 $\widetilde{E}/F$ 是 Galois 扩张. 令

$$\mathrm{Gal}(\widetilde{E}/F) = \{\sigma_1 = \mathrm{id}_{\widetilde{E}}, \sigma_2, \cdots, \sigma_n\},$$

则由定理 1.2.7 知对任意 $1 \leqslant i \leqslant s$, $p_i(x)$ 的根为

$$\sigma_1(\alpha_i), \sigma_2(\alpha_i), \cdots, \sigma_n(\alpha_i),$$

所以

$$\widetilde{E} = F(\sigma_1(\alpha_1), \sigma_2(\alpha_1), \cdots, \sigma_n(\alpha_1), \sigma_1(\alpha_2), \sigma_2(\alpha_2), \cdots, \sigma_n(\alpha_2), \cdots,$$
$$\sigma_1(\alpha_s), \sigma_2(\alpha_s), \cdots, \sigma_n(\alpha_s)).$$

令 $S_0 = \varnothing$, 并对任意 $1 \leqslant i \leqslant s$, 记

$$S_i = \{\sigma_1(\alpha_1), \sigma_2(\alpha_1), \cdots, \sigma_n(\alpha_1), \cdots, \sigma_1(\alpha_i), \sigma_2(\alpha_i), \cdots, \sigma_n(\alpha_i)\}.$$

由于 $F_i = F_{i-1}(\alpha_i) = F(\alpha_1, \cdots, \alpha_i)$, 故 $F_i \subseteq F(S_i)$. 进一步地, 对任意 $1 \leqslant i \leqslant s$ 和 $0 \leqslant j \leqslant n$, 记

$$S_{i-1,j} = S_{i-1} \cup \{\sigma_1(\alpha_i), \cdots, \sigma_j(\alpha_i)\},$$

其中 $S_{i-1,0} = S_{i-1}$, 则显然有 $S_{i-1,n} = S_i$. 考察扩张链

$$F(S_{i-1}) = F(S_{i-1,0}) \subseteq F(S_{i-1,1}) \subseteq \cdots \subseteq F(S_{i-1,n}) = F(S_i). \tag{1.10}$$

易见对于 $1 \leqslant j \leqslant n$, $S_{i-1,j} = S_{i-1,j-1} \cup \{\sigma_j(\alpha_i)\}$. 由于 $\alpha_i^{n_i} \in F_{i-1} \subseteq F(S_{i-1})$, 我们有

$$\sigma_j(\alpha_i)^{n_i} = \sigma_j(\alpha_i^{n_i}) \in \sigma_j(F(S_{i-1})) = F(\sigma_j(S_{i-1})) = F(S_{i-1}) \subseteq F(S_{i-1,j-1}),$$

故链 (1.10) 是根式扩张链. 由此得到对每个 $1 \leqslant i \leqslant s$, 都有从 $F(S_{i-1})$ 到 $F(S_i)$ 的根式扩张链. 由于 $F(S_0) = F$, $F(S_s) = \widetilde{E}$, 把这 s 个链连接起来就得到一个从 F 到 $\widetilde{E}$ 的根式扩张链, 故 $\widetilde{E}/F$ 是根式扩张. □

下面讨论特征为 0 的域上多项式的根式可解性. 设 $\operatorname{char} F = 0$, n 为正整数,

$$f(x) = x^n - 1 \in F[x],$$

则有 $f'(x) = nx^{n-1}$, 从而 $f(x)$ 与 $f'(x)$ 互素, 故 $f(x)$ 没有重根. 设 G 为 $f(x)$ 在它的分裂域 E 中的全部根构成的集合, 容易验证 G 为 E^* 的 n 阶子群, 由《代数学 (三)》中推论 2.3.2 知 G 是循环群. 设 ζ 是 G 的一个生成元, 则 $o(\zeta) = n$, 从而 ζ 是一个 n 次本原单位根. 这表明特征为 0 的域的某个扩域中一定有 n 次本原单位根.

定理 1.3.1 *设 F 是特征为 0 的域, $f(x) \in F[x]$. 如果代数方程 $f(x) = 0$ 在 F 上根式可解, 那么 $f(x)$ 在 F 上的 Galois 群 G_f 是可解群.*

证明 由于 $\operatorname{char} F = 0$, 故 F 包含有理数域 $\mathbb{Q}$. 设 K 是 $f(x)$ 在 F 上的分裂域, 因为 $f(x) = 0$ 在 F 上根式可解, 所以存在 F 的根式扩张 E 使得 $E \supseteq K$, 根据引理 1.3.1, 可设 E/F 是有限正规扩张, 并设 (1.9) 是从 F 到 E 的根式扩张链. 令

$$n = \operatorname{lcm}(n_1, n_2, \cdots, n_s),$$

ζ_n 是一个在 F 的某个扩域中的 n 次本原单位根.

对任意 $0 \leqslant i \leqslant s$, 记 $F_i' = F_i(\zeta_n)$, $E' = E(\zeta_n)$, 考察扩张链

$$F = F_0 \subseteq F_0' \subseteq F_1' \subseteq \cdots \subseteq F_{s-1}' \subseteq F_s' = E'. \tag{1.11}$$

显然 F_0' 是 $x^n - 1$ 在 F 上的分裂域, 而对于 $1 \leqslant i \leqslant s$, F_i' 是多项式 $x^{n_i} - \alpha_i^{n_i}$ 在 F_{i-1}' 上的分裂域, 因而上述 $s+1$ 个扩张都是 Galois 扩张. 根据 Galois 基本定理, 可得次正规群列

$$\mathrm{Gal}(E'/F_0) \trianglerighteq \mathrm{Gal}(E'/F_0') \trianglerighteq \mathrm{Gal}(E'/F_1') \trianglerighteq \cdots \trianglerighteq \mathrm{Gal}(E'/F_{s-1}') \trianglerighteq \{\mathrm{id}_{E'}\}. \tag{1.12}$$

由注 1.2.2 知 F_0'/F_0 是一个 Abel 扩张, 所以

$$\mathrm{Gal}(E'/F_0)/\mathrm{Gal}(E'/F_0') \cong \mathrm{Gal}(F_0'/F_0)$$

是一个交换群. 对于 $1 \leqslant i \leqslant s$, $F_i' = F_{i-1}'(\alpha_i)$, $\alpha_i^{n_i} \in F_{i-1} \subseteq F_{i-1}'$, 由于 n_i 次本原单位根 $\zeta_n^{\frac{n}{n_i}} \in F_{i-1}'$, 而 F_i' 是 $x^{n_i} - \alpha_i^{n_i}$ 在 F_{i-1}' 上的分裂域, 所以由命题 1.2.1 知 F_i'/F_{i-1}' 是循环扩张, 故

$$\mathrm{Gal}(E'/F_{i-1}')/\mathrm{Gal}(E'/F_i') \cong \mathrm{Gal}(F_i'/F_{i-1}')$$

是循环群. 这便证出次正规群列 (1.12) 的因子群都是交换群, 由《代数学（三）》中定理 3.4.3 得到 $\mathrm{Gal}(E'/F)$ 是可解群. 又因为

$$F \subseteq K \subseteq E'$$

并且 K/F 是 Galois 扩张, 所以

$$\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E'/F)/\mathrm{Gal}(E'/K).$$

故 $\mathrm{Gal}(K/F)$ 作为可解群 $\mathrm{Gal}(E'/F)$ 的商群依然可解, 从而群 G_f 是可解群. □

反之, 若 $f(x)$ 的 Galois 群 G_f 为可解群, $f(x) = 0$ 是否根式可解?

命题 1.3.1 (Lagrange 预解式)　*设 F 是特征为 0 的域, p 是素数, 且 F 包含一个 p 次本原单位根 ζ_p, 那么 F 的任意 p 次循环扩张 E 都是单根式扩张.*

证明　因为 E 是 F 的 p 次循环扩张, 所以 $[E:F] = p$ 且 $G = \mathrm{Gal}(E/F) = \langle\sigma\rangle$ 为 p 阶循环群. 任取 $\theta \in E \backslash F$, 有 $[F(\theta):F] \mid p$ 且 $[F(\theta):F] > 1$, 所以 $[F(\theta):F] = p$, 故 $E = F(\theta)$. 下面我们构造一个 E 中的元素, 它不在 F 中, 但它的 p 次幂在 F 中.

