《数学史》论文

学年学期: 2022-2023-2

论文编号: 2022-2023-2-

提交日期: 2023 年 3 月 3 日

姓　　名: 周晟煜

院　　系: 求真书院

班　　级: 求真 30

学　　号: 2023013219

评阅意见:
论文成绩（百分制）:
论文考核意见: ☐ 通过 ☐ 不通过

尺规作图和群论及代数学发展

周晟煜

2024 年 3 月 3 日

前言

代数学是数学的一个重要分支，它研究的是数、量、结构和变化等数学对象之间的关系。

大约三千年来，直到十九世纪初，“代数”一直意味着求解多项式方程。这些方程的符号问题、方程根的性质，以及根所隶属的各种数系的规律，也都是与此相关的问题。所有这些问题后来都被称为古典代数。

在一代代数学家所关注的解方程这一基本问题的漫长求索过程中，古典代数学得到极大丰富与发展。而更为重要的是，跑最后一棒的Galois为解决问题而创造性地引人了全新的“群”概念与崭新的“群论”思想。这开辟了代数学的新的源泉，引发了代数学的革命性变化。

在他之前，解方程始终占据着代数舞台的中心，代数学曾仅仅被认为是解方程的学问，而在他之后，代数学被引入一个新的轨道，代数的面貌为之焕然一新。代数不再限于研究方程，而是更多地把注意的目标转向各种代数结构。

Arthur Cayley , Richard Dedekind , Evariste Galois , Carl Friedrich Gauss , William Rowan Hamiltonm , Emmy Noether 和 Emil Artin 等许多数学家在这个领域不断的探索，代数学结束了解方程的历史，进入研究新的数学对象(群、环、域、格等)的发展阶段，由此逐渐形成了数学的重要分支“近世代数”，又称“抽象代数”。而追根溯源，群的引入正是在方程根式解这一古典问题的深入研究中获得的。

周晟煜

2024 年 3 月 3 日

目录

一、 古典代数的历史

1、 古典代数的由来

大约三千年来，直到十九世纪初，“代数”一直意味着求解多项式方程，主要是四次或四次以下的方程。这些方程的符号问题、方程根的性质，以及根所隶属的各种数系的规律，也都是与此相关的问题。所有这些问题后来都被称为古典代数(“代数”一词在公元九世纪才被创造出来)。

大多数主要的古代文明，如巴比伦文明、埃及文明、中国文明和印度文明，都涉及多项式方程的解法，主要是线性方程和二次方程。古埃及人在各类纸草书中求解了形如 $x+ax=b$ 或 $x+ax+bx=c$ 的一次方程，他们还研究并处理了简单的二次方程，如在某一部纸草书中有一个问题：

把一个面积为 100 的正方形分为两个小正方形，使其中一个的边长是另一个的 $\frac{3}{4}$ 。

容易看到，这一问题可以引出一个形如 $ax^2=b$ 的二次方程，相当于古埃及人解决了最简单的一类二次方程。

图 1: 古埃及纸草书

古巴比伦人(约公元前 1700 年)是特别杰出的代数学家，他们能够用类似于我们的方法解一元二次方程。在有一块泥板文书中有这样一个问题：

已知igibum比igum大7，问igibum和igum各为多少？

这里igibum和igum是古巴比伦数学中互为倒数的两数。值得注意的是，这里古巴比伦人相当于用记号来表示未知量。另外，古巴比伦使用 60 进制，则上述问题相当于求解方程：

$$\begin{cases} xy = 60 \\ x - y = 7 \end{cases} \tag{1}$$

如我们所熟知的，这可以转化成求解一个二次方程 $x^2 - 7x - 60 = 0$ 。对这个问题古巴比伦人给出算法： $x = \sqrt{\left(\frac{7}{2}\right)^2 + 60} + \frac{7}{2} = 12$ ，相当于对二次方程 $x^2 - px - q = 0$ 使用了求根公式 $x = \sqrt{\left(\frac{p}{2}\right)^2 + q} + \frac{p}{2}$ ，这与我们更熟悉的 $x = \frac{p + \sqrt{p^2 + 4q}}{2}$ 是等价的。

图 2: Plimpton 322 泥板

虽然古巴比伦人给出了求解的步骤，但是他们并没有给出这么做的理由。此外，在古巴比伦代数系统中，他们只承认正有理数，零、负数、无理数都不属于古巴比伦的代数系统。相比之下，古中国和古埃及更胜一筹，他们允许在方程和代数式中使用负的系数，尽管不允许使用负根。

中国古典数学从公元前到公元 14 世纪，先后经历了三次发展高潮，即两汉时期、魏晋南北朝时期和宋元时期。在成书于 1 世纪的经典著作《九章算术》“少广章”中最早记载了开平方术和开立方术，即解方程 $x^2 = a$ 与 $x^3 = b$ 。在这类开方的过程中会遇到开不尽的情形，即遇到无理数。对此，中国古代数学家已经能够有效计算这些方程解的近似值。魏晋时期的著名数学家刘徽在为《九章算术》作注时，更是明确提出“求微数法”相当于用十进制小数任意逼近不尽根数。在《九章算术》的开平方术中，实际上还包含了二次方程$x^2 + bx = c$ 的数值求解程序，被称为“开带从平方”。到唐代时，数学家王孝通在《缉古算经》中研究了“开带从立方”，书中他给出 28 个形如 $x^3 + px^2 + qx = c$ 的正系数方程，并得出其正有理根。这表明，王孝通已掌握了求三次方程正根的数值解法。这些方法在宋元时代发展为一般高次方程的数值求解。先是在 11 世纪，宋代数学家贾宪创造出一种新的开方法——增乘开方法，通过随乘随加导出减根方程，逐步求出高次方程的正根。其后，12 世纪北宋数学家刘益第一次突破方程系数为正的限制。在前人

工作的基础上，南宋数学家秦九韶总其大成，提出一套完整的逐步求出高次方程正根的程序“正负开方术”，用这种方法可以简便有效地求出形如 $a_nx^n + a_{n-1}x^{n-1} + \ldots a_1x + a_0 = 0$ 的高次方程的正根。这种求高次方程正根的一般方法现被称为秦九韶法，它与英国数学家霍纳 1819 年创立的霍纳法基本上一致。秦九韶法的提出，表明中国古代数学已经能解决任意次方程的数值求正根问题。

古希腊数学的繁荣时期是在5至12世纪。其间印度出现了许多有代表性的数学家，如婆罗摩笈多、婆什伽罗等。婆罗摩笈多在其主要著作《婆罗摩笈多修正体系》中，给出了一次方程与二次方程的解法。对一次方程他给出的法则是：“绝对项之差变号后，除以未知数系数之差就是方程的未知数的值。”这法则相当说，对于一次方程 $ax + b = cx + d$ 其解为 $x = \dfrac{-(b-d)}{a-c}$ 。对二次方程他给出“消去中项法则”：从平方项及简单项的另一端取绝对项。绝对项乘以平方项系数的4倍，加上中项系数的平方。其和的平方根，减去中项的系数把结果除以平方项系数的2倍，得中项的值。这一法则相当于说，二次方程 $ax^2 + bx = c$ 的解为 $x = \dfrac{\sqrt{b^2 + 4ac} - b}{2a}$ 。与其他人不同的是，婆罗摩笈多允许方程的系数出现负数和零，方程的解也可以是负数和无理数。

古典代数随着时间的推移和数学研究的进展不断发展和完善。到了19世纪，代数学家们将古典代数与抽象代数相结合，形成了现代代数学的基础。古典代数的思想和方法在现代数学研究中仍然具有重要的地位，并为解决各种数学问题提供了强有力的工具。我们将在下文详细介绍。

2、 方程的解与复数

多项式方程的根式解就是用方程的系数给出方程根的公式。对系数允许进行的运算只有四种代数运算(加、减、乘、除)和开方运算(平方根、立方根等，即 "根式")。例如，在上文中，我们介绍了二次方程式 $ax^2+bx+c=0$ 的解是 $x=\dfrac{-b\pm\sqrt{b^2-4ac}}{2a}$。对于三次方程根式解的探索，卡尔达诺是第一位公布解的数学家。但是更早的，德尔费罗和塔塔里亚最先发现三次方程的根式解，后者将他的方法传给了卡尔达诺。尽管卡尔达诺承诺不会发表，但他很快就发表了。这个公式是：三次方程 $x^3=ax+b$ 的解是

$$x=\sqrt[3]{\frac{b}{2}+\sqrt{\left(\frac{b}{2}\right)^2-\left(\frac{a}{3}\right)^3}}+\sqrt[3]{\frac{b}{2}-\sqrt{\left(\frac{b}{2}\right)^2-\left(\frac{a}{3}\right)^3}}$$

这个根式解被称为**卡尔达诺公式**。对于一般的情形只需换元消去二次项即可套用卡尔达诺公式。

利用卡尔达诺公式我们也可以轻松给出四次方程的解。

我们只考虑缺少三次项的四次方程 $x^4+bx^2+cx+d=0$ (因为可以通过换元消去三次项)，引入参数 t 配方得 $\left(x^2+\dfrac{b}{2}+t\right)^2=2tx^2-cx+\left(-d+\dfrac{b^2}{4}+bt+t^2\right)$，我们希望等式右边也是完全平方，即判别式 $\triangle=c^2-8t\left(-d+\dfrac{b^2}{4}+bt+t^2\right)=0$ ，这是一个关于 t 的三次方程，利用卡尔达诺公式解出 t 后自然可以解出 x。

图 3: 卡尔达诺

几个世纪以来，数学家一直坚持一种观点，即负数的平方根不存在。既然正数和负数的平方都是正数，那么负数的平方根自然不存在，也不可能存在。这一切在出现三次方程求根公式后发生了变化。例如，将该公式应用于方程 $x^3=9x+2$ ，则有 $x=\sqrt[3]{\dfrac{2}{2}+\sqrt{\left(\dfrac{2}{2}\right)^2-\left(\dfrac{9}{3}\right)^3}}+$

$\sqrt[3]{\frac{2}{2}-\sqrt{\left(\frac{2}{2}\right)^2-\left(\frac{3}{3}\right)^3}}=\sqrt[3]{1+\sqrt{-26}}+\sqrt[3]{1-\sqrt{-26}}$ 。我们在这种观点下又该如何理解这个解呢？由于卡尔达诺不喜欢负数，因此更别说负数的平凡根了，所以他认为他的公式不适用于 $x^3=9x+2$ 这样的方程。纵观古今，毕达哥拉斯也有过类似的判断，他认为面积为 2 的正方形不存在(即 $x^2=2$ 无解)。

意大利数学家邦贝利改变了这一观点。在他的《代数》一书中，他将卡尔达诺公式应用于方程 $x^3=15x+2$ ，得到 $x=\sqrt[3]{1+\sqrt{-121}}+\sqrt[3]{1-\sqrt{-121}}$ 。但是他通过观察发现 $x=4$ 是原方程的一个根。此外，$2\pm\sqrt{3}$ 也是该方程的根，这与公式得到的结果相悖！虽然 $x^3=15x+2$ 三个根均为实数，但求根公式中却出现了复数的平方根——这在当时是毫无意义的。

邦贝利为了解决这个矛盾，将实数的运算法则应用于负数的平方根之上。他规定，或者说利用 $\left(+\sqrt{-1}\right)\left(+\sqrt{-1}\right)=-1$ 与 $\left(+\sqrt{-1}\right)\left(-\sqrt{-1}\right)=1$ 证明了 $\sqrt[3]{1+\sqrt{-121}}=2+\sqrt{-1}$ 与 $\sqrt[3]{1-\sqrt{-121}}=2-\sqrt{-1}$ ，这样就有 $x=\sqrt[3]{1+\sqrt{-121}}+\sqrt[3]{1-\sqrt{-121}}=\left(2+\sqrt{-1}\right)+\left(2-\sqrt{-1}\right)=4$ 。现在我们将 $\sqrt{-1}$ 记作 i 并熟悉它的运算法则，但这个做法在当时可谓是天马行空，邦贝利写道：

> 在许多人看来，这是一种天马行空的想法；我也曾在很长一段时间里持同样的观点。整个事情似乎是建立在诡辩之上，而不是建立在真理之上。然而，我一直在寻找，直到我真的证明了这一点。
>
> It was a wild thought in the judgment of many; and I too was for a long time of the same opinion.The whole matter seemed to rest on sophistry rather than on truth. Yet I sought so long until I actually proved this to be the case.

