# 代数

在伽罗瓦 (Galois)(1811-1832) 的工作发表 (1846 年) 之前，代数学研究的主要问题是解方程，即求多项式的零点。

1. **代数方程**. 人们自古希腊以来一直探索解代数方程的一般方法，即寻找求解公式，这种公式应当是方程的系数经过有限次加减乘除和开方的结果。我们以前曾经讲过塔尔塔利亚、卡尔丹得到了三次方程的求解的一般方法 (1545 年出现于卡尔丹的《大衍术》(Ars Magna) 一书中), 费拉里紧接着给出了四次方程的解法，他的办法是通过一系列变换把四次方程的求解问题归结为三次方程 ( 发表在卡尔丹的《重要的艺术》一书中 )，但是他们都不承认复数根。

莱布尼兹重新考虑了整系数不可约三次多项式，深信解这种方程不可能不用到复数。他接着求五次方程的解，但没有成功。欧拉完整地给出了三次方程的求根公式，并且强调三次方程必定有三个根。拉格朗日则从根的对称函数出发，对于一般高次方程提出了“予解函数”的概念 ( $n$ 次方程的予解函数是该方程的根与 $n$ 次单位根的某个函数。如果它在 $n$ 个根的所有置换下有 $r$ 个不同的表达式，则此函数是 $r$ 次方程的根。如果这个 $r$ 次方程可解，则用它的 $r$ 个解可以求出原方程的根 )。用予解式可以成功地解三、四次方程 ( 予解函数是低一次方程的根 )，而且他的前辈用以解方程的所有方法都可以统一在他的方法之内。例如三次方程 $x^3+px+q=0$ 的予解函数可以取为 $\phi=(x_1+\omega x_2+\omega^2x_3)^3$, 其中 $x_1,\ x_2,\ x_3$ 是原方程的三个根，$\omega=(-1+\mathrm{i}\sqrt{3})/2$ 为三次单位根。可以证明 $\phi$ 满足一个二次方程，其系数是原方程的系数的有理函数 ( 原因是 $\phi$ 在 $x_1,\ x_2,\ x_3$ 的所有可能的 6 种置换下只能取两个值，即 $\phi$ 和 $\phi'=(x_1+\omega^2x_2+\omega x_3)^3$ )。将此二次方程的两个根记为 $A,\ B$, 则有关系式

$$\begin{cases} x_1+\omega x_2+\omega^2x_3=\sqrt[3]{A}, \\ x_1+\omega^2x_2+\omega x_3=\sqrt[3]{B}, \\ x_1+x_2+x_3=0. \end{cases}$$

由此即可解出 $x_1,\ x_2,\ x_3$. 对于四次方程 $x^4+px^2+qx+r=0$, 拉格朗日取的予解函数为 $x_1x_2+x_3x_4$, 它在四个根的所有 24 种置换下只可能取三个值，所以此予解函数满足一个三次方程，其系数是原方程的系数的有理函数。解出这个三次方程的三个根，在结合 $x_1+x_2+x_3+x_4=0$, 就可以求出 $x_1,\ x_2,\ x_3,\ x_4$. 但是五次方程的予解函数是至少六次多项式的根。因此拉格朗日被迫认为：对于次数大于 4 的方程用代数的方法求解看来是不可能的。但是他洞察到了解五次方程困难的关键所在。鲁菲尼 (Ruffini)(1765-1822) 在 1799-1813 年间一直试图证明五次以上方程没有根式解的公式，但是没有成功。他用拉格朗日的方法证明了对于五次以上的方程不存在满足次数小于 5 的方程的予解函数。拉格朗日的洞察后来被阿贝尔和伽罗瓦所借鉴。

找不出五次以上方程的求解公式并不意味着所有五次以上方程都不能解。特别是二项方程 $x^n-a=0$, 它的全部根是其一个根与 $x^n-1$(称为 $n$ 次分圆多项式) 的所有根的乘积。$n$ 次分圆多项式的求解与正 $n$ 边形作图有关。高斯断言：正 $n$ 边形可以用圆规直尺作图的充分必要条件是 $n=2^tp_1p_2\cdots p_m$, 其中 $p_i$ 是形如 $2^{2^k}+1$ 的两两不同的素数 ( 即所谓“费马素数” )。高斯证明了充分性，必要性则没有证明。1796 年他带着正 17 边形的