考察下述 p 个 Lagrange 预解式

$$\begin{cases} \xi_0 = \theta + \sigma(\theta) + \sigma^2(\theta) + \cdots + \sigma^{p-1}(\theta), \\ \qquad\qquad \cdots\cdots\cdots\cdots \\ \xi_i = \theta + \zeta_p^i\sigma(\theta) + \zeta_p^{2i}\sigma^2(\theta) + \cdots + \zeta_p^{(p-1)i}\sigma^{p-1}(\theta), \\ \qquad\qquad \cdots\cdots\cdots\cdots \\ \xi_{p-1} = \theta + \zeta_p^{p-1}\sigma(\theta) + \zeta_p^{2(p-1)}\sigma^2(\theta) + \cdots + \zeta_p^{(p-1)^2}\sigma^{p-1}(\theta), \end{cases}$$

记 $\underline{\xi}=(\xi_0,\xi_1,\cdots,\xi_{p-1})^{\mathrm{T}}$, $\underline{\theta}=(\theta,\sigma(\theta),\cdots,\sigma^{p-1}(\theta))^{\mathrm{T}}$, $A=(a_{ij})_{p\times p}$, 其中 $a_{ij}=\zeta_p^{(i-1)(j-1)}$, 则显然矩阵 A 可逆, 且有

$$\underline{\xi}=A\underline{\theta}.$$

下面证明存在某个 i 使得 $\xi_i\notin F$. 事实上若否, 则 $\underline{\xi}$ 是域 F 上的列向量. 由于 A 为域 F 上的可逆矩阵, 自然 A^{-1} 也是域 F 上的矩阵, 从而 $\underline{\theta}=A^{-1}\underline{\xi}$ 是域 F 上的列向量, 于是 $\theta\in F$, 得到矛盾. 最后, 注意到

$$\sigma(\xi_i)=\sigma(\theta)+\zeta_p^i\sigma^2(\theta)+\zeta_p^{2i}\sigma^3(\theta)+\cdots+\zeta_p^{(p-1)i}\sigma^p(\theta)=\zeta_p^{-i}\xi_i,$$

所以

$$\sigma(\xi_i^p)=\sigma(\xi_i)^p=\xi_i^p.$$

又 $\mathrm{Gal}(E/F)=\langle\sigma\rangle$, 故

$$\xi_i^p\in\mathrm{Inv}(\mathrm{Gal}(E/F))=F,$$

从而 $E=F(\xi_i)$ 是一个单根式扩张. □

定理 1.3.2 设 F 是特征为 0 的域, $f(x)\in F[x]$. 如果 $f(x)$ 在 F 上的 Galois 群 G_f 可解, 那么方程 $f(x)=0$ 在 F 上根式可解.

证明 设 K 是 $f(x)$ 在 F 上的分裂域, 且 $G=\mathrm{Gal}(K/F)\cong G_f$ 是一个可解群, 则只需证明存在 F 的根式扩张 E 使得 $K\subseteq E$.

设 $[K:F]=n$, $m=\mathrm{rad}(n)$ 为 n 的所有互不相同的素因子的乘积. 令 ζ_m 是一个 m 次本原单位根, 则 $L=F(\zeta_m)$ 是 x^m-1 在 F 上的分裂域, 由例 1.3.1 知 L/F 是单根式扩张. 令 E 是 $f(x)$ 在 L 上的分裂域, 则 $K\subseteq E$, 且由命题 1.1.2 得到 $H=\mathrm{Gal}(E/L)$ 同构于 $G=\mathrm{Gal}(K/F)$ 的一个子群, 于是 H 也是可解群. 因为 H 有限, 由《代数学(三)》中定理 3.5.1 知存在次正规群列

$$H=H_0\trianglerighteq H_1\trianglerighteq H_2\trianglerighteq\cdots\trianglerighteq H_s=\{e\},\tag{1.13}$$

使得对于每个 $1\leqslant i\leqslant s$, 因子群 H_{i-1}/H_i 都是素数阶循环群. 记 $L_j=\mathrm{Inv}(H_j)$, $0\leqslant j\leqslant s$. 根据 Galois 基本定理, 存在 L 到 E 的扩张链

$$L=L_0\subseteq L_1\subseteq L_2\subseteq\cdots\subseteq L_s=E,\tag{1.14}$$

使得对于每个 $1\leqslant i\leqslant s$, L_i/L_{i-1} 为 Galois 扩张且

$$\mathrm{Gal}(L_i/L_{i-1})\cong H_{i-1}/H_i.$$

记 $|H_{i-1}/H_i|=p_i$, p_i 为素数, 由于

$$p_i=[L_i:L_{i-1}]\mid[E:L]=|\mathrm{Gal}(E/L)|\mid|\mathrm{Gal}(K/F)|=n,$$

故 $p_i \mid m$. 从而 p_i 次本原单位根

$$\zeta_m^{\frac{m}{p_i}} \in L \subseteq L_{i-1},$$

由命题 1.3.1 可知, L_i 是 L_{i-1} 的单根式扩张. 这样我们得到从 F 到 E 的根式扩张链

$$F \subseteq L = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_s = E,$$

故 E 是 F 的根式扩张且 $f(x)$ 在 F 上的分裂域 $K \subseteq E$, 所以 $f(x) = 0$ 在 F 上根式可解. □

由于对称群 S_4 是可解群, 由定理 1.3.2 可立得如下推论.

推论 1.3.1　设 F 是特征为 0 的域, $f(x) \in F[x]$. 如果 $\deg f(x) \leqslant 4$, 那么方程 $f(x) = 0$ 在 F 上根式可解.

注意到定理 1.3.2 的结论对特征为素数的域不一定成立, 参见本节习题第 7 题.

习题 1.3

1. 设 $f(x)$ 是域 F 上的不可约多项式, 证明若 $f(x)$ 的一个根在 F 的一个根式扩张中, 则 $f(x)$ 的所有根也在 F 的某个根式扩张中.

2. 设 $f(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$, β 是 $f(x)$ 的一个根.

(i) 证明 $\mathbb{Q}(\beta)$ 是 $\mathbb{Q}$ 的 3 次 Galois 扩张;

(ii) 令 $\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{3}}$, 证明 $\mathbb{Q}(\omega, \beta)$ 是 $\mathbb{Q}(\omega)$ 的 3 次 Galois 扩张;

(iii) 由命题 1.3.1 知存在 $\alpha \in \mathbb{Q}(\omega, \beta)$ 使得

$$\mathbb{Q}(\omega, \beta) = \mathbb{Q}(\omega, \alpha)$$

且 $\alpha^3 \in \mathbb{Q}(\omega)$, 给出一个这样的元素 α.

3. 设 n 为正整数, F 是特征为素数 p 的域, 证明 F 的某个扩域中存在 n 次本原单位根当且仅当 $p \nmid n$.

4. 判断下面有理数域 $\mathbb{Q}$ 上的多项式是否根式可解:

(i) $2x^5 - 5x^4 + 5$;

(ii) $x^6 + 2x^3 + 1$;

(iii) $3x^5 - 15x + 5$.

5. 给出一个 $\mathbb{Q}$ 上的 7 次多项式使得其 Galois 群为 S_7.

6. 设 $f(x)$ 是 $\mathbb{Q}$ 上的 3 次不可约多项式, 它的分裂域 K 是 $\mathbb{Q}$ 的 3 次扩张, 证明 $f(x)$ 根式可解, 但是 K 并不是根式扩张链的最大的域. 给出满足如上条件的多项式 $f(x)$ 的例子.

7. 设 p 为素数, $F = \mathbb{F}_p(t)$, $f(x) = x^p - x - t \in F[x]$, 证明 $f(x)$ 在 F 上根式不可解.

8. 能否在 $\mathbb{Q}$ 上根式求解 5 次方程 $x^5 - 6x + 3 = 0$?

1.4 尺规作图

在域论部分的最后一节, 我们来讨论如何用域论来解决欧氏几何中的几何作图问题. 欧氏几何中几何作图的工具是没有刻度的直尺和圆规, 在中学的平面几何中我们知道如何作出一条给定线段的垂直平分线, 如何作一个给定角的角平分线, 我们还可以作出正三角形、正五边形等图形. 早在古希腊时期, 当时希腊人提出了三个著名的问题, 后来被称为三大几何作图难题. 它们分别是

(i) 化圆为方: 给定一个圆, 作一个面积与它相等的正方形;

(ii) 三等分角: 给定任意一个角, 作两条线三等分这个角;

(iii) 立方倍积: 给定一个正方体, 作体积为这个立方体体积两倍的立方体.