在接下来的两个世纪里，复数一直被蒙上一层神秘的面纱。人们对复数知之甚少，而且经常忽视复数。直到 1831 年高斯将复数表示为平面上的点之后，复数才被视为数字系统中的元素。19 世纪的研究表明，这种三次方程的任何根式解都必须涉及复数。因此，在化简不可约立方根(如上文中的 $\sqrt[3]{1+\sqrt{-121}}$与$\sqrt[3]{1-\sqrt{-121}}$)时，复数是不可避免的。正因为如此，复数是在求解三次方程而非二次方程时出现的，而人们往往错误地认为复数是在求解二次方程时出现的。事实上，一元二次方程 $x^2+1=0$ 的解不存在这一件事几个世纪以来一直被人们所接受。

3、 代数系统与代数基本定理

数学符号现在已被视为理所当然。事实上，没有完善的符号记号的数学是不可想象的。然而，数学学科在几乎没有符号的情况下发展了约三千年。

代数中符号符号的引入和完善主要发生在十六世纪和十七世纪初，主要归功于韦达和笛卡尔。韦达在其《分析艺术导论》中迈出了决定性的一步。他认为代数是“数学中正确发现的科学”，并有一个宏伟的愿景，即“没有解决不了的问题”(事实上我们知道由于哥德尔不完备定理这句话并不正确)。韦达的基本思想是在方程中引入任意参数，并将这些参数与方程的变量区分开来。他用辅音(B、C、D...)表示参数，用元音(A、E、I...)表示变量。因此，一元二次方程被写成 $BA^2 + CA + D = 0$ 。于我们而言，这似乎是一个简单且自然的想法，但它却是代数学的一次根本性变革：三千多年来，人们第一次可以谈论一般的一元二次方程，即一个具有任意字母系数的方程，而不是一个具有任意数字系数的方程。

图 4: François Viète

这是一项开创性的成果，因为它将代数学从对特殊问题的研究转变为对一般问题的研究，从对具有数值系数的方程的研究转变为对一般方程的研究。韦达本人也开始系统地研究具有字母系数的多项式方程。例如，他提出了五次及以下多项式方程的根与系数之间的关系，即现在我们所说的韦达定理。代数从此开始变得更加抽象，并逐渐成为一门符号科学。

但是事实上，韦达并没有将方程完全符号化。例如，三次方程 $x^3 + 3B^2x = 2C^3$ 将被韦达表述为“x cubus + B plano 3 in x aequari C solido 2”。更特别的是，韦达同古希腊人一样要求代数表达式齐次。从上面这个奇怪的三次方程的写法就能看出来。按照他们的思维方式，比如乘积 ab 表示面积，c 表示长度，那么 $ab + c$ 这样的算式是没有意义的，因为面积与长度不能相加。

笛卡尔在他的重要著作《几何》中克服了这些问题，他在书中阐述了解析几何的基本要素。笛卡尔的符号是完全符号化的，本质上是现代符号。例如，他用 x、y、z...表示变量，用 a、b、c 表示参数。最重要的是，他引入了“线段代数”，即对于长度为 a 和 b 的任意两条线段，他构造了长度为 $a+b$、$a-b$、ab 和 a/b 的线段。这样，代数表达式的齐次性就不再需要了。例如，$ab+c$ 现在是一个合法的表达式，即一条线段。这一思想代表了一项最重要的成就：它消除了代数中对几何的需求。

两千年来，几何在很大程度上一直是数学的语言，现在，代数开始扮演这一角色。

图 5: 笛卡尔

x 韦达和笛卡尔的著作将人们的注意力从数字方程的可解性转移到了对有字母系数的方程的理论研究，多项式方程理论开始出现。其主要关注点包括确定此类方程根的存在性、性质和数量。

Q1：是否每个多项式方程都有一个根？ 如果有，是什么样的根？ 这是所有问题中最重要也是最难的一个。事实上，问题的第一部分比第二部分容易回答得多。代数基本定理回答了这两个问题：每个多项式方程，无论是实系数还是复系数，都有一个复根。

Q2：一个多项式方程有几个根？ 笛卡尔在《几何》一书中证明了若 α 是多项式 $p(x)$ 的根，则 $p(x)$ 可以被写成 $(x-\alpha)q(x)$ 的形式，其中 $q(x)$ 是次数比 $p(x)$ 低一次的多项式。反复利用这个结论与代数基本定理可以得到任意一个 n 次多项式方程有 n 个根 $\alpha_1, \alpha_2, \ldots, \alpha_n$ 是复数，且 $p(x) = c(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$ 。

Q3：我们能确定这些根是有理根、实数根、复数根还是正数根吗？ 在十七和十八世纪，人们凭直觉接受了对于奇数次实系数多项式方程，它一定有一个实根。十九世纪，微积分中的中值定理作为一个简单的结果正式证明了这一观点。牛顿证明了复根都是成对共轭出现的。即，若 $a+bi$ 是多项式 $p(x)$ 的根，那么 $a-bi$ 也是 $p(x)$ 的根。

笛卡尔给了一个算法寻找一个整系数多项式方程的有理根。若既约分数 $\frac{q}{p}$ 是多项式 $a_n x^n +$

$a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$ 的根，则 $p \mid a_n$ 且 $q \mid a_0$。这是因为在等式 $a_n\left(\frac{q}{p}\right)^n+a_{n-1}\left(\frac{q}{p}\right)^{n-1}+\cdots+a_1\frac{q}{p}+a_0=0$ 两端乘 p^n 可以得到 $a_nq^n+a_{n-1}q^{n-1}p+\cdots+a_1qp^{n-1}+a_0p^n=0$。注意到 p 整除除了第一项以外的所有项，故只能也整除第一项。但 p 与 q 互素，因此只能 $q \mid a_n$。$p \mid a_0$ 同理。

他还陈述了后来被称为笛卡尔符号法则的内容(但并未证明)：多项式 $p(x)$ 的正根数不超过其系数的符号变化次数(从“$+$”变成“$-$”或反之)，负根数不超过连续出现两个“$+$”符号或两个“$-$”符号的次数。

Q4：多项式的根与系数之间有什么关系？ 人们早就知道，若 α_1 和 α_2 是二次函数 $p(x)=ax^2+bx+c$ 的根，那么 $\alpha_1+\alpha_2=-\frac{b}{a}$，$\alpha_1\alpha_2=\frac{c}{a}$。韦达将这一结果推广到五次及以内的多项式，给出了用系数表示多项式根的某些和与积的公式。牛顿为任意次数的多项式建立了这种类型的一般结果，从而引入了多项式根的对称函数这一重要概念。

Q5：如何确定多项式的根？ 最理想的方法是确定根的精确公式，最好是根式解。我们已经看到四次以内的多项式都有这样的公式，并尝试将结果扩展到更高的多项式。在没有精确的根式解的情况下，人们开发了各种方法来求出所需精确度的近似根。其中最著名的是十七世纪末和十九世纪初牛顿和霍纳的方法，前者涉及微积分的使用，即我们熟知的牛顿逼近法。

十七世纪初，吉拉尔和笛卡尔对代数基本定理作了陈述但是并不精确，且没有给出证明。例如，笛卡尔对该定理的表述如下：“每个方程都可以有与方程中未知量的次数一样多的不同根”。鉴于他对复数的使用感到不安，他的“可以有”是可以理解的。

复数在十七世纪末的微积分学中非常重要，因为它使数学家能够通过将有理函数的分母分解为一次因式和二次因式来求解有理函数的积分。但是，人们该如何相信这个定理呢？尽管大多数数学家都认为这一结果是正确的，但莱布尼茨却不这么认为。例如，在 1702 年的一篇论文中，他声称 x^4+a^4 无法分解为一次因式和二次因式。

达朗贝尔于 1746 年给出了第一个代数基本定理的证明，随后欧拉也很快给出了证明。达朗贝尔的证明使用了分析的思想，欧拉的证明主要是代数的。但是这两个证明都不完整，缺乏严谨性，尤其是假定 n 次多项式都有 n 个根，可以根据实数法则进行运算，以此来证明这些根是复数。

在 1797 年，年仅 20 岁的高斯完成了证明，并在 1799 年发表于博士论文中，以当时的标准给出了一个严谨证明。从现代的角度来看，高斯基于几何和分析思想的证明也有不足之处。而后数十年内，高斯又陆续进行了三次证明。

自此以后，人们给出了许多关于代数基本定理的证明，其中一些证明是在 2000 年代给出的。其中一些是代数证明，另一些是分析证明，还有一些是拓扑证明。这是可以理解的，因为具有复

数系数的多项式同时是代数、分析和拓扑对象。有点自相矛盾的是，代数基本定理并没有纯代数证明。“有理数上奇数次的多项式有一个实根”这一分析结果在所有代数证明中都被证明是不可避免的。

对多项式方程解法的研究不可避免地会导致对各种数系的性质和属性的研究，因为解法本身就是数。因此，数系研究构成了古典代数的一个重要方面。负数和复数虽然在十八世纪被频繁使用，但人们往往对它们心存疑虑，了解甚少。尽管人们自古以来就知道负数的运算规则，如$(-1)(-1)=1$，但过去却没有给出合理的解释。十八世纪末和十九世纪初，数学界人士开始追问为什么这些规则会成立。剑桥大学分析学会的成员在这个问题上取得了重要进展。在剑桥，数学是文科学习的一部分，被视为绝对真理的典范，用于培养年轻人的逻辑思维。因此，这些数学家认为，代数学，尤其是负数运算法则，必须建立在坚实的基础之上。

接下来，Peacock提出了符号代数理念，英国数学家将之付诸实践，提出了具有不同于算术性质的代数方程。用布尔巴基的话说：英国学派的代数学家在 1830 年至 1850 年间首先提出了构成律这一抽象概念，并通过将这一概念应用于一系列新的数学对象，立即扩大了代数领域：Boole提出了逻辑代数，Hamilton提出了向量、四元数和一般超复数系统，Cayley提出了矩阵和非交换律。因此，无论符号代数有怎样的局限性，它都为后来代数学的发展提供了积极的氛围。符号及其运算定律开始有了自己的生命，成为研究对象，而不是表示关系的语言。