作图的证明到格廷根大学去见克斯特纳 (Kästener) 教授，教授不相信，企图赶走高斯，就像现在我们赶走三等分角的证明者一样，并说这个作图法不重要，因为实际的作图法是熟知的。但是高斯并仅不是给出实际的作图法，并且给出了理论上的证明，于是高斯说自己解出了一个 17 次方程。教授则说这是不可能的。

与解方程密切相关的是多项式的因子分解，而因子分解问题在积分学（部分分式法）中很重要。一个多项式有一个一次因子等价于它有一个根。关于实系数多项式，我们现在当然知道他必可以分解成一次、二次不可约因子的乘积，但是在 19 世纪以前这并不是一个明显的事实。莱布尼兹就不相信这个事实。欧拉是正确的，他在 1742 年给尼古拉 - 伯努利的一封信中说到了这个事实。但是后者不相信其正确性并且举了一个例子 $x^4-4x^3+2x^2+4x+4$ 有四个零点 $(1\pm\sqrt{2\pm\sqrt{-3}})$, 这与欧拉的结论矛盾 (?) 。欧拉在同年稍后时间给歌德巴赫 (Golebach)(1690-1764) 的信中说实系数多项式的复根是成对出现的，而 $x-(a+b\sqrt{-1})$ 与 $x-(a-b\sqrt{-1})$ 的乘积是实二次多项式，接着欧拉证明了尼古拉 - 伯努利的例子是两个实二次多项式的乘积。但是歌德巴赫也拒绝欧拉的思想，并给出例子 $x^4+72x-20$ 。后来欧拉告诉歌德巴赫（后者的）错误，并说明直到 6 次多项式这个结果都是对的。但是歌德巴赫仍不相信，因为欧拉没有给出一般性的证明。实系数多项式必可以分解成一次、二次不可约因子的乘积的问题关键在于这样的多项式至少有一个实根或复根，即所谓代数基本定理是否成立。达朗贝尔和拉格朗日都曾给出过欧拉的结论的证明，但都有错误。代数基本定理的第一个证明是高斯 (1777-1855) 在他的博士论文（ 1799 年）中完成的，即任一多项式在复数范围内一定有零点（发表于 1081 年），因而 $n$ 次方程有 $n$ 个根。后来高斯又给出了三个新的证明。在前三个证明中他都假定多项式的系数是实数，最后一个证明 (1848 年) 中的多项式是一般的复系数的。高斯的证明是存在性的而不是构造性的，因此不能用他的证明方法去解方程。事实上，他在 1081 年的一篇论文中声称次数大于 4 的方程一般无法用代数的方法求解。

阿贝尔在中学时就学习了拉格朗日和高斯的著作，并研究高次方程的求解问题。开始他以为自己解决了用根式解一般高次方程的问题，后来很快发现了错误。然后他致力于证明这种公式不存在。在 1826 年他证明了一个关键性的结果，即：如果一个方程能用根式求解，则解中出现的根式必定都能表为方程的根和单位根的有理函数。在此基础上他在 1826 年给出了五次以上方程没有根式解的第一个（复杂、迂回的）证明，其中有一个非本质性的错误。后来他又给出两个精心的证明。