这三个作图问题有着悠久的历史, 吸引了很多著名数学家去研究解决, 但直到问题提出 2000 多年之后的 19 世纪应用了代数的工具才最终得以解决.

正如三大几何作图难题那样, 几何作图就是在已知的一些几何图形 (如点、直线、角、圆等) 的基础上作出新的图形. 但是一条直线由它上面的两个不同的点确定, 一个角由其顶点和每边上取一个点共三点确定, 一个圆由其圆心和圆周上的一点确定, 所以几何作图问题的前提总可以归结为给定了平面上的有限个点. 设 S 是欧氏平面 $\mathbb{R}^2$ 上给定的一个有限子集, $|S| \geqslant 2$, 则通过 S 可以作出什么样的图形? 这取决于作图的法则. 因为欧氏几何作图的工具是没有刻度的直尺和圆规, 所以用直尺只能去作经过 S 中给定两点的直线; 而圆规的两个端点可以放在 S 中的任意两个点上, 故利用圆规只能作以 S 中某一点为圆心并经过 S 中另外一点的圆. 再在这样作出的直线与直线、直线与圆、圆与圆相交得到的新的点集和 S 的并集上用直尺和圆规施行同样的操作, 然后再如此反复有限次作出新的图形. 这样法则的作图称为**尺规作图**, 为简单起见, 就称其为**作图**.

经过 S 中任意不同两点的直线称为 **S-直线**, 以 S 中某一点为圆心并经过 S 中另外一点的圆称为 **S-圆**. 对于 $\mathbb{R}^2$ 上的点 P, 若 $P \in S$, 或者 P 为两条 S-直线、两个 S-圆、或一条 S-直线和一个 S-圆的交点, 则称点 P **可用尺规至多一步从 S 作出**. 用 S_1 表示可用尺规至多一步从 S 作出的点的集合, 则 S_1 是 $\mathbb{R}^2$ 的有限子集且 $S_1 \supseteq S$. 对 S_1 进行同样的操作, 若 $\mathbb{R}^2$ 上的点可用尺规至多一步从 S_1 作出, 则称其可用尺规至多两步从 S 作出. 用 S_2 表示可用尺规至多两步从 S 作出的点的集合, 则 S_2 仍为 $\mathbb{R}^2$ 的有限子集且 $S_2 \supseteq S_1 \supseteq S$. 继续下去, 得到可用尺规至多三步从 S 作出的点的集合. 以此类推, 我们给出如下定义.

定义 1.4.1 设 S 是欧氏平面 $\mathbb{R}^2$ 的一个有限子集且 $|S| \geqslant 2$, 若 $\mathbb{R}^2$ 中的点 Q 可

用尺规至多有限步从 S 作出, 则称 Q **可用尺规从** S **作出**, 简称为**可作出点**. 经过两个可作出点的直线称为**可作出直线**, 以可作出点为圆心并经过另一个可作出点的圆称为**可作出圆**.

下面的点或直线是可作出的.

(a) 一条线段的中点和垂直平分线.

设 PQ 是一条给定的线段, 其两个端点 P 和 Q 是可作出点, 则 PQ 的中点是可作出点, PQ 的垂直平分线 (即与 PQ 垂直且平分 PQ 的直线) 是可作出直线. 事实上, 以 P 为圆心经过点 Q 的圆与以 Q 为圆心经过点 P 的圆有两个交点 R 和 S. R 和 S 都是可作出点, 过 R 和 S 的直线就是 PQ 的垂直平分线, 故为可作出直线. 直线 RS 与 PQ 的交点 T 是 PQ 的中点, 是可作出点 (图 1.1).

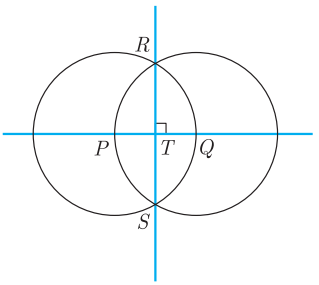


图 1.1

(b) 过直线外一点与该直线垂直的直线.

设 ℓ 是一条给定的直线, P 是 ℓ 外的一个给定点, 即 ℓ 是可作出直线, P 为可作出点. 因为 ℓ 可作出, 所以 ℓ 上有至少两个可作出点, 设 Q 是其中之一. 以 P 为圆心经过点 Q 的圆是可作出圆, 若该圆与 ℓ 只有一个交点 Q, 则直线 PQ 就是经过点 P 且与 ℓ 垂直的直线, 它显然是可作出的. 若此圆与 ℓ 有两个交点, 记除 Q 外的另一个交点为 R, 则 R 为可作出点. 由前面的 (a) 知线段 QR 的垂直平分线可作出, 而 QR 的垂直平分线就是经过点 P 且与 ℓ 垂直的直线 (图 1.2).

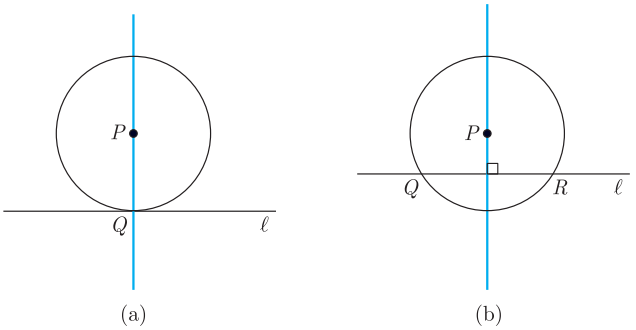


图 1.2

(c) 过直线上一点与该直线垂直的直线.

设 ℓ 是一条给定的直线, P 是 ℓ 上的一个给定点. 同样地, 由于 ℓ 可作出, 除可作出点 P 外, ℓ 上还至少有另一个可作出点 Q. 以 P 为圆心经过点 Q 的圆是可作出圆, 它与 ℓ 的另一个交点为 R, R 是可作出点. 由前面的 (a) 知线段 QR 的垂直平分线可作出, 而 QR 的垂直平分线就是经过点 P 且与 ℓ 垂直的直线 (图 1.3).

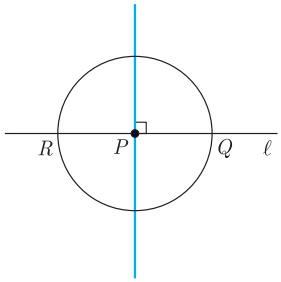


图 1.3

(d) 过直线外一点与该直线平行的直线.

设 ℓ 是一条给定的直线, P 是 ℓ 外的一个给定点. 由 (b) 知过点 P 且与 ℓ 垂直的直线 m 是可作出直线, 又由 (c) 知过点 P 且与 m 垂直的直线 n 是可作出直线. 显然 n 就是过点 P 且与 ℓ 平行的直线 (图 1.4).

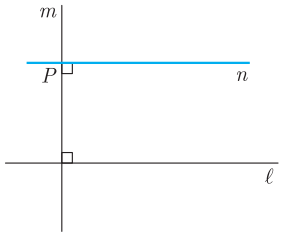


图 1.4

尺规作图中圆规的用法是以可作出点 (设为 P) 为圆心并且经过另一个可作出点 (设为 Q) 作圆, 这也是以 P 为圆心、以可作出点 P 与 Q 之间的距离 $|PQ|$ 为半径的圆. 实际上, 圆规的用法可以进一步扩充, 以可作出点为圆心、以任意两个可作出点之间的距离为半径的圆也是可以尺规作出的. 即设 P, Q, R 是三个可作出点, 则可以作出以 R 为圆心、以 P, Q 之间的距离 $|PQ|$ 为半径的圆. 事实上, 经过点 P 和 R 作直线 ℓ, 以 P 为圆心经过 Q 作圆 O_P, 过点 P 作与 ℓ 垂直的直线 m, 设 m 与圆 O_P 的交点为 S (S 可以为 Q), 过 S 作与 ℓ 平行的直线 n, 过点 R 作与 ℓ 垂直的直线 k, 设 k 与 n 的交点为 T, 则 T 为可作出点且 $|RT| = |PQ|$. 以 R 为圆心经过点 T 的圆 O_R 是可作出圆, 显然 O_R 是以 R 为圆心、以可作出点 P, Q 之间的距离 $|PQ|$ 为半径的圆 (图 1.5).