二、 尺规作图的历史

1、 几何三大问题的由来

公元前 5 世纪，古希腊雅典出现了一个包括各方面学者的巧辩学派(也称智者学派)。他们第一次提出并研究了三个作图问题：倍立方问题、三等分角问题、化圆为方问题。这就是数学上著名的具有历久不衰魅力的几何三大问题。这三个问题的共同点是寻求一种仅用直尺和圆规的解法。在这一非常关键的限制条件下，三大问题虽一直吸引着人们的注意，但历经 2000 多年却一直未获真正解决。直到 19 世纪，人们才最终证明了找不到解法是因为它们根本不存在，也就是说这三大问题是尺规不能问题。

几何三大问题的表述较为简单：**倍立方问题**：求作一立方体，使其是给定立方体体积的两倍。**三等分角问题**：将任意一个给定角三等分。**化圆为方问题**：求作一正方形，使其面积等于给定圆的面积。

关于这些问题有一些传说故事起到了推波助澜的作用。实际上，这三个问题的产生都是相当自然的。当古希腊人熟知以正方形对角线为一边的正方形有两倍于前者的面积，提出相应的体积问题是理所应当的，即倍立方问题。三等分角也应当是古希腊人解出了任意角三等分的方法后的衍生，化圆为方则是两个基础图形之间联系的探索。

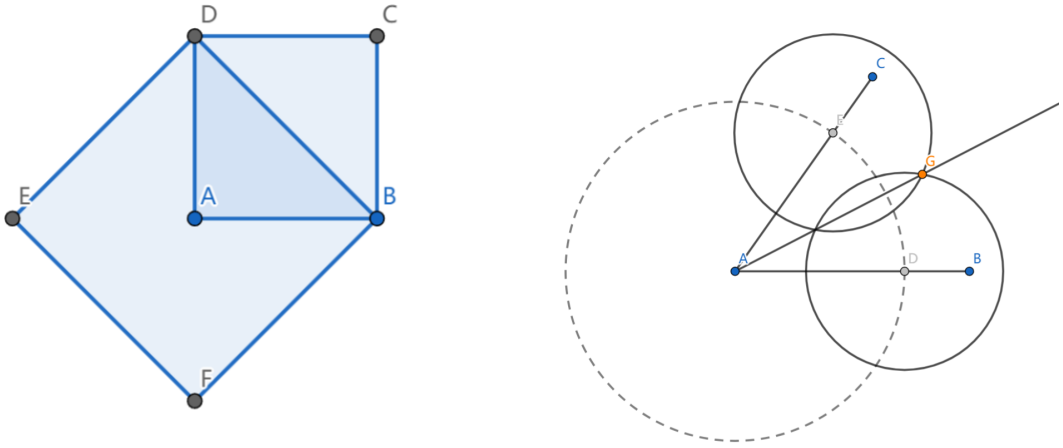


图 6: 倍正方形(左)和二等分角(右)

这三个问题都有前提条件，即需要尺规作图完成。尺规作图是一种几何构图方法，使用直尺和圆规来绘制各种几何形状和图形。直尺通常是一种无刻度的直棍，用于画直线。圆规由两个可以移动的脚组成，其中一个脚可以画圆的弧线，另一个脚用以固定圆心。

根据现有的资料，在历史上最先明确提出尺规限制的是伊诺皮迪斯。在这以前，许多作图题都是不限工具的。他以后经过柏拉图大力提倡尺规的限制渐渐成为一种公约，最后总结在《几何

原本》一书中，并由公设的形式规定下来。欧几里得提出的公设有 5 条，其衍生出的尺规作图作图公法也有 5 条：

(1)过两已知点作一直线。

(2)确定二已知直线的交点。

(3)已知圆心和半径作圆。

(4)确定已知直线和已知圆的交点。

(5)确定二已知圆的交点。

在作图公法的限制下，用尺规确实可以作出许多图形，甚至可以做出相当复杂的图形，但是否如古希腊人所相信的那样“不论多么复杂的图形都能依靠足够的耐心和聪明的才智，仅用尺规把图作出来”呢？并非如此。事实上，有些图形确实无法只用尺规完成，本章介绍的三大作图问题就是最典型的尺规作图不能问题。在长达 2000 多年的时间里，由于人们未能意识到这一点，所以为解决此问题付出了无数的心血，而结果都以失败告终。

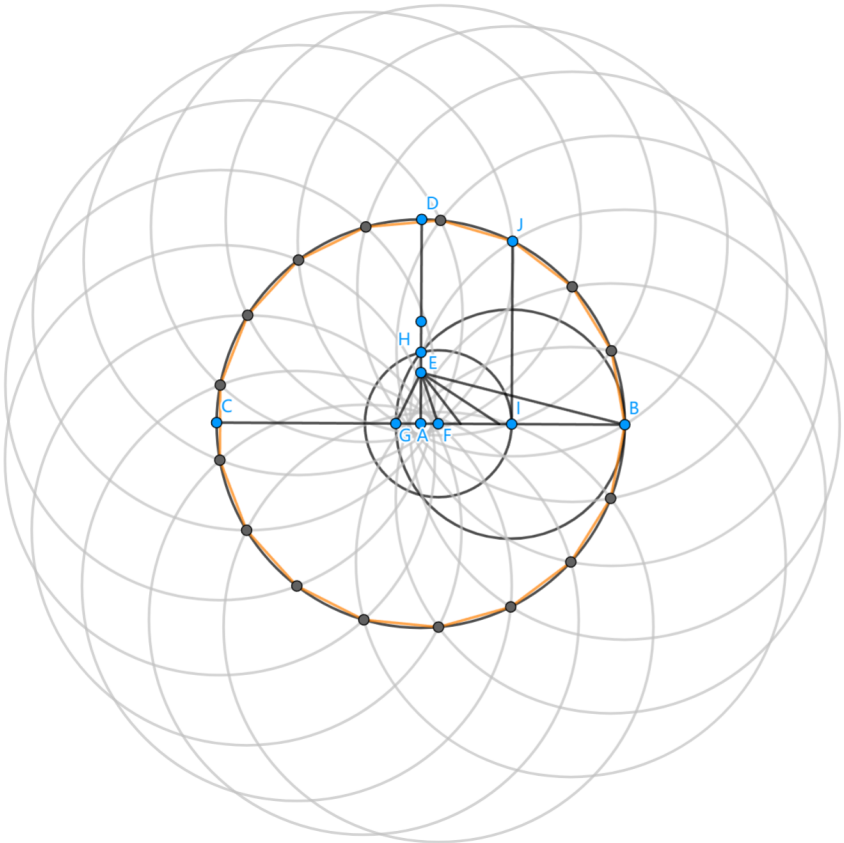


图 7: 尺规作正十七边形

2、 几何三大问题的历史解答

倍立方问题提出不久之后，古希腊数学家希波克拉底将问题化简为，对于给定的a，寻找x, y满足$\frac{a}{x} = \frac{x}{y} = \frac{y}{2a}$，称$x, y$是$a, 2a$的**双比例中项**。在这一思路的启发下，公元前 3 世纪的门奈赫莫斯给出了两种做法。一种是考虑抛物线$x^2 = ay$和$y^2 = 2ax$在第一象限的交点，另一种是考虑抛物线$x^2 = ay$与双曲线$xy = 2a^2$的交点。

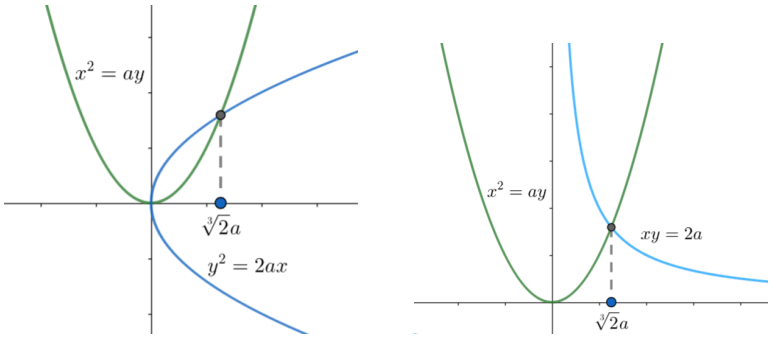


图 8: 门奈赫莫斯的做法

该做法引出了我们现在熟知的圆锥曲线。但是它不满足尺规作图的要求。柏拉图借助器械给出了另外的做法。在x轴正半轴上取$OA = a$，在y轴负半轴上取$OB = 2a$。取两个直角的曲尺，使一曲尺通过A点，且直角顶点在y轴上；另一曲尺通过B点，且直角顶点在x轴上。调整两个曲尺使得另一直角边至贴合为止。这样便在两条坐标轴上确定了点A和点B。注意到$\triangle AOC \sim \triangle DOC \sim \triangle BOD$，故有$\frac{a}{OC} = \frac{OA}{OC} = \frac{OC}{OD} = \frac{OD}{OB} = \frac{OD}{2a}$，即$OC, OD$是$a, 2a$的双比例中项。

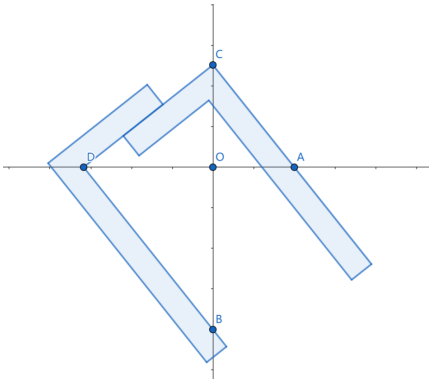


图 9: 柏拉图的做法

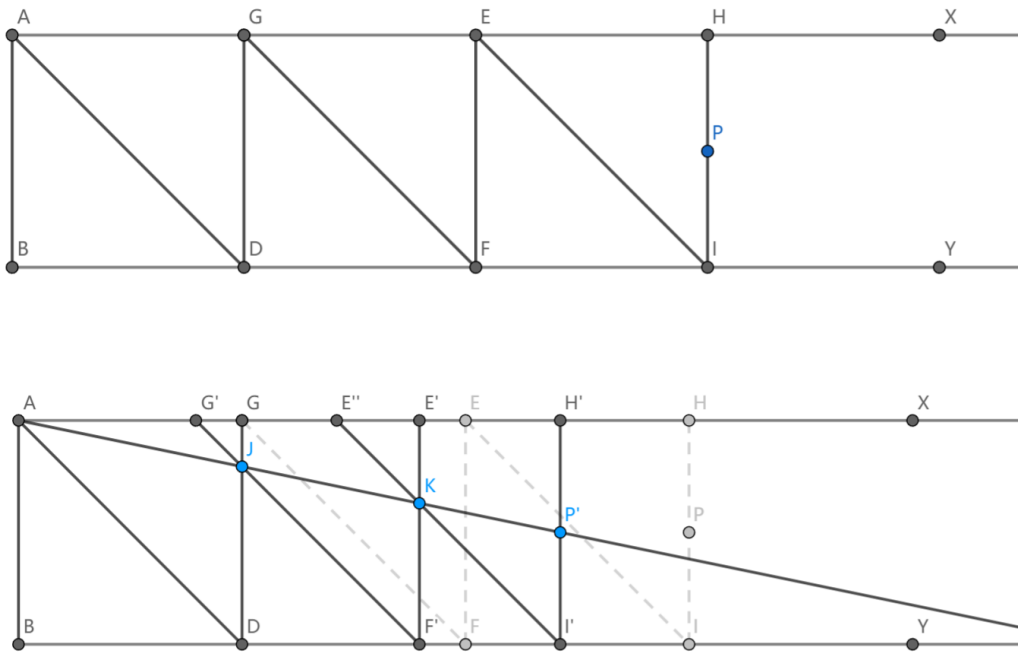


图 10: 埃拉托塞尼的做法

希腊数学家埃拉托塞尼借助另一种器械也给出了解答。如上图，在两条平行线AX, BY之间有三个相同的等腰直角三角形AGD，GEF，EHI，前者固定，后两者可以在平行线之间滑动。取HI中点P，滑动三角形GEF至$G'E'F'$，滑动三角形EHI至$E''H'I'$，使得$G'F'$和GD的交点J，和$E''I'$和$E'F'$的交点K都在线段AP'上。注意到$\triangle AJD \sim \triangle JKF' \sim \triangle KP'I'$，若设$AB = 2a$，$PI = a$，则$\dfrac{AD}{JD} = \dfrac{JF'}{KF'} = \dfrac{KI'}{P'I'}$，进而有$\dfrac{2a}{JD} = \dfrac{AB}{JD} = \dfrac{JD}{KF'} = \dfrac{KF'}{P'I'} = \dfrac{KF'}{a}$，即$JD, KF'$是$a, 2a$的双比例中项。

