尺规作图的代数解析

Aug 2025

古希腊数学家在欧几里得几何学的框架下，提出了仅用**无刻度直尺**和**圆规**进行几何作图的一系列挑战。其中，三个问题因其表述简洁却又悬而未决而闻名于世，历经两千余年而无人能解：**倍立方问题**、**三等分任意角问题**以及化圆为方问题。与这些问题并列的，还有对任意**正多边形作图**可能性的探寻。这些古典问题构成了数学史上最持久的谜题之一，吸引了无数数学家和爱好者的尝试。

然而，这些问题的最终解决并非源于更精妙的几何技巧，而是来自于 Galois 理论对其进行了透彻的代数解析。这与方程的根式可解问题一样，成为了 Galois 理论最具代表性的应用。

1 可作图数的域结构

本节的任务是使用代数语言对可作图数进行刻画，这是使得尺规作图的几何问题转化为域论的代数语言。

1.1 几何作图的公理化

首先我们必须严格定义尺规作图的规则：

对于工具的使用有如下定义：

- **直尺**：一把没有刻度、无限长的理想化直尺，仅能用于连接两个已知点以作一条直线。
- **圆规**：一个可以张开至任意宽度且没有刻度的理想化圆规。其半径只能取自先前已作出的两点之间的距离，或一个任意的长度。

我们还有指定的作图公法：任何尺规作图过程都必须是有限步骤的，且每一步都必须是以下五种基本操作之一：

1. 通过两个已知点，作一条直线。
2. 以一个已知点为圆心，以两已知点间的距离为半径，作一个圆。
3. 确定两条已知直线（若不平行）的交点。
4. 确定一条已知直线与一个已知圆的交点（若相交）。

5. 确定两个已知圆的交点（若相交）。

一个几何对象（如点、线段长度）如果能从初始给定的两个点（通常定义了单位长度）出发，通过有限次上述基本操作得到，则称该对象是**可作图的**。

1.2 代数转译

为了方便分析，我们将问题置于解析几何的背景下，从两个初始点 $O(0,0)$ 和 $A(1,0)$ 开始，建立 Descartesz 坐标系。我们现在将五条作图公法翻译为代数语言，假设我们已经作出的点的坐标都包含在一个域 $F \subseteq \mathbb{R}$ 中。

- **作直线**：通过两点 (x_1, y_1) 和 (x_2, y_2) 的直线方程 $(y_2 - y_1)x - (x_2 - x_1)y + x_2y_1 - x_1y_2 = 0$。其中 $x_1, y_1, x_2, y_2 \in F$。该方程的所有解显然仍在域 F 中。
- **作圆**：以 (h, k) 为圆心 $(h, k \in F)$，半径 r（其中 $r^2 \in F$）的圆的方程为 $(x-h)^2+(y-k)^2 = r^2$。
- **求交点**：
  1. 两直线相交：求解一个系数在 F 中的二元一次方程组，其解必然仍在 F 中。
  2. 直线与圆相交：求解一个系数在 F 中的一元二次方程和一个一元一次方程构成的方程组，其交点坐标要么数域 F，要么数域 F 的一个二次扩张 $F(\sqrt{\delta})$，其中 $\delta \in F$ 且 $\delta > 0$。
  3. 两圆相交：求解两个二元二次方程组（实际上通过消元可以得到直线与圆相交一致的结构，其实就是圆与它们的根轴相交），其交点的坐标也与直线与圆相交一致。

这一转换揭示了一个同构关系：即 Euclid 几何中的工具限制域代数中的线性及二次方程求解能力完全对应。作图的每一步在代数上都对应着一个域扩张，且扩张的次数最多为 2。

1.3 可作图数的结构

于是我们可以定义可作图数的代数结构：

一个实数 α 称为可作图数当且仅当 $(\alpha, 0)$ 是一个可作图点。对于可作图数的全体有这样一个巧妙的定理：

可作图域
可作图数的集合，即为 $\mathcal{K}$，构成 $\mathbb{R}$ 的一个子域。

通过具体的几何作图很容易证明可作图数的加减乘除都是可作图的。

另外至关重要的是，如果一个正的可作图数 a 已知，那么其平方根 $\sqrt{a}$ 也是可作图的。

因此，可作图数域 $\mathcal{K}$ 是包含 $\mathbb{Q}$ 且在开平方根运算下封闭的最小的 $\mathbb{R}$ 的子域。这种结构为我们建立了一个清晰的数系层级：有理数域 $\mathbb{Q}$ 是基础，可作图数域 $\mathcal{K}$ 是代数数域 $\mathbb{A}$ 的一个可数无限子集，而代数数域又是实数域 $\mathbb{R}$ 的子集。即 $\mathbb{Q} \subseteq \mathcal{K} \subseteq \mathbb{A} \subseteq \mathbb{R}$。这个层级关系直接导出一个重要推论：任何超越数（非代数数）都不可能是可作图数，这一点将在化圆为方问题的讨论中起到决定性作用。