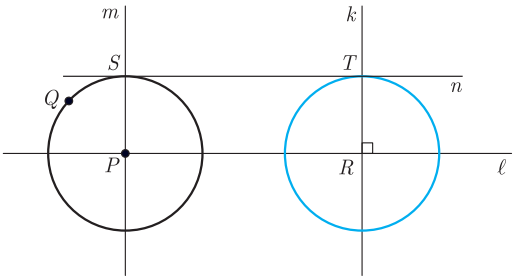


图 1.5

为解决包括前面提到的三大几何作图难题的作图问题, 我们先把上述几何作图问题转化为代数问题, 由此需要用平面直角坐标系. 作图问题的开始, 已知有平面上的有限点集 S, S 中至少有两个点, 即作图时已经有至少两个可作出点, 分别把它们取作坐标原点 $O=(0,0)$ 和单位点 $P=(1,0)$, 而经过这两点的可作出直线就是 x 轴, 方向为从左到右. 过原点 O 作 x 轴的垂线 p, 以原点 O 为圆心过点 P 作圆与直线 p 交于 x 轴上方的点 Q. 直线 p 从下向上的方向就是 y 轴, 而点 Q 就是 y 轴上的单位点 $(0,1)$, 这样我们便作出了平面直角坐标系 (图 1.6).

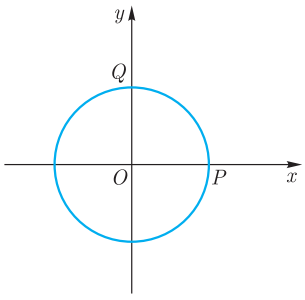


图 1.6

把欧氏平面 $\mathbb{R}^2$ 等同于复平面 $\mathbb{C}$, 即把 $\mathbb{R}^2$ 上的点 (a,b) 等同于复数 $a+b\mathrm{i}$, 其中 $a,b\in\mathbb{R}$. 下面就把点 (a,b) 记为复数 $a+b\mathrm{i}$.

定义 1.4.2　设 $z=a+b\mathrm{i}\in\mathbb{C}$, 称 z 是**可作出**的, 若其对应的点 (a,b) 是可作出点.

由定义可知, 如果 a 为实数, 则 a 是可作出的若 x 轴上的点 $(a,0)$ 是可作出点, 从而实数 0 和 1 是可作出的. 若两个可作出点之间的距离为 d, 则以原点 O 为圆心、以 d 为半径的圆是可作出的, 该圆与 x 轴交于点 $(\pm d,0)$, 所以实数 d 是可作出的, 即两个可作出点之间的距离是可作出实数. 进一步, 若非零复数 z 可作出, 则以原点 O 为圆心过可作出点 z 的圆与经过 O 和 z 的直线交于另一可作出点 $-z$, 所以复数 $-z$ 也是可作出的, 即可作出复数集在取负下是封闭的.

设点 $z=(a,b)$ 是可作出的, 过 z 分别作 x 轴和 y 轴的垂线与 x 轴和 y 轴交于点 $(a,0)$ 和 $(0,b)$, 所以实数 a 可作出, 若 $b=0$, 则显然 b 可作出. 若 $b\neq 0$, 则以原点 O 为圆心过点 $(0,b)$ 的圆与 x 轴交于点 $(b,0)$ 和 $(-b,0)$, 所以实数 b 也是可作出的. 这表明

可作出点的横、纵坐标都是可作出实数. 反之, 设实数 a,b 是可作出的, 若 $b=0$, 由定义点 (a,b) 为可作出点; 若 $b\neq 0$, 则以 O 为圆心经过可作出点 $(b,0)$ 的圆与 y 轴交于点 $(0,b)$ 和 $(0,-b)$. 这样过可作出点 $(a,0)$ 且垂直于 x 轴的直线与过可作出点 $(0,b)$ 且垂直于 y 轴的直线交于点 (a,b), 从而点 (a,b) 是可作出的, 即横、纵坐标都是可作出实数的点为可作出点. 由此便证明了如下命题.

命题 1.4.1 设 $a,b\in\mathbb{R}$, $z=a+b\mathrm{i}\in\mathbb{C}$, 则 z 为可作出复数 (或点 (a,b) 为可作出点) 当且仅当 a 和 b 都是可作出实数.

用 E 来表示所有可作出复数构成的集合, 下面来讨论 E 的代数性质.

命题 1.4.2 E 是复数域 $\mathbb{C}$ 的子域.

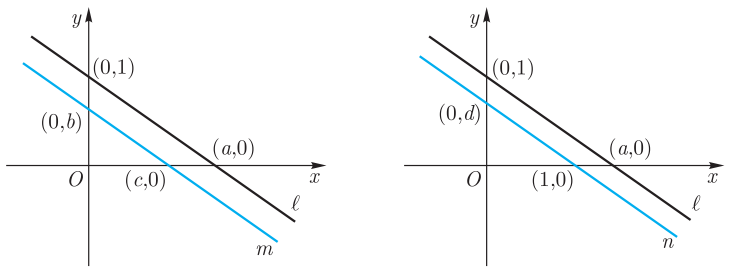
证明 显然 $0,1\in E$, 我们只需证明对任意 $z_1,z_2\in E$ 有 $z_1\pm z_2\in E$, $z_1z_2\in E$, 且若 $z_1\neq 0$, 有 $z_1^{-1}\in E$.

首先设 $z_1=a,z_2=b$ 均为实数, 由于 E 在取负下封闭, 不失一般性假设 $0<b\leqslant a$.

以点 $(a,0)$ 为圆心、以 b 为半径的圆与 x 轴交于点 $(a\pm b,0)$, 所以 $a\pm b\in E$. 下面证明 $ab\in E$ 和 $a^{-1}\in E$, 若 $a=1$ 或 $b=1$, 结论显然成立. 下面设 $a\neq 1$ 且 $b\neq 1$. 由于 $0,1,a,b\in E$, 故

$$(a,0),\ (0,b),\ (1,0),\ (0,1)$$

都是可作出点. 过 $(a,0)$ 和 $(0,1)$ 作直线 ℓ, 过点 $(0,b)$ 作直线 m 平行于直线 ℓ, 过点 $(1,0)$ 作直线 n 平行于 ℓ. 设 m 与 x 轴的交点坐标为 $(c,0)$, n 与 y 轴的交点坐标为 $(0,d)$, 这两个交点都是可作出点 (图 1.7). 由相似三角形性质可以得到 $ab=c\in E$ 和 $a^{-1}=d\in E$.



(a) (b)

图 1.7

设 $z_1=a_1+b_1\mathrm{i}$, $z_2=a_2+b_2\mathrm{i}$, 其中 $a_1,a_2,b_1,b_2\in\mathbb{R}$. 由于 $z_1,z_2\in E$, 由命题 1.4.1 知 $a_1,b_1,a_2,b_2\in E$, 所以由前面实数情形的证明有

$$a_1\pm a_2\in E,\quad b_1\pm b_2\in E,$$

再由命题 1.4.1 得到

$$z_1\pm z_2=(a_1\pm a_2)+(b_1\pm b_2)\mathrm{i}\in E.$$

进一步地,

$$z_1z_2=(a_1a_2-b_1b_2)+(a_1b_2+a_2b_1)\mathrm{i},$$

且当 $z_1\neq 0$ 时,

$$z_1^{-1}=\frac{a_1}{a_1^2+b_1^2}+\frac{-b_1}{a_1^2+b_1^2}\mathrm{i},$$

由此得到 $z_1z_2\in E$, 且当 $z_1\neq 0$ 时, $z_1^{-1}\in E$. □

由于 E 是 $\mathbb{C}$ 的子域, 故 E 包含有理数域 $\mathbb{Q}$, 从而每个有理数都是可作出的. 一个复数 z 的平方根有两个, 下面用 $\sqrt{z}$ 来表示 z 的一个平方根, 这样 z 的两个平方根可表示为 $\pm\sqrt{z}$.

命题 1.4.3　设复数 $z\in\mathbb{C}$, 若 $z\in E$, 则 $\sqrt{z}\in E$.

证明　显然只需考虑 $z\neq 0$ 的情形, 首先设 z 为正实数 a. 因为 $1,a\in E$, 由命题 1.4.2 有 $a+1\in E$. 设 O 为坐标原点 $(0,0)$, 点 P, Q 的坐标分别为 $(a,0)$ 和 $(a+1,0)$, 并设 R 为线段 OQ 的中点. 以 R 为圆心经过点 Q 作圆 O_R (O_R 自然也经过坐标原点 O), 过点 P 作 x 轴的垂线, 在第一象限内与圆 O_R 交于点 T, T 为可作出点 (图 1.8). 设 $|PT|=t$, 由勾股定理有

$$|OQ|^2=|OT|^2+|TQ|^2=|OP|^2+|PT|^2+|PT|^2+|PQ|^2,$$

即

$$(a+1)^2=a^2+t^2+t^2+1,$$

故 $a=t^2$, 从而 $\sqrt{a}=t$. 由于 t 为可作出点 P 和 T 之间的距离, 故 $t\in E$, 即 $\sqrt{a}\in E$.