有趣的是，将该器械中的三角形个数改成n个，那么类似的我们便能作出n比例中项，即可以通过该器械开n次根。

对于三等分角问题，阿基米德在其《引理集》中证明了一个类似命题。

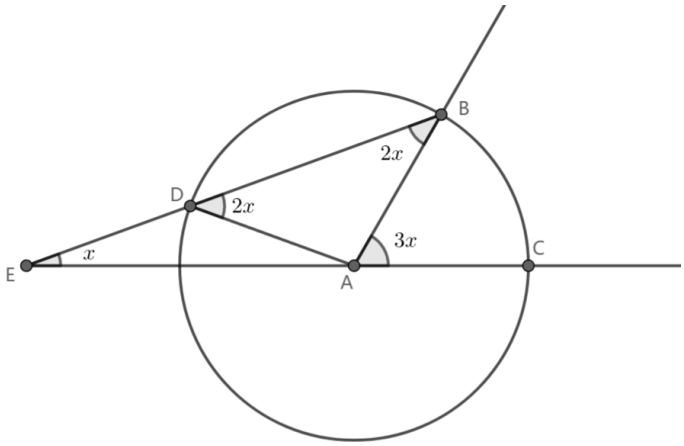


图 11: 阿基米德的做法

如上图，以已知角A的顶点为圆心作圆，分别交已知角两边于B,C，过B点引线与圆交于D，与直线AC交于E，使得DE长恰为圆的半径，此时角E即为所求的三等分角。该方法的难点在于如何做出符合条件的线BDE。可以通过在直尺上刻出两个距离为圆的半径的点，将直尺绕点B旋转并调整位置来确定D和E。但这相当于使直尺有了刻度，不符合尺规作图的条件。

帕普斯利用双曲线给出了另一个解答。对给定角CAB，如图作矩形$ADCE$，过点A取射线交CD于H，EC于F，使得$HF = 2CA$，此时AH即为所求。

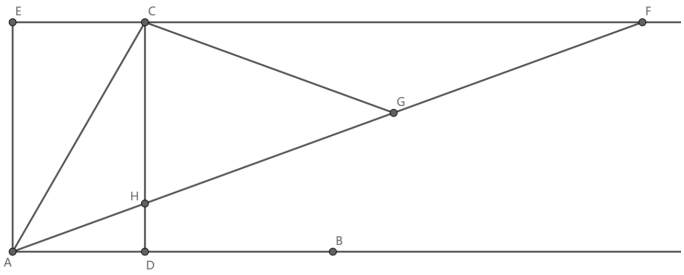


图 12: 帕普斯的做法

尼科米迪斯用蚌线也给出了解答，本质与欧几里得的做法相同，是利用蚌线确定了上文中符合条件的线BDE，不再赘述。

对于化圆为方问题，古希腊数学家狄诺斯特拉托斯使用割圆曲线提出了一种方法。割圆曲线定义如下：设$OABC$是边长为a正方形，OC绕O以固定角速度顺时针转动，同时BC以固定线速度向下移动，两者同时开始并且同时到达OA的位置，它们在运动过程中的交点轨迹即为割圆曲线。容易得到该曲线方程为$x = y\cot\dfrac{\pi y}{2a}(0 \le y \le 4)$。设曲线与$OA$的交点$M$，则$OM = \dfrac{2a}{\pi}$。进而

可以利用单位长度的线段构造出长为$\sqrt{\pi}$的线段，完成了该问题。但是割圆曲线本身并不能够通过尺规作图画出来。

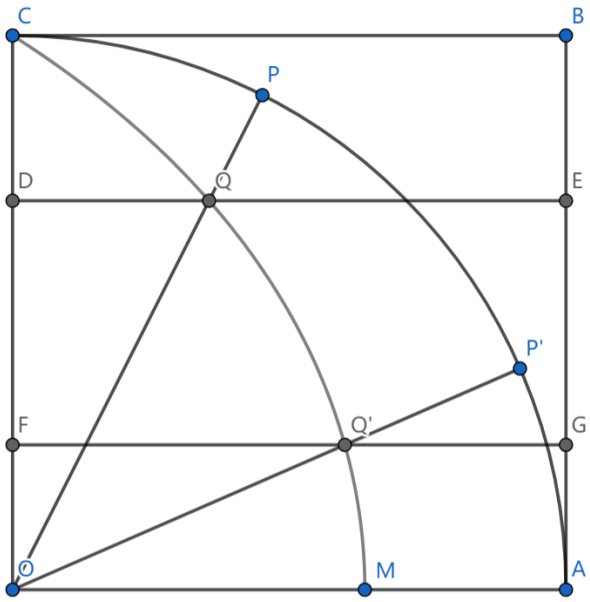


图 13: 割圆曲线

几何三大作图问题历经上千年，花费了无数数学家的心血，却始终没有真正解决。我们将在下文域论的讨论中解释尺规作图和域的联系，并给出几何三大问题不可解的证明。

三、 群论的历史

1、 群论的由来

直到大约十八世纪末，代数在很大程度上都是对多项式方程解法的研究。而到了二十世纪，代数成为抽象公理系统的研究。故事的转折点，即从所谓的古典多项式方程代数到所谓的现代公理系统代数的过渡发生在十九世纪。

在上文中，我们知道在公元前 1700 年左右，巴比伦人研究了如何解一元二次方程，利用的是补齐平方的方法。大约在 1540 年，人们给出了解三次方程和四次方程的代数方法。接下来两个世纪的主要问题之一是五次方程的解。这是拉格朗日在 1770 年的论文中为自己设定的任务。在这篇论文中，拉格朗日首先分析了韦达、笛卡尔、欧拉和裴蜀设计的各种已知求解三次方程和四次方程的方法。他指出，这些方法的共同特点是将这些方程简化为辅助方程，即所谓的预解方程，而后者比原始方程低一次。

具体而言，我们先定义：称 $f(x_1,x_2,\ldots,x_n)$ 是**对称多项式**，如果对任意 $1,2,\ldots,n$ 的排列 $j_1,j_2,\ldots,j_n$ 都有 $f(x_1,x_2,\ldots,x_n)=f(x_{j_1},x_{j_2},\ldots,x_{j_n})$。

对于多项式 $f(x_1,x_2,\ldots,x_n)$，考虑 $x_1,x_2,\ldots,x_n$ 在不同排列下有 m 种取值 $f_1,f_2,\ldots,f_m$，构造多项式 $g(y)=\prod\limits_{i=1}^{m}(y-f_i)=y^m+\sum\limits_{k=1}^{m}\left((-1)^k\sum\limits_{i_1<i_2<\cdots<i_k}f_{i_1}f_{i_2}\ldots f_{i_k}\right)y^{m-k}$，容易看出上式的系数都是对称多项式，且 $f_1,f_2,\ldots.f_m$ 是 $g(y)$ 的 m 个根。我们称 $g(y)$ 是**预解方程**，$f(x_1,x_2,\ldots,x_n)$ 为**预解式**。如果能解出预解方程的根，就可以获取关于原方程根的一些信息，最好的情况我们可以直接把原方程的根都求出来。

拉格朗日构造了如下 n 个预解式，称之为**拉格朗日预解式**：

$$L_k(x_1,x_2,\ldots,x_n)=x_1+\zeta^k x_2+\cdots+\zeta^{k(n-1)}x_n,k=0,1,2,\ldots,n-1$$

其中 $\zeta=e^{\frac{2\pi i}{n}}$ 是 n 次本原单位根。如果我们能得到 $L_0,L_1,\ldots,L_{n-1}$ 的取值，可以通过解线性方程组

$$\begin{cases}x_1+x_2+\cdots+x_n=L_0\\ \vdots\\ x_1+\zeta^k x_2+\cdots+\zeta^{k(n-1)}x_n=L_k\\ \vdots\\ x_1+\zeta^{n-1}x_2+\cdots+\zeta^{(n-1)^2}x_n=L_{n-1}\end{cases}\Longrightarrow\begin{cases}x_1=\dfrac{L_0+L_1+\cdots+L_{n-1}}{n}\\ \vdots\\ x_k=\dfrac{L_0+\zeta^{k-1}L_1+\cdots+\zeta^{(n-1)(k-1)}L_{n-1}}{n}\cdots(*)\\ \vdots\\ x_n=\dfrac{L_0+\zeta^{n-1}L_1+\cdots+\zeta^{(n-1)^2}L_{n-1}}{n}\end{cases}$$

得到 $x_1,x_2,\ldots,x_n$ 的取值。

图 14: 拉格朗日

例如，对于二次方程 $x^2-bx+c=0$ 的根 x_1,x_2，令 $L=x_1-x_2$ ，则 L 在 x_1,x_2 不同排列下有两种取值 $L,-L$，对应的预解方程 $g(y)=(y-L)(y+L)=y^2-(b^2-4c)=0$，解得 $y=\pm\sqrt{b^2-4c}$，不妨 y 取正号，结合 $x_1+x_2=b$ 解得 $\begin{cases} x_1=\dfrac{b+\sqrt{b^2-4c}}{2} \\ x_2=\dfrac{b-\sqrt{b^2-4c}}{2} \end{cases}$ 。

对于三次方程 $x^3-bx^2+cx-d=0$ 的根 x_1,x_2,x_3，令 $L=x_1+\zeta x_2+\zeta^2x_3$，$R=x_1+\zeta^2x_2+\zeta x_3$，其中$\zeta=e^{\frac{2i\pi}{3}}$是 3 次本原单位根。则 L 在 x_1,x_2,x_3 不同排列下有六种取值 $L,\zeta L,\zeta L^2,R,\zeta R,\zeta^2R$，预解方程 $g(y)=(y-L)(y-\zeta L)(y-\zeta^2L)(y-R)(y-\zeta R)(y-\zeta^2R)=0$。注意到 $1+\zeta+\zeta^2=0$，带入展开式得 $g(y)=y^6-(L^3+R^3)y^3+L^3R^3=0$，这是一个关于 y^3 的二次方程。