1.4 域塔定理与次数条件

我们将给出判断一个数是否可作图的代数判据：

域塔定理
一个数 α 是可作图的，当且仅当存在一个域塔

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n \tag{1}$$

使得 $\alpha \in F_n$，并且对于所有的 $i = 0, 1, \cdots, n-1$ 都有 $[F_{i+1}, F_i] = 2$

必要性已经在 1.2 节证明，充分性同样由 1.3 节推出。

次数条件
如果 α 是一个可作图数，那么 α 必然是 $\mathbb{Q}$ 上的代数数，并且其在 $\mathbb{Q}$ 上的次数（即其最小多项式的次数）$[\mathbb{Q}(\alpha) : \mathbb{Q}]$ 必须是 2 的幂。

若 α 可作图，则 α 属于域塔顶端的 F_n。我们有域的包含关系 $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq F_n$。根据域扩张的次数公式（塔律）：

$$[F_n : \mathbb{Q}] = [F_n : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] \tag{2}$$

由域塔定理，我们知道 $[F_n:\mathbb{Q}]=[F_n:F_{n-1}]\cdots[F_1:F_0]=2^n$。因此，$[\mathbb{Q}(\alpha):\mathbb{Q}]$ 必须是 2^n 的因子，这意味着它本身也必须是 2 的幂。

2 三大古典难题的不可解性证明

2.1 倍立方问题

倍立方问题在代数上等价于“能否用尺规作出长度 $\sqrt[3]{2}$”。

这个问题对于我们目前而言是十分容易证否的，因为 $\sqrt[3]{2}$ 在 $\mathbb{Q}$ 上的技校多项式为 x^3-2，于是扩张次数 $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$，并非 2 的幂次，故其不是可作图数。

因此，用尺规作图解决倍立方问题是不可能的。

2.2 三等分任意角问题

作图一个角 θ 等价于作出长度为 $\cos(\theta)$ 的线段。三等分角问题即是：给定一个任意角 α（即已知可作图长度 $\cos(\alpha)$），我们能否构造出角 $\alpha/3$（即作出长度 $\cos(\alpha/3)$）？我们利用三角学中的三倍角公式：$\cos(\alpha)=4\cos^3(\alpha/3)-3\cos(\alpha/3)$。令 $y=\cos(\alpha)$ 为已知量，$x=\cos(\alpha/3)$ 为待求量，则 x 必须满足三次方程 $4x^3-3x-y=0$。

我们无需证明所有角都不能三等分（例如 90° 角就可以三等分），只需找到一个反例，即可证明不存在通用的三等分角方法。一个经典的、具有决定性的反例是三等分 60° 角。

角 $\alpha=60^\circ$ 是可作图的，因为 $\cos 60^\circ=\frac{1}{2}$，是一个有理数。将其代入到三次方程中得到了 $\cos 20^\circ$ 需满足的方程 $8x^3-6x-1=0$

我们使用有理根定理容易证明多项式 $p(x)=8x^3-6x-1$ 在 $\mathbb{Q}$ 上不可约，于是域扩张次数 $[\mathbb{Q}(\cos 20^\circ):\mathbb{Q}]=3$，同样不是 2 的幂次。

这表明 60° 角无法用尺规三等分，因此不存在通用的三等分任意角的方法。

2.3 化圆为方问题

给定一个半径为 $r=1$ 的圆，其面积为 π。要作一个与它面积相等的正方形，需要作出边长为 s 的正方形，使得 $s^2=\pi$。这等价于作出长度为 $\sqrt{\pi}$ 的线段。

如果 $\sqrt{\pi}$ 是可作图数，由于可作图数域 $\mathcal{K}$ 对乘法封闭，那么 $(\sqrt{\pi})^2 = \pi$ 也必定是可作图数。然而，之前的一个直接结果是，所有可作图数都必须是代数数。

Lindemann–Weierstrass 定理是一个深刻的超越数理论结果。其一个关键推论，由 Lindemann 首次证明，即圆周率 π 是一个超越数。

由于 π 不是代数数，它自然不可能是可作图数。因此，作出长度为 π 或 $\sqrt{\pi}$ 的线段都是不可能的，从而化圆为方问题用尺规作图无法解决。

这三个经典问题的解决过程揭示了 " 不可解性 " 的不同层次。倍立方和三等分角问题失败的原因是代数性的：它们所要求的数虽然是代数数，但其最小多项式的次数（3 次）不符合可作图数的次数条件（2 的幂）。而化圆为方问题的失败则更为根本，它源于数 π 的超越性，这个数完全超出了代数方程所能描述的范畴。这清晰地表明，可作图数域 $\mathcal{K}$ 只是代数数域 $\mathbb{A}$ 中一个非常小的子集。