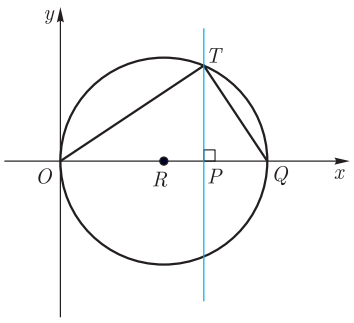


图 1.8

下面设 $z=r\mathrm{e}^{\mathrm{i}\theta}=r(\cos\theta+\mathrm{i}\sin\theta)$, 其中 $r>0$ 为复数 z 的模长. 由于 r 是点 z 与坐标原点 O 之间的距离, 故 $r\in E$. 进一步地, 由 $r\cos\theta,r\sin\theta,r\in E$ 和命题 1.4.2 可以得到 $\cos\theta,\sin\theta\in E$. 又

$$\sqrt{z}=\sqrt{r}\left(\cos\frac{\theta}{2}+\mathrm{i}\sin\frac{\theta}{2}\right),$$

由前面的证明知 $\sqrt{r}\in E$, 再由

$$\cos\frac{\theta}{2}=\pm\sqrt{\frac{1+\cos\theta}{2}},\quad \sin\frac{\theta}{2}=\pm\sqrt{\frac{1-\cos\theta}{2}}$$

和 $1\pm\cos\theta\geqslant 0$ 得到 $\cos\dfrac{\theta}{2},\sin\dfrac{\theta}{2}\in E$, 从而 $\sqrt{z}\in E$. □

注 1.4.1 由于 E 为 $\mathbb{Q}$ 的扩域, 显然 $3\in E$. 由命题 1.4.3 知 $\sqrt{3}\in E$, 再利用命题 1.4.3 可以得到实数

$$\sqrt{\sqrt{3}}=\sqrt[4]{3},\sqrt{\sqrt[4]{3}}=\sqrt[8]{3},\cdots,\sqrt[2^n]{3},\cdots$$

都在 E 中, 其中 n 为任意正整数, 由此得到

$$\bigcup_{n=1}^{\infty}\mathbb{Q}(\sqrt[2^n]{3})\subseteq E.$$

显然 $\sqrt[2^n]{3}$ 在 $\mathbb{Q}$ 上的极小多项式为 $x^{2^n}-3$, 故 $[\mathbb{Q}(\sqrt[2^n]{3}):\mathbb{Q}]=2^n$, 这表明 E 包含 $\mathbb{Q}$ 的次数任意大的扩域, 所以 E 作为 $\mathbb{Q}$ 的扩张是无限次的.

例 1.4.1 取单位圆上的点 1, ζ_5, ζ_5^2, ζ_5^3, ζ_5^4 为正五边形的顶点, 其中

$$\zeta_5=\mathrm{e}^{\mathrm{i}\frac{2\pi}{5}}=\cos\frac{2\pi}{5}+\mathrm{i}\sin\frac{2\pi}{5}.$$

由于 $\zeta_5^k=\zeta_5^{-(5-k)}$ 和

$$\zeta_5+\zeta_5^{-1}=2\cos\frac{2\pi}{5},$$

又 ζ_5 在 $\mathbb{Q}$ 上的极小多项式为分圆多项式

$$\Phi_5(x)=x^4+x^3+x^2+x+1,$$

我们有

$$\begin{aligned}0&=\zeta_5^4+\zeta_5^3+\zeta_5^2+\zeta_5+1\\&=(\zeta_5^2+\zeta_5^{-2})+(\zeta_5+\zeta_5^{-1})+1\\&=(\zeta_5+\zeta_5^{-1})^2+(\zeta_5+\zeta_5^{-1})-1\\&=4\cos^2\frac{2\pi}{5}+2\cos\frac{2\pi}{5}-1,\end{aligned}$$

由此得到

$$\cos\frac{2\pi}{5}=\frac{-1+\sqrt{5}}{4}\in E,$$

故 $\cos\dfrac{2\pi}{5}$ 为可作出实数. 再由

$$\sin\frac{2\pi}{5}=\sqrt{1-\cos^2\frac{2\pi}{5}}$$

知 $\sin\dfrac{2\pi}{5}$ 也是可作出实数, 从而点 ζ_5 是可作出的.

作以原点为圆心、1 为半径的圆 O_0, 这就是单位圆, 可作出点 ζ_5 也在此圆上. 以点 ζ_5 为圆心经过点 1 (即点 $(1,0)$) 的圆交 O_0 于另一点 ζ_5^2, 以点 ζ_5^2 为圆心经过点 ζ_5 的圆交 O_0 于另一点 ζ_5^3, 类似地可作出点 ζ_5^4, 所以正五边形的 5 个顶点 $1,\zeta_5,\zeta_5^2,\zeta_5^3,\zeta_5^4$ 都是可作出点, 从而可尺规作出正五边形 (图 1.9).

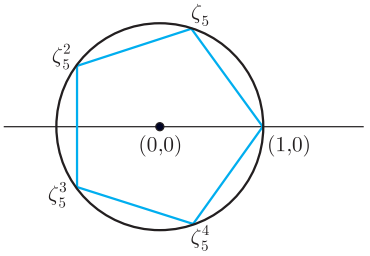


图 1.9

设 K 为实数域 $\mathbb{R}$ 的一个子域, 由中学的解析几何容易给出 K^2-直线和 K^2-圆的方程形式. 设点 $(a_1,b_1),(a_2,b_2)\in K^2$, 则过这两点的方程为

$$(y-b_1)(a_2-a_1)=(x-a_1)(b_2-b_1),$$

该方程可以化简为形式

$$ax+by+c=0,$$

其中

$$a=b_2-b_1,\ b=a_1-a_2,\ c=b_1(a_2-a_1)-a_1(b_2-b_1).$$

显然 $a,b,c\in K$, 故每条 K^2-直线的方程都可以写成

$$ax+by+c=0$$

的形式, 其中 $a,b,c\in K$. 类似地, 以点 (a_1,b_1) 为圆心经过点 (a_2,b_2) 的圆的方程为

$$(x-a_1)^2+(y-b_1)^2=(a_2-a_1)^2+(b_2-b_1)^2,$$

它可以化简为

$$x^2+y^2+dx+ey+f=0,$$

其中 $d,e,f\in K$, 这是任意 K^2-圆的方程形式.

命题 1.4.4 设 K 为实数域 $\mathbb{R}$ 的一个子域, 则两条 K^2-直线的交点坐标依然在域 K 中, 而一条 K^2-直线和一个 K^2-圆的交点以及两个 K^2-圆的交点坐标或在 K 中或在 K 的某个 2 次扩张中.

证明 (i) 设所给两条 K^2-直线的方程分别为

$$ax + by + c = 0$$

和

$$a'x + b'y + c' = 0,$$

其中 $a, b, c, a', b', c' \in K$, 这两条直线的交点坐标就是方程组

$$\begin{cases} ax + by + c = 0, \\ a'x + b'y + c' = 0 \end{cases} \tag{1.15}$$

的解. 因为这两条直线有交点, 所以有 $ab' - a'b \neq 0$, 容易得到该二元一次方程组的解为

$$x = \frac{bc' - b'c}{ab' - a'b}, \quad y = \frac{a'c - ac'}{ab' - a'b},$$

它们是由 K 中的元素作加、减、乘、除 (除数不为 0) 运算得到的, 故依然在域 K 中.