设 $L^3+R^3=B,L^3R^3=C$ ，则 $L^3,R^3=\dfrac{B\pm\sqrt{B^2-4C}}{2}$(不妨 L^3 取正号，R^3 取负号)。于是有 $\begin{cases} L=\zeta^j\sqrt[3]{\dfrac{B+\sqrt{B^2-4C}}{2}},j=0,1,2 \\ R=\zeta^k\sqrt[3]{\dfrac{B+\sqrt{B^2-4C}}{2}},k=0,1,2 \end{cases}$ 。注意到 LR 是对称多项式，设它的值为 A。

若 $A=0$ ，则原方程恰好可以凑成完全立方 $\left(x-\dfrac{b}{3}\right)^3=B$，解得 $\begin{cases} x_1=\dfrac{b}{3}+\sqrt[3]{B} \\ x_2=\dfrac{b}{3}+\zeta\sqrt[3]{B} \\ x_3=\dfrac{b}{3}+\zeta^2\sqrt[3]{B} \end{cases}$ 。

若 A 不为 0 ，则只有三组 (j,k) 能满足 $LR=A$ ：$\begin{cases} L=\zeta^i\sqrt[3]{\dfrac{b+\sqrt{b^2-4c}}{2}} \\ R=\dfrac{A}{\zeta^i\sqrt[3]{\dfrac{b+\sqrt{b^2-4c}}{2}}} \end{cases}$ ，$i=0,1,2$。

由 $(\cdot *)$ 可以解得 $\begin{cases} x_1 = \dfrac{b+L+R}{3} \\ x_2 = \dfrac{b+\zeta^{-1}L+\zeta^{-2}R}{3} \\ x_3 = \dfrac{b+\zeta^{-2}L+\zeta^{-4}R}{3} \end{cases}$，即 $\begin{cases} x_1 = \dfrac{1}{3}\left(b + \sqrt[3]{\dfrac{b+\sqrt{b^2-4c}}{2}} + \dfrac{A}{\sqrt[3]{\dfrac{b+\sqrt{b^2-4c}}{2}}}\right) \\ x_2 = \dfrac{1}{3}\left(b + \zeta^{-1}\sqrt[3]{\dfrac{b+\sqrt{b^2-4c}}{2}} + \dfrac{A}{\zeta^{-1}\sqrt[3]{\dfrac{b+\sqrt{b^2-4c}}{2}}}\right) \\ x_3 = \dfrac{1}{3}\left(b + \zeta^{-2}\sqrt[3]{\dfrac{b+\sqrt{b^2-4c}}{2}} + \dfrac{A}{\zeta^{-2}\sqrt[3]{\dfrac{b+\sqrt{b^2-4c}}{2}}}\right) \end{cases}$

对于四次方程而言解法略有不同。设方程 $x^4 - bx^3 + cx^2 - dx + e = 0$ 的根 x_1, x_2, x_3, x_4，令 $L = x_1 - x_2 + x_3 - x_4$，$L^2$ 在 x_1, x_2, x_3, x_4 不同排列下有三种取值 $\begin{cases} f_1 = (x_1 - x_2 + x_3 - x_4)^2 \\ f_2 = (x_1 - x_2 - x_3 + x_4)^2 \\ f_3 = (x_1 - x_2 + x_3 - x_4)^2 \end{cases}$，对应的预解方程 $g(y) = (y - f_1)(y - f_2)(y - f_3) = 0$ 是三次方程，因此可以解出 f_1, f_2, f_3 的值。

进而有 $\begin{cases} x_1 + x_2 + x_3 + x_4 = b \\ x_1 - x_2 + x_3 - x_4 = \pm\sqrt{f_1} \\ x_1 - x_2 - x_3 + x_4 = \pm\sqrt{f_2} \\ x_1 + x_2 - x_3 - x_4 = \pm\sqrt{f_3} \end{cases}$，不妨全部取正号得到 $\begin{cases} x_1 = \dfrac{b+\sqrt{f_1}+\sqrt{f_2}+\sqrt{f_3}}{4} \\ x_2 = \dfrac{b-\sqrt{f_1}-\sqrt{f_2}+\sqrt{f_3}}{4} \\ x_3 = \dfrac{b+\sqrt{f_1}-\sqrt{f_2}-\sqrt{f_3}}{4} \\ x_4 = \dfrac{b-\sqrt{f_1}+\sqrt{f_2}-\sqrt{f_3}}{4} \end{cases}$。

尽管该方法无法解五次方程，但拉格朗日的工作是一块里程碑：这是第一次将多项式方程的解与方程根的排列联系起来。拉格朗日推测，这构成了“解方程的真正原理”。当然，伽罗瓦后来证明了他的想法是正确的。虽然拉格朗日在谈到排列时没有考虑排列的“计算”，但可以说，在他的著作中存在着群概念的萌芽——即置换群。

在十八世纪，高斯在他的《算术研究》中总结并统一了他之前的许多数论，它可以说开创了有限阿贝尔群理论。事实上，高斯在没有使用任何群论术语的情况下，就建立了这些群的许多重要性质。这些群以四种不同的面貌出现：整数模n的加法群、整数模n的乘法群、二元二次型的等价类群以及n次单位根群。虽然这些例子是在数论背景下出现的，但高斯是把它们作为阿贝尔群来处理的，并使用了现代代数证明的明显原型。

例如，他证明了这些非零整数在模p(是素数)意义下都是同个元素的幂，也就是说，群 $\mathbb{Z}_p^*$ 是循环群。此外，他还证明了这个群的生成元个数为 $\varphi(p-1)$，其中 φ 是欧拉函数。

给定 $\mathbb{Z}_p^*$ 的任何元素，他定义了元素的阶(没有使用术语)，并证明了元素的阶次是 $p-1$ 的因数。然后，他利用这一结果证明了费马小定理，即如果 p 不整除 a，则 $a^{p-1} \equiv 1(modp)$。接着，他证明了如果 t 是 $p-1$ 的正因子，那么在 $\mathbb{Z}_p^*$ 中存在一个阶为 t 的元素——本质上是循环群上

的拉格朗日定理的逆定理。

关于 1 的 n 次方根(他在研究分圆方程时考虑了这些根)，他证明它们也构成一个循环群。关于这个群，他提出并回答了许多与他在 $\mathbb{Z}_p^*$ 的情况下提出并回答的相同问题。他也证明了所有形式为 $4n+1$ 的素数都可以表示为两个平方 x^2+y^2 之和。

高斯在《算术研究》中用了很大篇幅来详尽研究二元二次型和用二元二次型表示整数。二元二次型是形式为 $ax^2+bxy+cy^2$ 的表达式，其中 a、b、c 为整数。高斯定义了这种二次型的复合，并证明了这种复合使之构成了阿贝尔群。

尽管高斯具有这些非凡的洞察力，但我们不认为他具有群的概念，他所考虑的各种类型的“群”都是分别处理的，没有一种统一的群论方法可以适用于所有情况。

十九世纪见证了几何学在广度和深度上的爆炸式发展。新的几何学出现了：投影几何学、非欧几里得几何学、微分几何学、代数几何学、n 维几何学，以及格拉斯曼的外延几何。各种几何方法竞相争雄：合成法与解析法、度量法与射影法。世纪中期，出现了一个重大问题，即对不同几何图形和几何方法之间的关系和内在联系进行分类。这就产生了“几何关系”的研究，其重点是研究在变换下不变的图形的属性。很快，研究重点转移到了对变换本身的研究。因此，对图形几何关系的研究变成了对相关变换的研究。各种类型的变换成为专门研究的对象。

克莱因于 1872 年在被 Erlangen 大学录取时发表演讲，意在将几何学归类为研究各种变换下的不变量。在这演讲里，出现了射影群、刚体运动群、相似群、双曲群、椭圆群等群，以及与之相关的几何图形。随后，人们开始研究变换之间的逻辑联系，并由此提出了变换的分类问题，最终形成了克莱因的群论几何综合。

图 15: 克莱因

1874 年，李提出了连续变换群的一般理论——基本上就是我们今天所说的李群。这样的群由

变换 $x_i^1 = f_i(x_1, x_2, \ldots, x_n, a_1, a_2, \ldots, a_n)$表示，$i = 1, 2, ..., n$。其中 f_i 是 x_i 和 a_i 的解析函数(a_i 是参数，x_i 和 a_i 都是实数或复数)。例如，$x_1 = \dfrac{ax + b}{cx + d}$，其中 a, b, c, d 均为实数，$ad - bc \neq 0$给出的变换定义了一个连续变换群。

李认为自己是阿贝尔和伽罗瓦的继承者，在微分方程上完成了他们在代数方程上的工作。他的工作灵感来自于一个观察结果，即几乎所有用老方法求解的微分方程，在容易构造的连续群下都保持不变。于是，他开始考虑在给定连续群下保持不变的微分方程的一般情况，并研究这些方程中可能存在的、由给定群的已知性质(参见伽罗瓦理论)引出的结论。

他的工作对后来 Picard 和 Vessiot 提出的“微分方程伽罗瓦理论”至关重要。

2、 群论的发展

在上一节中，我们概述了群论演变的四个主要来源。第一个来源是经典代数，它引出了置换群理论；第二个来源是数论，引出了阿贝尔群理论；第三和第四个来源是几何和分析，引出了变换群理论。现在，我们将概述这些专门理论的一些发展。

如前所述，拉格朗日于 1770 年发表的著作开创了与方程求解研究相关的排列研究。这可能是数学中隐含群论思想的第一个明确实例，它直接影响了十九世纪 Ruffini、Able 和 Galois 的著作，以及置换群的概念。Ruffini 和 Able 以拉格朗日的预解式思想为基础，证明了五次方程的不可解性。拉格朗日证明，一般的 n 次多项式方程可解的一个必要条件是存在一个小于 n 次的预解式。他们证明了当 $n > 4$ 时，这样的预解式是不存在的。在此过程中，他们发展了置换群理论。然而，在概念上取得根本性进展的是 Galois ，他被许多人视为(置换)群理论的创始人。

伽罗瓦是第一个在技术意义上使用“群”这一术语的人，对他来说，“群”意味着在乘法下封闭的排列集合：“如果一个人在同一个组中有 S 和 T 的置换，就一定会有 ST 的置换。”

群的严谨叙述的定义如下：

在非空集合 G 上定义了运算 $\cdot$ 满足如下性质：

(1)封闭性，即对任意 $a, b \in G$，有 $a \cdot b \in G$。

(2)结合律，即对任意 $a, b, c \in G$，有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$。

(3)存在单位元 $e \in G$，即满足对任意 $a \in G$，$a \cdot e = e \cdot a = a$。

(4)对任意 $a \in G$ 在逆元 a^{-1}，即满足 $a \cdot a^{-1} = a^{-1} \cdot a = e$。

则称 G 关于运算 $\cdot$ 构成群，记为 $(G, \cdot)$，或简记为 G。

在上文中提到的置换群就是在 $1, 2, \ldots, n$ 所有排列上定义了复合运算。

伽罗瓦认识到，代数方程最重要的性质反映在与方程唯一相关的群的某些性质中——”方程的群”。为了描述这些性质，他发明了正规子群这一基本概念，并将其运用得炉火纯青。

正规子群的定义如下：

群 G 的子群 N (即 N 作为集合是 G 子群且构成群) 满足：

对任意的 $g \in G$，$gN = Ng$，即 $\left\{gn \middle| n \in N\right\} = \left\{ng \middle| n \in N\right\}$。