同样值得注意的是，这些 " 不可解性 " 是严格限定在尺规作图公理体系内的。如果放宽规则，例如允许使用带刻度的直尺（二刻尺），三等分角就成为可能。如果允许使用超越曲线，如阿基米德螺线，那么化圆为方也可以实现。这说明了数学中的 " 不可能 " 证明，通常是关于特定公理系统能力的精确陈述。

3 正多边形作图问题

与三大难题的“否决式”证明不同，正多边形作图问题是一个完整的分类问题。

3.1 与分圆域的联系

作一个正 n 边形，等价于在单位圆上定出其 n 个顶点。这在复平面上等价于作出 n 次单位根，特别是需要作出一个本原 n 次单位根 $\zeta_n = e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n)$。由于可作图数域对复共轭封闭，作出 ζ_n 等价于作出其实部 $\cos(2\pi/n)$ 和虚部 $\sin(2\pi/n)$。因此，正 n 边形的可作图性问题，最终归结为判断复数 ζ_n 是否是可作图数。

3.2 分圆域的伽罗瓦理论

包含 $\mathbb{Q}$ 和 ζ_n 的最小域称为 n 次分圆域，记为 $\mathbb{Q}(\zeta_n)$。ζ_n 在 $\mathbb{Q}$ 上的最小多项式是 n 次分圆多项式 $\Phi_n(x)$。

域扩张 $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ 的次数等于 $\Phi_n(x)$ 的次数，即欧拉函数 $\phi(n)$ 的值。

分圆域扩张 $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ 是一个伽罗瓦扩张。其伽罗瓦群 $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ 与模 n 的整数乘法群 $(\mathbb{Z}/n\mathbb{Z})^\times$ 是同构的。该群的阶为 $\phi(n)$。群中的一个自同构 σ_k（其中 $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ 由它对本原根的作用定义：$\sigma_k(\zeta_n) = \zeta_n^k$。

3.3 可作图性判据（Gauss-Wanzel 定理）

现在，我们可以将正多边形的可作图性与分圆域的伽罗瓦群结构联系起来。

由于作出 ζ_n 意味着 $[\mathbb{Q}(\zeta_n):\mathbb{Q}]$ 必须是 2 的幂，我们得到一个必要条件：正 n 边形可作图 $\Longrightarrow$ $\phi(n) = 2^k$ 对于某个整数 $k \geq 0$。

于是我们对 $\phi(n)$ 进行算术分析：

回顾欧拉函数的计算公式：若 n 的素数分解为 $n = p_1^{a_1} \dots p_r^{a_r}$，则 $\phi(n) = \prod_{i=1}^r \left(p_i^{a_i} - p_i^{a_i-1}\right) = \prod_{i=1}^r p_i^{a_i-1}(p_i - 1)$。

为了使 $\phi(n)$ 是 2 的幂，其每一个因子 $p_i^{a_i-1}(p_i-1)$ 都必须是 2 的幂。

对于奇素数因子 p_i，这要求 $a_i - 1 = 0$（即 $a_i = 1$）并且 $p_i - 1$ 是 2 的幂。一个形如 $p = 2^m + 1$ 的素数，必然要求 m 本身是 2 的幂，即 $m = 2^j$。这种形如 $F_j = 2^{2^j} + 1$ 的素数被称为 Fermat 素数。

对于素数因子 $p = 2$，因子 2^{a-1} 已经是 2 的幂。

综合起来，$\phi(n)$ 是 2 的幂的充要条件是 n 的形式为 $n = 2^k \cdot p_1 \cdot \dots \cdot p_t$，其中 $k \geq 0$，且 $p_1, \dots, p_t$ 是互不相同的 Fermat 素数。

Gauss-Wanzel 定理
一个正 n 边形可以用尺规作图的充要条件是，n 是 2 的幂与任意多个不同费马素数的乘积。目前已知的费马素数仅有五个：

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

$\phi(n)$ 是 2 的幂这一条件，在伽罗瓦理论中具有深刻的结构性意义。它意味着伽罗瓦群 $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ 是一个 2 - 群（阶为 2 的幂的群）。根据群论基本定理，任何有限 p - 群都存在一个合成列，其商群均为 p 阶。对于 2 - 群，这意味着存在一列子群 $G = G_0 \supset G_1 \supset \dots \supset G_k = \{e\}$，使得 $[G_i : G_{i+1}] = 2$。根据伽罗瓦理论基本定理，这一子群链正好对应一个域塔 $\mathbb{Q} = F_0 \subset F_1 \subset \dots \subset F_k = \mathbb{Q}(\zeta_n)$，且 $[F_{i+1} : F_i] = 2$。这恰好就是可作图性条件。