(ii) 设所给 K^2-直线和 K^2-圆的方程分别为

$$ax + by + c = 0$$

和

$$x^2 + y^2 + dx + ey + f = 0,$$

其中 a, b, c, d, e, $f \in K$ 且 a, b 不全为 0. 要求它们的交点坐标, 需要解方程组

$$\begin{cases} ax + by + c = 0, \\ x^2 + y^2 + dx + ey + f = 0. \end{cases} \tag{1.16}$$

不妨设 $b \neq 0$, 则由方程组 (1.16) 的第一个方程得到

$$y = -\frac{a}{b}x - \frac{c}{b},$$

代入 (1.16) 的第二个方程并化简得

$$Ax^2 + Bx + C = 0, \tag{1.17}$$

其中

$$A = a^2 + b^2,\ B = 2ac + b^2 d - abe,\ C = c^2 - bce + b^2 f.$$

显然 $A, B, C \in K$ 且一元二次方程 (1.17) 的解为 $x = s \pm q\sqrt{t}$, 其中

$$s = -\frac{B}{2A},\ q = \frac{1}{2A},\ t = B^2 - 4AC.$$

将 $x = s \pm q\sqrt{t}$ 代入 (1.16) 的第一个方程可求出 $y = s' \pm q'\sqrt{t}$, 其中 $s', q' \in K$. 由于 $s, s', q, q', t \in K$, 故当 $\sqrt{t} \in K$ 时, 交点坐标在域 K 中, 而当 $\sqrt{t} \notin K$ 时, 交点坐标在 K 的 2 次扩张 $K(\sqrt{t})$ 中.

(iii) 设所给两个 K^2-圆的方程分别为

$$x^2 + y^2 + dx + ey + f = 0$$

和

$$x^2 + y^2 + d'x + e'y + f' = 0,$$

其中 $d, e, f, d', e', f' \in K$. 它们的交点坐标是方程组

$$\begin{cases} x^2 + y^2 + dx + ey + f = 0, \\ x^2 + y^2 + d'x + e'y + f' = 0 \end{cases} \tag{1.18}$$

的解. 方程组 (1.18) 中两个方程相减得到一次方程

$$(d - d')x + (e - e')y + (f - f') = 0.$$

从而方程组 (1.18) 与方程组

$$\begin{cases} x^2 + y^2 + dx + ey + f = 0, \\ (d - d')x + (e - e')y + (f - f') = 0 \end{cases} \tag{1.19}$$

同解. 类似于前面 (ii) 的讨论, 方程组 (1.19) 的解或在 K 中或在 K 的某个 2 次扩张中, 这表明两个 K^2-圆的交点坐标或在 K 中或在 K 的某个 2 次扩张中. □

有了这些准备, 我们就可以刻画可作出数了. 可作出数显然与作图开始给定的点集 S 有关, 设 S 中除坐标原点 $0 = (0,0)$ 和 x 轴上单位点 $1 = (1,0)$ 外还有 n 个点 $z_1, z_2, \cdots, z_n$, 其中 $n \geqslant 0$. 显然, 任意有理数都可以通过 $0, 1$ 做有限次四则运算得到. 对于 $1 \leqslant k \leqslant n$, 设

$$z_k = a_k + b_k\mathrm{i},$$

由于 z_k 是给定的, 当然是可作出的, 从而 a_k, b_k 都是可作出的, 所以 z_k 的共轭 $\overline{z_k} = a_k - b_k\mathrm{i}$ 也是可作出数. 令

$$F = \mathbb{Q}(z_1, z_2, \cdots, z_n, \overline{z_1}, \overline{z_2}, \cdots, \overline{z_n}),$$

则 F 中的每个数都是可作出的, 域 F 为作图开始时给定的点集 S 对应的域, 也就是该作图问题已知条件给出的域. 设 $F_0 = F(\mathrm{i})$, 则 F_0 中的每个数也都是可作出的且有 $[F_0 : F] = 1$ 或者 2. 记

$$F_{\mathbb{R}} = \mathbb{Q}(a_1, a_2, \cdots, a_n, b_1, b_2, \cdots, b_n),$$

则 $F_{\mathbb{R}}$ 是实数域 $\mathbb{R}$ 的子域, 且有 $F_0 = F_{\mathbb{R}}(\mathrm{i})$. 下面的讨论中, 作图问题给定的域都设为 F 且 $F_0 = F(\mathrm{i})$.

定理 1.4.1 *复数 z 为可作出数当且仅当存在 F 的一个根式扩张 L/F 使得 $z \in L$, 并且从 F 到 L 有一个根式扩张链*

$$F \subseteq F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r = L \tag{1.20}$$

满足对任意 $1 \leqslant j \leqslant r$, 有 $[F_j : F_{j-1}] = 2$.

证明 充分性: 在根式扩张链 (1.20) 中, F_0 中的数都是可作出的. 由于 $[F_1 : F_0] = 2$, 取 $\alpha \in F_1 \backslash F_0$, 则有 $F_1 = F_0(\alpha)$. 设 α 在 F_0 上的极小多项式为

$$g(x) = x^2 + bx + c \in F_0[x],$$

则有

$$\left(\alpha + \frac{b}{2}\right)^2 = \frac{b^2 - 4c}{4}.$$

令

$$d = \frac{b^2 - 4c}{4},$$

则有 $d \in F_0$ 且

$$\sqrt{d} = \alpha + \frac{b}{2} \in F_1,$$

从而

$$F_1 = F_0(\alpha) = F_0(\sqrt{d}).$$

由于 $d \in F_0$ 可作出, 由命题 1.4.3 知 $\sqrt{d}$ 可作出, 再利用命题 1.4.2 得到 F_1 中的数均可作出. 以此类推, 对 r 做归纳可以得到 L 中的数可作出, 由 $z \in L$ 知 z 可作出.

必要性: 设 z 可作出, 若 $z = a + b\mathrm{i}$ 可用尺规至多一步从 S 作出, 其中 $a, b \in \mathbb{R}$. 在命题 1.4.4 中令 $K = F_{\mathbb{R}}$, 则得到 $a, b \in F_{\mathbb{R}}$ 或 $a, b \in F_{\mathbb{R}}(\sqrt{t})$, 其中 $t \in F_{\mathbb{R}}$ 但是 $\sqrt{t} \notin F_{\mathbb{R}}$. 从而 $z \in F_{\mathbb{R}}(\mathrm{i}) = F_0$ 或者

$$z \in F_{\mathbb{R}}(\sqrt{t})(\mathrm{i}) = F_0(\sqrt{t}).$$

在后一种情形中取 $F_1 = F_0(\sqrt{t})$, 则 $[F_1 : F_0] = 2$ 且 $z \in F_1$.

如果 z 不能用尺规至多一步从 S 作出, 则 z 是经过有限步尺规作图从 S 作出的, 而这只是添加了一些中间步骤. 对步数做归纳可以证明从 F_0 出发, 存在有限步 2 次扩张

$$F_1 = F_0(w_1),\ F_2 = F_1(w_2),\ \cdots,\ F_r = F_{r-1}(w_r)$$

使得 $z \in F_r$, 且 $[F_j : F_{j-1}] = 2,\ 2 \leqslant j \leqslant r$. 于是有从 F 到 F_r 的一个根式扩张链

$$F \subseteq F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r$$

使得 $z \in F_r$, 且 $[F_j : F_{j-1}] = 2,\ 1 \leqslant j \leqslant r$. □

推论 1.4.1　*设 z 为可作出数, 则 z 是域 F 上的代数元, 且 z 在 F 上的极小多项式的次数为 2 的幂.*

证明　设 z 为可作出数, 则由定理 1.4.1 知存在根式扩张链 (1.20) 使得 $z \in F_r$, 故 $F(z)$ 为 F_r 的子域. 由于

$$[F_r : F(z)][F(z) : F] = [F_r : F] = \left(\prod_{j=1}^{r} [F_j : F_{j-1}]\right) [F_0 : F] = 2^s,$$

其中 $s = r$ 或者 $r+1$, 故 $[F(z) : F] \mid 2^s$. 所以 $[F(z) : F] = 2^t$, 其中 $t \leqslant s$, 从而 z 是域 F 上的代数元, 且 z 在 F 上的极小多项式的次数为 2^t. □

例 1.4.2　在化圆为方问题中, 设已知圆的圆心在原点, 经过 x 轴上单位点 $(1, 0)$, 即该问题给定的已知点只有 0 和 1, 这时域 $F = \mathbb{Q}$. 所要作的正方形面积等于给定圆的面积 π, 故边长为 $\sqrt{\pi}$, 所以化圆为方问题需要作的数为 $\sqrt{\pi}$. 德国数学家 Lindemann (林德曼) 于 1882 年证明了 π 不是 $\mathbb{Q}$ 上的代数元, 所以 $\sqrt{\pi}$ 不可作出, 否则 $\pi = \sqrt{\pi}^2$ 可作出, 与推论 1.4.1 矛盾, 从而化圆为方问题不可解.