进而我们可以定义**商群** $G/N = \left\{aN \middle| a \in G\right\}$。

虽然拉格朗日、拉夫尼和阿贝尔一直在关注预解方程的问题，但伽罗瓦的基本想法是绕过他们，因为预解方程的构造需要高超的技巧，而且并不基于明确的方法。伽罗瓦指出，预解方程的存在等同于方程组中存在一个素指数的正规子群。

十九世纪上半叶置换群理论的另一个主要贡献者是柯西。在 1815 年和 1844 年的几篇重要论文中，他开创了置换群理论作为一门自主学科。在柯西之前，置换不是独立研究的对象，而是研

究多项式方程解的有用工具。尽管柯西很清楚拉格朗日和鲁菲尼的工作(伽罗瓦的著作当时尚未发表)，但他“绝对没有直接受到当代代数方程可解性问题的群论表述的启发”。

这两条发展路线的最高成就——关于伽罗瓦和柯西宏大主题的交响曲——是 Jordan 在 1870 年发表的重要而有影响力的《关于替代和代数方程的论文》。尽管作者在序言中说“这项工作的目的是发展伽罗瓦的方法，并通过展示它能用什么手段解决方程理论的所有主要问题，使它成为一个适当的研究领域”，但事实上，群论本身——而不是作为方程可解性理论的一个分支——构成了研究的中心对象。

在 Jordan 看来，(置换)群的概念提供了这样一个关键的想法。他的方法使他能够统一介绍伽罗瓦、柯西和其他人的结果。他将群概念应用于方程理论、代数几何和理论力学。他的目标是按置换群理论已经应用或似乎可能适用的领域对所有数学进行调查。

这篇论文体现了 Jordan 当时关于群体的大多数出版物的实质内容(在 1860 年至 1880 年期间写了 30 多篇关于群的文章)，并将注意力引向了大量难题，引入了许多基本概念。例如，他明确了群的同构和同态的概念，首次在技术意义上引入了术语“可解群”。

他对置换群进行了非常彻底的研究，获得了许多结果，例如证明了 n 元奇置换群 A_n 对于 $n > 4$ 是单群的。这篇论文的一个重要部分是专门研究“线性群”及其一些子群。用现代术语来说，它们构成了所谓的典型群，即一般线性群、酉群、正交群和辛群。Jordan 只在有限域考虑了这些群，并在某些情况下证明了它们的单性。然而，应该指出的是，他将这些群视为置换群，而不是矩阵组或线性变换。

Jordan 的论文是群论发展的一个里程碑。然而，他试图通过依靠置换群的概念来实现这样的综合，而数学发展的下一阶段将证明它受到了限制。

如前所述，阿贝尔群论的主要来源是数论，从高斯的《算术论》开始。与置换群理论相比，数论中的群论思维方式一直隐含在其中，直到19世纪后期才显露出来。在这之前，还没有明确使用“群”这个术语，并且没有与当代繁盛的置换群理论建立联系。

代数数论起源于费马大定理——不定方程 $x^n + y^n = z^n (n > 2)$ 的不可解性、高斯的二元二次型理论和更高次的互反律(见下一章)。代数数域及其算术性质是主要研究对象。

1846年，狄利克雷研究了代数数域中的单位元，并确定这些单位元群是有限循环群和有限秩的自由阿贝尔群的直接乘积。大约在同一时间，Kummer 引入了他的“理想数”，定义了它们的等价关系，并为循环域推导出了等价类数的某些特殊性质，即循环域的理想类群的阶数。狄利克雷早些时候对二次域进行了类似的研究。1869年，高斯的前学生先灵研究了二元二次形式的高斯等价类的结构。他发现了某些基本类，从中可以通过组合获得所有类的形式。在群论方面，Schering 找到了二元二次型等价类的阿贝尔群的基。

Kronecker 将 Kummer 在循环场方面的工作推广到任意代数数域。在 1870 年一篇关于代数数论的论文中，他考虑了一组有限的任意“元素”，并定义了满足某些定律的抽象操作——我们今天可以把这些定律作为有限阿贝尔群的公理。

尽管 Kronecker 没有将他对有限阿贝尔群的隐含定义与他当时公认的置换群概念联系起来，但他清楚地认识到他所采用的抽象观点的优点：简洁。

1879 年，Frobenius 和 Stickelberger 发表了一篇题为“关于交换群”的重要论文，对上述发展路线进行了限制。尽管他们建立在 Kronecker 的工作基础上，但他们明确地使用了阿贝尔群的概念，而且，在认识到抽象群概念包含同余和高斯的形式组合以及伽罗瓦的置换群方面取得了重要进展。他们的主要成果之一是证明了有限阿贝尔群的基本定理，包括对唯一分解性的证明。

他们继续研究素数幂的循环群的“不可约因子”。然后，他们将结果应用于代数数域中的整数模 m 、二元二次型和理想类。Frobenius 和 Stickelberger 的论文是一项了不起的工作，以接近现代观点的方式在自己的基础上建立了一个独立的有限阿贝尔群理论。

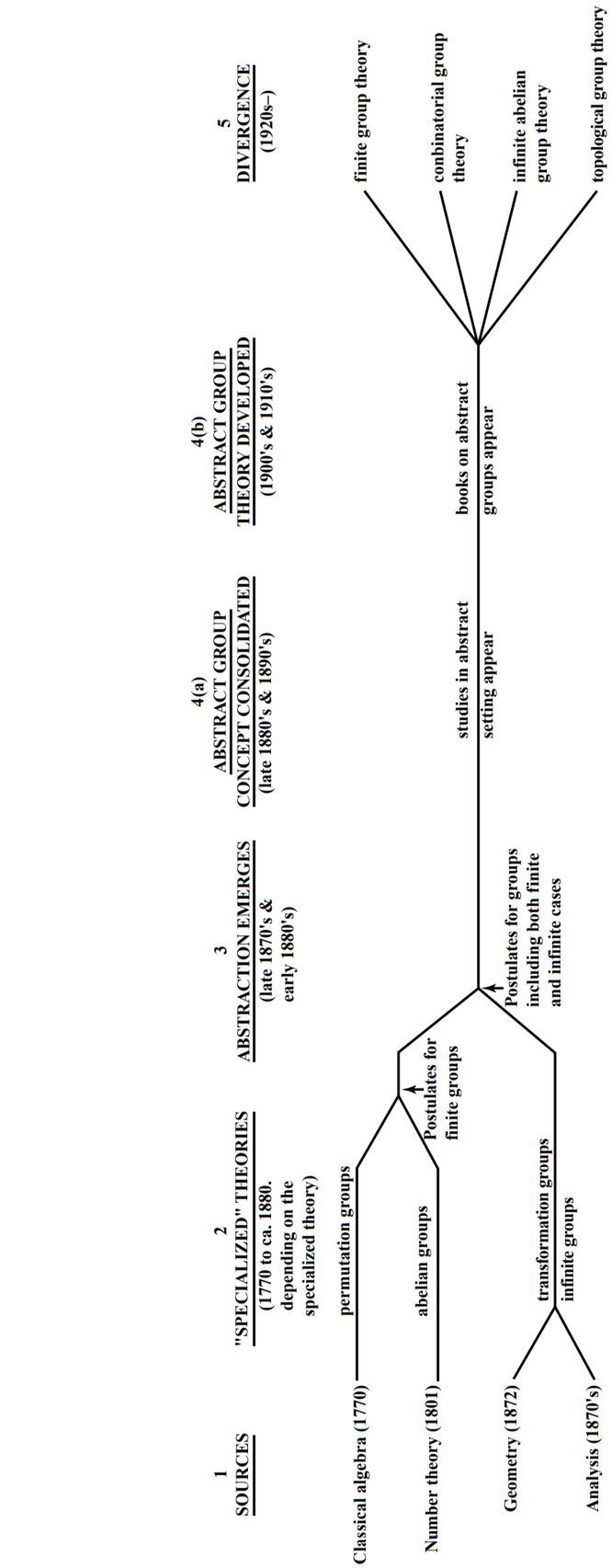
就像在数论中一样，在几何学和分析学中，群论思想一直隐含到十九世纪的最后三分之一。此外，Klein 在几何学中对群的明确使用在概念上而不是在技术上影响了群论的演变。它标志着群论发展的真正转变，从对置换群的关注转向对变换群的研究。这种转变也值得注意，因为它指出了从有限群到无限群的转变。

在 1860 年代后期，Klein 和 Lie 共同致力于“研究通过变化群转化为自身的几何或分析对象”。Klein 专注于离散群，而 Lie 则研究连续变换群。Lie 意识到连续变换群理论是几何学和微分方程中非常强大的工具。几年前，Poincaré 和 Klein 给出了不连续变换群的分类。

群论中的抽象观点慢慢出现。从拉格朗日 1770 年的隐含群论的工作开始，抽象群概念才得以发展，历时一百多年。基于抽象群概念的群论专著直到二十世纪初才出现。它们的出现标志着抽象群论的诞生。群论是从几个不同的来源演变而来的，产生的各种理论从 1770 年开始独立发展，有些理论持续了一百多年，直到1880年代初才汇聚在抽象群概念中。

最早专门讨论抽象群的专著是 J. A. de Séguier 于 1904 年出版的《Elements of the Theory of Abstract Groups》一书，这本书没有直观的考虑，并主要致力于有限群。第一本关于群论的抽象专著是 O. J. Schmidt 在1916年出版的《Abstract Theory of Groups》。他在本书的前四章专门讨论了有限群和无限群共有的群性质。

从 1880 年代开始到接下来的三十到四十年中，抽象群概念得到巩固，并在大约在 1920 年左右，人们可以看出群论分裂为几个不同的“理论”。


1
SOURCES
2
"SPECIALIZED" THEORIES
(1770 to ca. 1880.
depending on the
specialized theory)
3
ABSTRACTION EMERGES
(late 1870's &
early 1880's)
4(a)
ABSTRACT GROUP
CONCEPT CONSOLIDATED
(late 1880's & 1890's)
4(b)
ABSTRACT GROUP
THEORY DEVELOPED
(1900's & 1910's)
5
DIVERGENCE
(1920s–)
Classical algebra (1770)
permutation groups
Number theory (1801)
abelian groups
Geometry (1872)
transformation groups
Analysis (1870's)
infinite groups
Postulates for
finite groups
Postulates for groups
including both finite
and infinite cases
studies in abstract
setting appear
books on abstract
groups appear
finite group theory
combinatorial group
theory
infinite abelian
group theory
topological group theory

四、 环论的历史

1、 交换环论的由来

追根溯源，从 19 世纪开始，交换环论开始萌生。代数数论、代数几何和不变量理论是交换环论的主要来源，而且交换环论的发展和逐步成熟亦与这三大学科息息相关。随着它们相互作用和共同影响，其研究内容不断丰富，理论层次不断上升，最终形成了愈发严谨并充满生命力的现代数学理论。

代数数论

在 19 世纪之前，高次互反律一直是数论的核心，其中的关键是唯一因子分解问题。高斯在欧几里得、拉格朗日、欧拉和勒让德等数学家的研究基础上，为了寻求建立唯一因子分解，引入了复整数。

图 16: 高斯

从上文我们能看到，求解多项式方程是代数中的重要问题，与之类似的，数论中的一个重要问题是求解形如 $a_0 + a_1x + \cdots + a_mx^m \equiv 0(\mathrm{mod}\ n)$的同余多项式方程。当 m 为任意数时，求解这个方程会变得十分困难。