伽罗瓦 15 岁进入巴黎的一所有名的公立中学，他仔细地研究了拉格朗日、高斯、哥西和阿贝尔的著作，后来进入了一个低等的所谓“预备学校”。 17 岁时他给出了一个代数方程能用根式解的判定准则（即 Galois 定理，用现在的话说就是：一个方程能用根式解当且仅当这个方程的分裂域的 Galois 群是可解群）。 1829 年他把两篇关于解方程的文章呈送给法国科学院，科学院转交给了哥西，结果哥西遗失了这两篇文章。 1830 年 1 月他又交给科学院另一篇仔细写成的文章，文章送到傅立叶处，但不久傅立叶去世了，该文也被遗失了。在波哇松的提议下，伽罗瓦在 1831 年写了《关于用根式解方程的可解性条件》一文，波哇松认为难以理解而退回。波哇松劝告他写一份较详尽的阐述。在 1832 年 5 月 31 日决斗被杀的前一夜，他匆忙起草了一份关于自己研究的说明，交给了他的朋友舍瓦利埃 (Shevalier), 这个说明被保存了下来。伽罗瓦曾因为政治罪两次被捕入狱，决斗之前他就在狱中，决斗的原因也是政治性的（他不愿忍受政治上的歧视）。 1846 年柳维尔在《数学杂志》上编辑出版了伽罗瓦的部分文章，其中有上面提到的 1831 年的那篇。对于伽罗瓦理论

的第一个全面、清楚介绍出现于若当 (Jordan)(1838-1922) 在 1870 年出版的《置换和代数方程专论》一书中。

1. **抽象代数**. 伽罗瓦的工作为代数方程的一千多年的研究画上了句号。不仅如此，人们从他的理论中看到了研究代数结构的重要性。伽罗瓦理论建立了一个代数方程的分裂域的子域与 Galois 群的子群之间的一一对应关系，对于域的研究在很大程度上等同于对于群的研究。这种深刻的思想导致后来人们把不同对象之间具有某些性质的一一对应称为伽罗瓦对应。

(i) **群**. 对于群的研究是从一些具体的群开始的。最初被研究的是置换群。拉格朗日和鲁菲尼在解方程时考虑一个方程的全部根的所有置换，实际上这些置换组成的就是对称群的子群，只不过他们的论述都是用 $n$ 个字母的函数所能取到的函数值给出的，因而一定程度上掩盖了群的本质。拉格朗日得到了一个结果，用现代的语言说，即（有限群的）子群的阶整除群的阶（这就是拉格朗日定理）。伽罗瓦在置换群中引入的最重要的概念是正规子群，他还引入了同构、单群的概念。他猜想阶为合数的最小单群是 60 阶群，即 5 次交错群。哥西在 1844-1846 年写了一大批文章，他也是用函数的取值进行叙述的。他证明了伽罗瓦的一个断言，该断言说：如果一个群的阶被某个素数 $p$ 整除，则它一定有 $p$ 阶子群。若当在 1869 年（对于置换群）引入了商群与合成群列的概念，并且证明了对于一个固定的群，其（不同的）合成群列对应的商群的阶的集合相同。 1899 年赫尔德 (Hölder) (1859-1937) 进一步证明了合成群列对应的商群的集合不依赖于合成群列。这就是若当 - 赫尔德定理。若当在前面提到的《置换和代数方程专论》一书中把置换群定义为一些置换组成的集合，该集合在符合运算下封闭。抽象群的定义中的其它定义性质都是作为明显的事实被使用的。书中明确地建立了同态与同构的概念，证明了关于合成群列和传递群的基本结果，他首次把交换群称为阿贝尔群。这本书出版以后不久，西洛 (Sylow)(1832-1918) 证明了以他名字命名的定理。

被研究的另一类具体的群是空间运动群（即三阶正交群），目的是确定晶体的可能结构。这项工作是物理学家和矿物学家布拉维 (Bravais)(1811-1863) 开始的。 1849 年他确定了晶体总共有 32 种对称的分子结构。

布拉维的研究给若当以深刻的印象。若当开创了置换群的表示论，即用可逆的线性变换来表示置换。由于若当研究的置换群都是有限群，所以必须对于线性变换加上一些限制，使得线性变换的个数与置换群的阶相等（伽罗华曾经限定线性变换定义在由素数 $p$ 个元素组成的有限域上）。接着若当开始研究无限运动群（他只考虑平移和旋转），他指出：确定运动群等价于确定分子系统（一个运动群对应于在该群作用下不变的分子系统）。于是他研究了各种不同的群，并将它们分类。他的群论工作也应用于几何，并很快被几何学家所接受（例如克莱因）。 1878 年若当证明了：如果一个线性变换连续作用 $p$ 次等于恒同变换，则适当地选择变量可以得到标准的线性变换

$$y_i' = \varepsilon_i y_i, \qquad i = 1, 2, \cdots, n.$$

19 世纪最后的二十年中另外一类被广泛研究的线性变换群是保持给定的二、三元二次型不变的（系数在某个范围内的）线性变换的全体构成的群。

作为抽象的群的第一个定义是凯莱在 1849 年提出来的。他所说的实际上是抽象的变换群（其元素都是算子）。由于任一抽象群都同构于某个变换群，所以他的定义不失普遍性。