三等分角问题要求三等分任意角, 即给定一个角 θ, 用尺规作出一个角 ψ 使得 $\theta = 3\psi$. 将角 θ 放在一个单位圆内, 使得角的顶点与圆心重合, 角的一边与 x 轴正向重合, 则角 θ 的另一边与此单位圆的交点为

$$\mathrm{e}^{\mathrm{i}\theta} = \cos\theta + \mathrm{i}\sin\theta,$$

故三等分角问题给定的已知点是 0, 1 和 $\mathrm{e}^{\mathrm{i}\theta}$, 从而域

$$F = \mathbb{Q}(\mathrm{e}^{\mathrm{i}\theta}, \mathrm{e}^{-\mathrm{i}\theta}),$$

而问题要求尺规作出的复数为 $\mathrm{e}^{\mathrm{i}\psi}$, 其中 $\theta = 3\psi$. 特别地, 设 $\theta = \dfrac{\pi}{3}$, 则

$$\mathrm{e}^{\mathrm{i}\theta} = \frac{1}{2} + \frac{\sqrt{-3}}{2},$$

从而 $F=\mathbb{Q}(\sqrt{-3})$. 要作出的是 $\psi=\dfrac{\pi}{9}$, 由

$$\cos\theta=\cos 3\psi=4\cos^3\psi-3\cos\psi$$

和 $\cos\theta=\dfrac{1}{2}$ 得到 $\cos\dfrac{\pi}{9}$ 是多项式

$$f(x)=x^3-\frac{3}{4}x-\frac{1}{8}$$

的根. 易知 $f(x)$ 无有理根, 所以 $f(x)$ 在有理数域 $\mathbb{Q}$ 上不可约, 故 $\cos\dfrac{\pi}{9}$ 在 $\mathbb{Q}$ 上的极小多项式是 $f(x)$, 次数为 3, 所以

$$\left[\mathbb{Q}\left(\cos\frac{\pi}{9}\right):\mathbb{Q}\right]=3.$$

进一步地, x^2+3 在实数域 $\mathbb{R}$ 上不可约, 自然在 $\mathbb{R}$ 的子域 $\mathbb{Q}\left(\cos\dfrac{\pi}{9}\right)$ 上不可约, 由此得

$$\left[\mathbb{Q}\left(\cos\frac{\pi}{9},\sqrt{-3}\right):\mathbb{Q}\left(\cos\frac{\pi}{9}\right)\right]=2.$$

从而

$$\left[\mathbb{Q}\left(\cos\frac{\pi}{9},\sqrt{-3}\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\cos\frac{\pi}{9},\sqrt{-3}\right):\mathbb{Q}\left(\cos\frac{\pi}{9}\right)\right]\left[\mathbb{Q}\left(\cos\frac{\pi}{9}\right):\mathbb{Q}\right]=6.$$

由此得

$$\left[F\left(\cos\frac{\pi}{9}\right):F\right]=\left[\mathbb{Q}\left(\cos\frac{\pi}{9},\sqrt{-3}\right):\mathbb{Q}\right]/[F:\mathbb{Q}]=3$$

不是 2 的幂, 由推论 1.4.1 得 $\cos\dfrac{\pi}{9}$ 不可作出, 从而角 $\dfrac{\pi}{9}$ 不能尺规作出, 这表明我们不能三等分角 $\dfrac{\pi}{3}$, 故三等分任意角是不可能的.

在立方倍积问题中设已知立方体的棱长为 1, 即该问题给定的已知点也只有 0 和 1, 所以域 $F=\mathbb{Q}$. 所要作的立方体体积为 2, 故棱长为 $\sqrt[3]{2}$, 即立方倍积问题需要作出的数为 $\sqrt[3]{2}$. 显然 $\sqrt[3]{2}$ 在 $\mathbb{Q}$ 上的极小多项式为 x^3-2, 次数不是 2 的幂, 由推论 1.4.1 得实数 $\sqrt[3]{2}$ 不能作出, 所以立方倍积问题不可解.

注 1.4.2 古希腊的三大几何作图问题都是不可解的, 这并不是说还没有找到只用直尺和圆规把要求的图作出来的方法, 而是把它们作出的尺规作图方法根本就是不存在的. 注意到解决这三个问题的方法本质上是代数方法, 所以在代数还没有发展到相当程度时是不可能解决这三大几何作图问题的.

例 1.4.3 设

$$f(x)=x^4-4x+2\in\mathbb{Q}[x],$$

由 Eisenstein 判别法易知 $f(x)$ 在有理数域 $\mathbb{Q}$ 上不可约. 设 $f(x)$ 的四个根分别为 α_1, α_2, α_3 和 α_4, 则 $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ 在 $\mathbb{Q}$ 上的极小多项式都是 $f(x)$, 次数为 $4=2^2$. 令

$$\alpha=(\alpha_1+\alpha_2)(\alpha_3+\alpha_4),$$

$$\beta = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4),$$

$$\gamma = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3),$$

则以 α, β, γ 为根的多项式为

$$g(x) = x^3 - 8x + 16,$$

它就是多项式 $f(x)$ 的预解式. 容易验证 $g(x)$ 无有理根, 所以 $g(x)$ 在 $\mathbb{Q}$ 上不可约, 从而 α 在 $\mathbb{Q}$ 上的极小多项式就是 $g(x)$, 次数为 3. 由推论 1.4.1 得到 α 不能作出. 故 $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ 中必有一个不能在只给出 0 和 1 的基础上尺规作出, 否则 $\alpha = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$ 也可以作出. 这表明推论 1.4.1 的逆命题不成立.

例 1.4.3 表明极小多项式的次数为 2 的幂并不是可作出数的充要条件, 下面我们利用 Galois 理论给出可作出数的一个刻画, 其中域 F 仍为作图问题已知条件给出的域.

定理 1.4.2　*设 z 是一个复数, 则 z 为可作出数当且仅当存在 F 的一个 Galois 扩张 L' 使得 $z \in L'$, 并且 Galois 群 $\mathrm{Gal}(L'/F)$ 的阶为 2 的幂.*

证明　必要性: 由于 z 可作出, 由定理 1.4.1 知存在 F 的一个根式扩张 L/F 使得 $z \in L$, 并且从 F 到 L 有一个根式扩张链

$$F \subseteq F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r = L,$$

其中 $[F_j : F_{j-1}] = 2$, $1 \leqslant j \leqslant r$. 设 L' 为扩张 L/F 的正规闭包, 由引理 1.3.1 的证明知存在连接形如 (1.10) 的子链所成的根式扩张链, 并且 $[F(S_{i,j}) : F(S_{i,j-1})] = 1$ 或者 2, 将该链中重复的项去掉, 可得到根式扩张链

$$F \subseteq F_0 = F_0' \subseteq F_1' \subseteq \cdots \subseteq F_{m-1}' \subseteq F_m' = L', \tag{1.21}$$

且 $[F_i' : F_{i-1}'] = 2$, $1 \leqslant i \leqslant m$. 因为 2 次扩张一定为正规扩张, 由 Galois 基本定理, 根式扩张链 (1.21) 可给出次正规群列

$$\mathrm{Gal}(L'/F) \trianglerighteq \mathrm{Gal}(L'/F_0') \trianglerighteq \mathrm{Gal}(L'/F_1') \trianglerighteq \cdots \trianglerighteq \mathrm{Gal}(L'/F_{m-1}') \trianglerighteq \mathrm{Gal}(L'/F_m') = \{\mathrm{id}_{L'}\}.$$

由 $[\mathrm{Gal}(L'/F) : \mathrm{Gal}(L'/F_0')] = [F_0 : F] = 1$ 或者 2, 且

$$[\mathrm{Gal}(L'/F_{i-1}') : \mathrm{Gal}(L'/F_i')] = [F_i' : F_{i-1}'] = 2,\ 1 \leqslant i \leqslant m,$$

有 $|\mathrm{Gal}(L'/F)| = 2^m$ 或者 2^{m+1}.