1801 年，高斯在《算术研究》里探讨了二次同余方程 $a_0 + a_1x + a_2x^2 \equiv 0(\mathrm{mod}\ n)$，并研究了 p 和 q 都是奇素数的同余式 $x^2 \equiv q(\mathrm{mod}\ p)$，他证明了，当 $q \equiv p \equiv 3(\mathrm{mod}\ 4)$ 时，同余式 $x^2 \equiv q(\mathrm{mod}\ p)$ 可解当且仅当 $x^2 \equiv p(\mathrm{mod}\ q)$ 可解；若不然，同余式 $x^2 \equiv q(\mathrm{mod}\ p)$ 可解当且仅当 $x^2 \equiv p(\mathrm{mod}\ q)$ 不可解。这就是我们现在说的二次互反律。

记勒让德符号 $\left(\frac{p}{q}\right)=\begin{cases}0\text{，}q\mid p\\1\text{，方程}x^2\equiv p(\mathrm{mod}\ q)\text{可解}\\-1\text{，方程}x^2\equiv p(\mathrm{mod}\ q)\text{不可解}\end{cases}$。

那么我们就有高斯的二次互反律：

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

之后高斯便意在解决互反律的高次情形。为了简洁地叙述四次的互反律，高斯在 1829 年和 1831 年的两篇文章中引入了高斯整数，即形如 $a+ib$ 的复数，其中 a,b 是整数，$i^2=-1$。将复整数的全体记作 $\mathbb{Z}[i]$，它的加、减、乘运算封闭，故构成了所谓的**环**。在此我们叙述环的严谨定义如下：

在非空集合 R 上定义了运算 $+$ 和 $\cdot$ 分别称为加法和乘法满足如下性质：

(1) R 对加法是一个 Able 群(这样 R 有零元素，记为 0)

(2)乘法结合律：$(x\cdot y)\cdot z=x\cdot(y\cdot z)$

(3)乘法分配律：$x\cdot(y+z)=x\cdot y+x\cdot z,(y+z)\cdot x=y\cdot z+z\cdot x$

(4)对乘法具有单位元(记为 1)

则称 R 关于运算 $+$ 和 $\cdot$ 构成环，记为 $(R,+,\cdot)$，或简记为 R。

容易验证 $\mathbb{Z}[i]$ 是满足如上定义的。

对于环 R 而言，$x\in R$ 称为**零因子**，如果$\exists y\in A,y\neq 0,xy=0$。

没有非零零因子(且$1\neq 0$)的环叫做**整环**。

我们知道在整数中有一个基本定理，就是每一个大于 1 的整数都可以被分解成素数的乘积，并且这个分解是唯一的。

在 19 世纪中期，Jacobi 和 Eisenstein 相继得到了三次互反律，这一结果是在整环 $\mathbb{Z}[\rho]=\left\{a+b\rho\middle|a,b\in\mathbb{Z}\right\}$ 上进行研究得出的。其中 ϕ 是 1 的三次本原单位根。数学家们进一步寻求高次互反律，但必须要有新的方法来研究不同于以 $\mathbb{Z}[i],\mathbb{Z}[p]$ 的情况，亦即利用其他算术域来阐述不满足唯一分解整环的互反律。

1637 年，费马在阅读古希腊数学家丢番图的代表性著作《算术》时，在书的空白处写下：把一个立方数分为两个立方数的和，或者把一个四次幂分为两个四次幂的和，或者更一般地，把一个高于二次的幂分为两个同次幂的和，这是不可能的。对于这个结论，我已经确定找到了一种好的方法来证明，无奈空白处甚小无法写下来。

费马所叙述的定理可以表述为：

当 $n>2$ 时，关于 x,y,z 的不定方程 $x^n+y^n=z^n$ 不存在正整数解。

这个定理被称为费马大定理或费马最后定理.这个定理经历了 300 多年，才由英国数学家维尔斯证明。在这个历史过程中，有很多新的数学结果和数学分支华丽诞生。

当 $n = p$ 为素数时，这个方程可以分解成 $(x + y)(x + y\omega) \dots (x + y\omega^{p-1}) = z^p$，其中 ω 是 1 的 p 次本原单位根，从现代数学的观点来看，我们就可以得到，分解后的方程是分圆整数环 $D_p = \left\{ a_0 + a_1\omega + \cdots + a_{p-1}\omega^{p-1} \middle| a_i \in Z, i = 1, 2, \dots, p-1 \right\}$ 上的一个方程。因此，若 D_p 是唯一因子分解整环，假设原方程有解，通过递降法来推得矛盾，最终证明费马大定理。但令人遗憾的是，D_p 不总是唯一因子分解整环，例如 $D_2 3$ 就不是。其实，从以上的讨论我们已经可以看到，这一时期证明费马大定理的方法，就是将不定方程看作是 D_p 中的方程，这个方法具有示范意义。

库默尔在 1846 年首次发表了他的理想数理论成果。库默尔将分圆整数分解为其素因子的乘积，如果素因子不存在，就引进理想素因子，从而证明了在普通数论中成立的某些结果也在分圆数域当中成立。库默尔由此阐述和证明了一个非常一般的高次互反律，也同时使得费马大定理的研究迈出了关键性的一步。

戴德金在狄利克雷《数论讲义》的附录中，先给出了代数数域的整数环、理想和素理想等的定义。戴德金还研究了代数数域的分歧理论，定义基本理想，即共辄差集，得出两条主定理他还得到一个模的关键结果，这对抽象理想论的意义非同一般。它就是升链条件 (the ascend chain condition) 及其证明。

总之，戴德金引入了交换代数的一些最为基本的概念，他还得出了代数数论的重要结果之一，即把代数数域的整环中的理想唯一表示成素理想的乘积.后来这个理论在代数曲线的研究中也有重要作用。

1892 年至 1899 年期间，希尔伯特主要研究代数数论，博采众长，他学习戴德金、克罗内克以及韦伯的作品，在学习的同时，开展数学研究和探索。1893 年，希尔伯特在慕尼黑举办的德国数学年会上公布了他所取得的第一个数论成果，对素理想的因子分解定理给出了新的证明。这个结果得到了数学家们的一致认可。1897 年 4 月，希尔伯特又公开发表了其成果《代数数域理论》。

在他的这份报告中，在统一的高观点之下，代数数论成为一个具有严密性结构和形式的数学整体。他所用的方法新颖而有力，他引进了一些新的概念，给出了一些新的定理，实际上描画出了一幅代数数论的宏伟图景。希尔伯特对环的研究工作不管是对代数数论，还是对抽象代数学都产生了不可忽视的作用。希尔伯特所主张的公理化思想，进一步促使数学家们运用公理化体系来给出数学理论的定义，同时对环定义的抽象化是一种有益的铺垫。

代数几何

交换环论的另一个起源是代数几何。代数几何研究代数曲线以及代数曲线的 n 维推广，也就是代数簇。代数曲线相当于是由代数函数的根所组成的集合，也就是由一个多项式方程 $P(x,y)=0$ 所定义的 $y=f(x)$。从这里可以看出几何与代数之间的对应关系。因此有些几何的问题和代数的问题是可以相互借鉴和转化的。

在历史上研究代数曲线的方法很多，其中主要的方法有解析方法、几何代数方法和代数算术方法。

对于黎曼而言，他通过引入黎曼面的概念，使得黎曼面上的代数函数成为单值函数。而在 19 世纪六七十年代，克莱布什、戈丹和布里尔，特别是诺特的父亲马克斯·诺特引入了几何代数方法，用来研究代数函数和代数曲线。

黎曼的解析方法和马克斯·诺特等人的几何代数方法虽各有优点，但都未能给代数函数论建立起严格的基础。

戴德金和韦伯在 1882 年发表了《单变量的代数函数理论》一文，已做好为代数函数域 K 上的黎曼曲面 S 给出一个严格的代数定义的准备工作，把黎曼的关于代数函数的思想大部分以代数形式严格地发展出来。

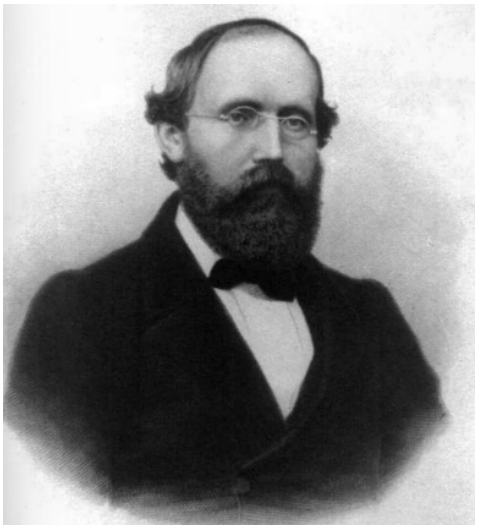


图 17: 黎曼

在历史上，代数学基本定理将代数和几何之间建立了联系，表明在复数域上的单变量的多项式由其根的集合来决定，而根的集合属于内在的几何对象。希尔伯特基定理指出有有限多方程满足这个条件，但由不同的多项式方程组可能会得到相同的根的集合。

希尔伯特零点定理给出了多项式环的理想与仿射空间子集的基本对应。利用零点定理和相关结果，我们可以用代数概念来解释簇的几何概念，也可以用几何来说明环论中的一些问题。

在现代的交换代数里，一个交换环 R 中的理想 Q 如果满足 $R/Q \neq (0)$，并且其中每个零除数均为幂零的，那么就可以称为准素理想。任意的素理想均为准素理想，在整数环中，准素理想对应着素数的幂。

拉斯克尔首先定义了准素理想，把准素理想作为素理想的推广，认为准素理想与素理想的关系就如同整环中素数幂与素数的关系。拉斯克尔是受到了库默尔、戴德金、克罗内克对理想论的贡献，希尔伯特关于不变量的工作以及马克斯·诺特和其他数学家对代数几何的贡献的影响，并把这些数学家的成果吸收和创新的。

在拉斯克尔和麦考莱的工作基础之上，希尔伯特对多项式理想论也有一些成果，体现在他关于不变量的工作上。下面我们将介绍希尔伯特在不变量方面的一些创新思想，从而更深刻地理解交换环论的源起。

不变量理论

交换环论的第三个重要来源是不变量理论. 前面我们已经涉及了关于它的一些内容. 不变量理论主要起源于 19 世纪下半叶的数论和几何, 当时英国和德国的数学家对其怀有高度的研究热情, 并身体力行, 付诸实施.

实际上, 如果要追溯它的历史, 可以更早地追溯到高斯在《算术研究》中对二元二次型的研究. 高斯定义了二元二次型的一个等价关系, 并且证明在此等价关系下判别式是型的不变量. 这是不变量理论在数论中的最早来源.

不变量理论的另一个重要来源为几何, 准确地说是射影几何. 射影几何可以追溯到 19 世纪 20 年代, 其重要问题是区分几何图形的欧氏性质和射影性质. 实际上, 射影性质就是在射影变换下保持不变的一些性质. 这些都是不变量理论的初步萌芽阶段.