他用可逆矩阵（乘法群）（作用于数组上）和四元数（加法群）（作用于自身）作为例子。但是他的定义没有引起人们的注意，其原因是当时矩阵和四元数并不为大多数人所知，另一个原因是其他的抽象的代数结构没有平行地出现。对于凯莱的过早的抽象地反应是寂寞无声。 1854 年他又写了一篇关于抽象群的文章，反应也不强烈。 1878 年他连续发表了四篇文章，他强调一个群可以看作是一个普遍的概念，无须限定于置换群。他指出任一有限群都可以表成一个置换群。这几篇文章有了较大的影响，因为人们此时已经抽象群比置换群远为广泛。其中的一些重要例子是克莱因在若当的影响下用变换群的观点研究几何， 1872 年提出爱尔兰根纲领。他所用到的变换群具有连续性（即变换群中的元素（矩阵）的各个位置上的实数可以连续变化）. 德德肯在 1877 年在数论的研究中抽象出来了交换群的严格定义（他称之为“代数数模”），克罗内克 (Kronecker)(1823-1891) 研究了有限交换群，得到了结构定理（即“基”的存在性，或者说有限交换群可以分解为循环群的直和）。 1879 年弗若宾纽斯 (Frobenius)(1849-1917) 和斯蒂尔伯格 (Stickelberger) (1850-1936) 的文章中认为抽象群应该包含整数的同余类、高斯的二次型和伽罗瓦的置换群。他们提到了无限群。

1870 年左右曾和克莱因一道工作的李 (Lie)(1842-1899) 开始研究连续群，其目的不是研究几何，而是要对微分方程的解进行分类，因为可以用经典的积分方法求解的微分方程在某些连续群的作用下不变。

现在我们教科书中的群的几种定义是 1902-1905 年由亨廷顿 (Huntington) 、穆尔 (Moore) 、迪克森 (Dickson) 给出的。在完成了群的抽象概念之后。数学家转向证明抽象群的定理，其中很多都是由具体的群的结果启发而来的。 1897 年德德肯和米勒 (George Miller) 引入换位子的概念并证明了换位子的全体生成正规子群。群论的研究集中在以下方面：群的自同构群、给定阶数的（互不同构的）有限群有多少种可能、可解群的判定、单群分类、群的生成关系的确定等。弗若宾纽斯、伯恩赛德 (Burnside)(1852-1927) 、莫利恩 (Molien)(1861-1941) 、舒尔 (Schur)(1875-1941) 等人将若当的置换群表示推广为一般的有限群表示论，弗若宾纽斯引入了可约和完全可约表示的概念并证明了若干基本结果。他还把群表示的特征标理论推广到所有的有限群上，并应用到无限群上。

二十世纪初的许多数学家都以为全部值得纪念的数学终究将会包含在群论中，特别是克莱因。庞卡莱也同样热情，他曾说：“ $\cdots\cdots$ 可以说，群论就是那摒弃其内容而化为纯粹形式的整个数学。”

(ii) **环**. 环论中的最重要的概念，即“理想”的引入者是库默尔 (Kummer)(1810-1893) 和德德肯。库默尔是高斯的学生。在研究费马大定理的过程中他为了弥补分圆整数范围内不可约因子分解唯一性的丧失，他引入了“理想数”。事实上， 1843 年库默尔曾经基于分圆整数环中的因子分解唯一性给出了费马大定理的证明。他把手稿寄给狄里赫勒，并说明这种唯一性是必需的。狄里赫勒通知他，唯一分解定理只对于某些分圆整数环成立。 1844 年库默尔认识到了狄里赫勒的批评是正确的，从而开始了弥补。拉梅也犯了同样的错误，并在 1847 年将错误的证明刊登在柳维尔主编的《数学杂志》上。当时柳维尔就指出了拉梅的错误。哥西也在这个方向上工作过，但后来他醒悟到了错误。库默尔在看到拉梅的文章后 1847 年写信给柳维尔，信中说他已经找到了一个挽救因子分解唯一性的办法，就是在分圆整数集合中添加上一些理想数。