充分性: 记 $G = \mathrm{Gal}(L'/F)$, 由于 $|G|$ 为 2 的幂, 记 $|G| = 2^s$. 由 Sylow 定理, G 有阶为 2^{s-1} 的子群 G_1, 且由于 $[G : G_1] = 2$, 有 $G_1 \trianglelefteq G$. 以此类推, 对 s 归纳便得到 G 的次正规群列

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_{s-1} \trianglerighteq G_s = \{e\},$$

其中 $[G_i : G_{i+1}] = 2$, $0 \leqslant i \leqslant s-1$. 记 $L_i = \mathrm{Inv}(G_i)$, $0 \leqslant i \leqslant s$, 根据 Galois 基本定理, 存在 L' 到 F 的扩张链

$$F = \mathrm{Inv}(G_0) = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_{s-1} \subseteq L_s = L'$$

使得对于每个 $0 \leqslant i \leqslant s-1$, $[L_{i+1} : L_i] = 2$. 令 $F_i = L_i(\mathrm{i})$, 我们有扩张链

$$F \subseteq F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{s-1} \subseteq F_s = L'(\mathrm{i}).$$

由于 $z \in L'$, 故 $z \in L'(\mathrm{i})$. 又显然对 $0 \leqslant i \leqslant s-1$, 有 $[F_{i+1} : F_i] \leqslant 2$, 由定理 1.4.1 得到 z 为可作出数. □

由于 Galois 扩张的次数等于对应的 Galois 群的阶, 由上面定理 1.4.2 立得如下推论.

推论 1.4.2 *设 z 是一个复数, 则 z 为可作出数当且仅当存在 F 的一个 Galois 扩张 L' 使得 $z \in L'$, 并且扩张次数 $[L' : F]$ 为 2 的幂.*

推论 1.4.3 *设 z 是一个复数, 则 z 为可作出数当且仅当 z 为 F 上的代数元, 并且 z 在 F 上的极小多项式在 F 上的分裂域 E' 对 F 的扩张次数 $[E' : F]$ 为 2 的幂.*

证明 由于 $z \in E'$, E' 是 F 上的 Galois 扩张, 又 $[E' : F]$ 为 2 的幂, 由推论 1.4.2 知 z 为可作出数.

反之, 设 z 为可作出数, 由推论 1.4.2 知存在 F 的一个 Galois 扩张 L' 使得 $z \in L'$, 并且存在某个 $s \geqslant 0$ 使得 $[L' : F] = 2^s$. 由于 $z \in L'$, 由 L' 的正规性得到 z 在 F 上的极小多项式的根都在 L' 中, 从而 $E' \subseteq L'$. 再由

$$2^s = [L' : F] = [L' : E'][E' : F]$$

知 $[E' : F]$ 为 2 的幂. □

同样地, 由于此时涉及的域的特征为 0, 故域 F 上多项式分裂域对 F 的扩张次数等于对应的 Galois 群的阶, 我们有如下推论.

推论 1.4.4 *设 z 是一个复数, 则 z 为可作出数当且仅当 z 为 F 上的代数元, 并且 z 在 F 上的极小多项式在 F 上的 Galois 群的阶为 2 的幂.*

例 1.4.4 依然设

$$f(x) = x^4 - 4x + 2 \in \mathbb{Q}[x],$$

它的四个复根为 $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, 例 1.4.3 中已经得到 $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ 不能都是可作出数. 由于 $f(x)$ 的预解式

$$g(x) = x^3 - 8x + 16$$

在 $\mathbb{Q}$ 上不可约, 又 $g(x)$ 的判别式 $D_g = -4864$ 不是 $\mathbb{Q}$ 中的平方数, 所以多项式 $f(x)$ 在 $\mathbb{Q}$ 上的 Galois 群为 S_4, 阶为 24. 由推论 1.4.4 知 $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ 都不是可作出数.

由例 1.4.1 知道可以尺规作出正五边形, 那么对于任意的正 n 边形又如何, 其中 $n \geqslant 3$ 为正整数? 同样类似于例 1.4.1, 我们仅仅已知 0 和 1, 即开始给定的域 $F = \mathbb{Q}$. 所求的正 n 边形的一个顶点落在单位圆上的点 1 处, 则正 n 边形的 n 个顶点为

$$1,\ \zeta_n,\ \zeta_n^2,\ \cdots,\ \zeta_n^{n-1},$$

其中 $\zeta_n = \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}}$, 所以能否作出正 n 边形就等价于能否作出复数 ζ_n. 由例 1.2.3 知 ζ_n 在 $\mathbb{Q}$ 上的极小多项式为分圆多项式 $\Phi_n(x)$, 而 $\Phi_n(x)$ 在 $\mathbb{Q}$ 上的分裂域为 $\mathbb{Q}(\zeta_n)$, 再由

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$$

可以立得如下定理.

定理 1.4.3　*设正整数 $n \geqslant 3$, $\phi(n)$ 为 n 的 Euler (欧拉) ϕ-函数值, 则可尺规作出正 n 边形当且仅当 $\phi(n)$ 为 2 的幂.*

设正整数 n 的素因子分解式为

$$n = 2^e p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m},$$

其中 $p_1, p_2, \cdots, p_m$ 是互不相同的奇素数, $e \geqslant 0$, $e_i \geqslant 1$, $1 \leqslant i \leqslant m$, 则有

$$\phi(n) = 2^{e-1} p_1^{e_1-1} p_2^{e_2-1} \cdots p_m^{e_m-1}(p_1 - 1)(p_2 - 1)\cdots(p_m - 1), \tag{1.22}$$

其中若 $e = 0$, 则认为式 (1.22) 中出现的 $2^{e-1} = 1$. 显然 $\phi(n)$ 为 2 的幂当且仅当

$$e_1 = e_2 = \cdots = e_m = 1,$$

且对每一个奇素数 p_i, 都存在正整数 t_i 使得 $p_i = 2^{t_i} + 1$. 又容易知道, 若形为 $2^t + 1$ 的数为素数, 则必有非负整数 h 使得 $t = 2^h$. 称形如

$$F_h = 2^{2^h} + 1$$

的素数为 **Fermat (费马) 素数**. 已知当 $0 \leqslant h \leqslant 4$ 时, F_h 确为素数, 分别为

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537,$$

但是

$$F_5 = 2^{32} + 1 = 4294967297 = 641 \times 6700417$$

不是素数. 由定理 1.4.3, 我们得到下面这个正 n 边形可尺规作出的充要条件.

推论 1.4.5　*设正整数 $n \geqslant 3$, 则可尺规作出正 n 边形当且仅当 n 形为*

$$n = 2^e p_1 p_2 \cdots p_m,$$

其中 $e \geqslant 0$, 而 $p_1, p_2, \cdots, p_m$ 为互不相同的 Fermat 素数.

注 1.4.3 可尺规作出正 n 边形等价于可作出 $\dfrac{2\pi}{n}$ 这个角, 从而三等分角问题不可解也可以作为推论 1.4.5 的一个推论. 由于尺规作不出正 9 边形, 我们就作不出角 $\dfrac{2\pi}{9}$, 也就不能把角 $\dfrac{2\pi}{3}$ 三等分.

推论 1.4.5 已经完美地解决了边数为多少的正多边形可尺规作出. 但这还涉及一个迄今仍未解决的问题, 即当自然数 h 为何值时, $F_h = 2^{2^h} + 1$ 为素数. 已经知道的是当 $0 \leqslant h \leqslant 4$ 时, F_h 是素数, 但除已知的这 5 个素数外, 还没有发现另外的 Fermat 素数. 现在可以确定的是对于 $5 \leqslant h \leqslant 13$, F_h 都不是素数.

一般认为, Gauss (高斯) 在他 19 岁时 (即 1796 年) 尺规作出了正 17 边形, 1801 年 Gauss 在专著 *Desquisitione Arithmeticae* 中证明了若 p 为 Fermat 素数, 则正 p 边形可尺规作出. 1832 年, Richelot (里歇洛) 在 *Journal für die Reine und Angewandte Mathematik* 上发表的论文给出了尺规作出正 257 边形的方法. 德国数学家 Hermes (赫密士) 花费了 10 年心血在 1894 年给出了正 65537 边形的尺规作图法, 其手稿装了一皮箱, 目前保管在 Göttingen (哥廷根) 大学.

习题 1.4

1. 证明可以尺规作出 3° 角.

2. 设 $\alpha \in \mathbb{C}$ 是可作出数, β 是 α 在 $\mathbb{Q}$ 上的极小多项式的另一个根, 证明 β 也是可作出数.

3. 判断下面有理数域 $\mathbb{Q}$ 上多项式的根能否在仅已知 0 和 1 的基础下尺规作出:

(i) $x^4 + 2x^2 + 4x + 2$;

(ii) $x^4 + 2x^2 + 2$;

(iii) $x^4 + 8x + 12$.

4. 求出 17 次本原单位根 ζ_{17} 并给出正 17 边形的尺规作法.

5. 设 p, q 为互素的正整数, 证明: 如果正 p 和正 q 边形可以尺规作出, 那么正 pq 边形也可以尺规作出.

6. 证明角 $\arccos \dfrac{6}{11}$ 不能用尺规三等分.