1871 年德德肯定义了代数整数和数域的概念，进而引入了“环”的概念，证明了一个数域中的代数整数的全体构成一个环。它定义了与不可约因子分解密切相关的概念，即“可逆

元素”。他用数集代替库默尔的理想数，并称它们为理想。他接着定义了理想的乘法、理想的因子，由此定义素理想（没有除了自身和整个环之外的因子的理想，不是现代意义下的素理想）。最后的基本定理是“素理想分解唯一性”。

克罗内克继续发展了德德肯的工作。但他用的方法和德德肯不同。他用添加不定元的方法得到更大的环（多项式环），并且通过对于素理想作商环的办法得到代数扩域（哥西曾经用 $\mathbb{Z}[x]$ 关于 $x^2+1$ 的同余关系下 $x$ 所在的同余类作为虚数 i 的定义，克罗内克的方法是哥西的作法的推广）。

环论的进一步发展有三个重要的方向：结合代数、交换代数、非结合代数（主要是李代数）。结合代数 (韦德伯恩 (Wedderburn)(1862-1948) 奠定的理论) 在群表示论中有重要的应用，交换代数 (主要是德德肯、诺特 (E. Noether)(1882-1936) 的工作) 则是代数数论和代数几何的基础。李代数则和李群密切相关。

(iii) **域**. 域的初等理论就已经足以给三大尺规作图问题以回答。一个简单的事实是：域的扩张次数具有可乘性，即：设 $E$, $K$, $F$ 都是域，并且 $E \supset K \supset F$, 则有 $[E:F] = [E:K][K:F]$, 其中 $[E:F]$ 表示 $E$ 在 $K$ 上的扩张次数（ $E$ 作为 $K$ 上的线性空间的维数）。简单的讨论（分别直线与圆相交的三种可能）可以说明：从复平面上的点集 $\mathbb{Q}+\mathbb{Q}$i(即数域 $\mathbb{Q}$(i)) 出发，通过尺规作图，所能得到的点的坐标只可能是 $\mathbb{Q}$(i) 的二次扩张链中的元素（复数）。而 $60^\circ$ 角的 $1/3$ 的余弦是不可约多项式为 $8x^3-6x-1$ 的根，所以 $cos20^\circ$ 不可能用尺规作图得到，因此 $20^\circ$ 角不能用尺规作图得到。类似地立方倍积需要作出 $\sqrt[3]{2}$, 也是尺规作图不能实现的。至于化圆为方，则要求作出超越数，更无法完成。同样的讨论说明高斯断言的“正 $n$ 边形可以用圆规直尺作图的充分必要条件是 $n = 2^t p_1 p_2 \cdots p_m$, 其中 $p_i$ 是形如 $2^{2^k}+1$ 的两两不同的素数”的必要性是正确的。

有限域起源于伽罗瓦。数域是德德肯引入的。抽象的域的定义则出自韦伯 (H. Weber)(1842-1913)1893 年的论文。体 (除环) 在 1905 年之前只有四元数体，之后迪克森 (Dickson)(1874-1954) 构造出了一系列新的体。

汉瑟尔 (Hensel)(1861-1941) 在 1908 年引入了 $p$- 进数域。这种域在代数数论与代数几何中同实数域、复数域同等重要。

抽象代数产生于数学的实际问题。用代数的方法可以构造无穷无尽的新对象，例如可以在已经定义的代数结构（如环上的代数）上再定义同样的代数结构。很多研究者都不清楚他作的事情是否有实际背景和应用价值。代数学变得越来越庞大，分支越来越细，这是 20 世纪代数学的一种倾向。当然，时间的进程将会把有用的知识保存下来，而淘汰掉无用的。