而不变量理论真正建立起来, 也就是从形式上建立起来, 则要从 1845 年凯莱和西尔维斯特出版第一本相关著作算起。凯莱发现了射影几何与度量几何之间的紧密联系. 他们二人在研究拉格朗日的齐次多项式的线性变换时, 对不变量进行了详细描述。整个 19 世纪以及 20 世纪的初期, 不变量理论和几何学是密切联系在一起的, 但到 19 世纪下半叶已成为代数学的一个重要分支。

设 $f(x_1, x_2)$ 是一个系数为 $a_i (1 \leqslant i \leqslant n)$ 的 n 次齐次二元型。设 T 是一个满足下列两个条件的变换：

$$x_1 = a_{11}y_1 + a_{12}y_2,$$

$$x_2 = a_{21}y_1 + a_{22}y_2,$$

令这个变换的行列式 $\delta = a_{11}a_{22} - a_{12}a_{21}$。这个变换实际上定义了一个新的关于变量 y_1, y_2 的 n 次型，$T(f) = F(y_1, y_2)$，这个新的型的系数 $b_i (1 \leqslant i \leqslant n)$ 是有理函数。

现在，一个不变量是 f 的系数 a_i 的任意一个函数 I，使得对于某一个整数 r，有

$$I(b_1, b_2, \cdots, b_n) = \delta^r I(a_1, a_2, \cdots, a_n).$$

这个定义可推广到三元型、四元型或更一般的 n 元型，也可推广到几个不同的不变量，或者是系数的不变量和共变量。

实际上，不变量理论中的一个重要问题就是找出各种型的不变量。19 世纪后半叶许多大数学家都在计算特殊型的不变量。这就引出了不变量理论中的主要问题，即对给定的型确定其不变量的一个完备系——基，使得其他每一个不变量都可表示成这些不变量的组合。人们猜想这个结论对有限个不变量可能成立。

1868 年，戈丹运用这些方法，证明了二元型的有限性定理。他证明了，对于任意次数的二元型的一个系统，我们可以选它的一个有限子系统，使得前者的任意一个不变量可以写成后者的有理组合。他用这种方法，通过烦冗的运算，给出了五次和六次的二元型的可能的最小的基本型系统。也就是说，戈丹用计算方法证明了任意次数的二元型都有一组有限基，且给出了不变量的一个完备系。

之后，人们证明了戈丹定理的各种不同的有限推广，也有人改进了他的证明。与此同时，计算不变量的方法也有了重大改进。但是，戈丹定理的完全推广仍是一个开放性问题：在任意一个有任意多个未定元和任一次数的不变量系统里，存在一个有限基。这是希尔伯特不变量研究的起点。

给定整数环上的两个二元二次型 $f = ax^2 + bxy + cy^2$ 和 $f_1 = a_1x_1^2 + b_1x_1y_1 + c_1y_1^2$，在线性变换 $x = px_1 + qy_1$ 及 $y = rx_1 + sy_1$ (其中 $ps - qr = 1$) 下，如果 f 能变成 f_1，高斯称 f 与 f_1 等价。等价的二次型代表着相同的整数集。另外，f 与 f_1 的判别式 $D = b^2 - 4ac$ 和 $D_1 = b_1^2 - 4a_1c_1$ 也相等。这时就说判别式是二次型在行列式为 1 的线性变换下的不变量。

19 世纪上半叶，射影几何、双曲几何、黎曼几何、代数几何等新几何不断涌现。数学家试图通过准确地描述不同类型几何的特征来区分它们，而在多种变换下的不变性质成为重要的研究工具，对它们的研究很快导向了克莱因的爱尔朗根纲领。比如，几何图形的射影性质是在线性变换下的不变量，而代数几何性质则是在双有理变换下的不变量。

如前所述，19 世纪中叶，不变量理论与数论和几何分开，成为独立的研究领域。实际上，19 世纪 60 年代到 80 年代期间，它已经成为代数学的重要分支，找到不同形式的特定不变量以及不变量的完备系成为数学家们追逐的焦点。

1888 年，希尔伯特发表了一个全新的概念性方法来解决不变量问题，震惊了整个数学界。其思想是考虑有限个变量的表达式而不是考虑不变量，简而言之，就是考虑这些变量的多项式环。

1910——1920 年，诺特在不变量理论方面得到了几个著名的结果。她从 1915 年和 1916 年关于不变量理论的两篇论文中发展出了新方法，并借此对戴德金最先提出的对于具有给定伽罗瓦群的数域找出其伽罗瓦扩张的问题的解决作出贡献。诺特被戴德金的方法和思想吸引，取得了一些突出成就，这便是她接下来的研究方向，即交换环论。

2、 非交换环理论

19 世纪早期，环论开始萌芽，许多交换环和非交换环的具体案例就源于这个时期。环有两种运算，一种是加法运算，另一种是乘法运算。环并不一定满足结合律与交换律。按照环是否满足结合律，可以把环分为结合环与非结合环。结合环主要包括结合代数、矩阵和群代数，其中，结合代数是由复数、四元数和超复数推广得到的，矩阵是由线性方程组和行列式发展得到的，群代数则是超复数系与群表示论相结合的产物。非结合环主要包括交错代数、李环和若尔当代数。其中，交错代数起源于八元数和双四元数，李环起源于李变换群、李代数，若尔当代数起源于量子力学。按照环是否满足交换律，可以把环分为交换环和非交换环。二者都是在 19 世纪开始进入数学的，但其实践基础却是大不相同的。

因为非交换环论远比交换环论丰富，所以相较而言，其结构和性质为人所知较少，不过，现在已有交换环的一些结果被成功地推广到非交换环上非交换环与交换环之间的一个主要区别是，必须分别考虑右理想和左理想。在现代数学的发展进程中，非交换环与很多重要学科和分支有密切关系。

3、 p-adic

从算术开始，人们就知道有理数经加减乘除之后仍为有理数，并满足通常的交换律、结合律、分配律等公理，亦即所有有理数构成现在所说的域。但直到 19 世纪末 20 世纪初，人们才从集合的角度来对有理数进行整体考虑，尝试运用公理定义并给出抽象域的观念。

亨泽尔出生于柯尼斯堡，在波恩和柏林求学他不但深受其老师利普希茨、魏尔斯特拉斯和克罗内克的影响，而且博采众长，研究戴德金等人的思想 1901 年开始在马尔堡任职，活跃在教学和研究的多个领域并有建树。最为有名的便是引进 p 进数。

早在 1893 年，亨泽尔就有了 p 进数的思想。当时人们对函数论中的结果(即黎曼曲面上一个亚纯函数可以在一点的邻域展开成单值化参数的事级数)非常熟悉，且知道代数数域与代数函数域相似，所以亨泽尔开始考虑对代数数域是否可以得到相应的展开。1897 年，他引入 p 进数。他对每个代数数域 K 中的元素给出对应的一个形式和 $\sum_{k=r}^{\infty} a_k p^k$。以后若干年，尤其是在 1901 年到马尔堡后，他继续系统地发展了这些思想。

1904 年，亨泽尔又向前迈进了一大步，把有理数域扩张成包含所有这种形式和的集合，而不管形式和是否对应一个有理数。我们通过对形式和定义四则运算，就可以构成一个 p 进域，而且他还进一步研究它的代数扩张以及其中的整数环，这样他就建立了一套全新的理论.在 p 进数的基础上，亨泽尔又发展起了 p 进代数数域从而在 p 进数上实现代数数的一般理论。

一个 g 进有理数是一个级数

$$A = a_r + a_{r+1} g^{r+1} + a_{r+2} g^{r+2} + \cdots ,$$

这里，r 是任意整数，g 是一个正整数，$a_i (i = r, r+1, \cdots)$ 是有理数，在约去与分子的公因子之后，其分母与 g 没有公因子。显然，可以定义两个有理 g 进数的加法和减法。g 进有理数 A 与 $B\,(B = b_r + b_{r+1} g^{r+1} + b_{r+2} g^{r+2} + \cdots)$ 的乘积定义为

$$AB = a_r b_r g^{2r} + (a_r b_{r+1} + a_{r+1} b_r)\, g^{2r+1} + \cdots ,$$

除法没有定义。如果 a_i 为 0 到 $g-1$ 的正整数，那么称 A 为约化的 g 进数。对任一确定的 g，每一有理数都可以唯一地表示为一个约化的 g 进数。这是亨泽尔理论的起点，通过选取不同的基，有理数可以有几种不同表达式。亨泽尔对这种数规定了四种基本运算，并证明它们构成一个域。p 进数的一个子集能够和普通的有理数成一一对应，而且这个子集在两个域同构的前提下与有理数域同构。对于 p 进数域，亨泽尔定义了 p 进整数、单位和其他类似于普通有理数的那些概念。

弗兰克尔比较详细地讨论了约化的有理 p 进数域，这里 p 是一个固定的素数。考虑表达式为 $\sum_n^{\infty} a_i p^i\,(a_i = 0, 1, \cdots, p-1)$ 的系统。如果称表达式的第一个非零系数的下标为它的“阶”，那

么，具有相同阶 i 的所有数就构成了类 C_i . 因为同一类的两个数被 p 除是类似的，所以我们认为它们是等价的。一般地，对于两个不等价的数 α, β，当 α 的阶低于 β 的阶时, 我们称 $\alpha < \beta$。按照类 C_i 各自的阶对 C_i 排序。C_∞ 只包含零元素，它的阶是 ∞。C_0 是单位元构成的类，它的阶是零。在一个确定的类 C_i 里，两个数排序如下。对于任意的两个元素,

$$\alpha = \sum_{n}^{\infty} a_i p^i \text{ 和 } \beta = \sum_{n}^{\infty} b_i p^i$$

一般地，若 $a_n = b_n, a_{n+1} = b_{n+1}, \cdots, a_{n+m} = b_{n+m}$，但 $_{n+m+1} < b_{n+m+1}$，那么 $\alpha << \beta$。

他通过假定一个有 12 个独立公理的系统 Π 定义了两种运算。前九条公理包括域的标准要求。后三条公理谈到两种运算以及序的性质。

如果 α 是 p 进系统的非零元素，那么 $p\alpha < \alpha$。特别地，$p\alpha$ 是倍数序列 $2\alpha, 3\alpha, \cdots$ 之中比 α 小的第一个元素。在一个 g 进系统中，若 $m\alpha$ 是序列中的第一个比 α 小的倍数，则 m 是 g 的一个因子，可能是 g 本身。

弗兰克尔认为这一结果体现了 p 进系统与 g 进系统的不同，前者结构更为简单。但后者仍有研究发展空间。他后来沿着 g 进系统的方向发展了环论。

后来亨泽尔的学生哈塞进一步发展了 p 进数理论，与亨浑尔一起确立了关于二次型的著名“局部——整体”原理，促进了赋值论和局部域理论的发展。虽然 p 进数理论主要是由在数论中引入幂级数的思想和技术引发和推动的，但产生的影响远不止于此。这种 p 进数分析实际上提供了另一种形式的微积分，在数论、代数几何、代数函数等方面有广泛的应用，近半个多世纪以来已成为数学领域乃至物理学领域的重要解析工具。p 进域亦和其他的具体域一起被抽象化、结构化，成为抽象域的子系统，在抽象代数学中占有一席之地。

五、 域论的历史

1、 域论的建立

从十九世纪初的几十年开始，域论的发展经历了大约 100 年的时间。这一时期也见证了其他主要代数理论，即群论、环论和线性代数的发展。正如我们将要看到的，域论的发展与其他三种理论的发展密切相关。

抽象域理论产生于三个具体理论——后来被称为伽罗瓦理论、代数数论和代数几何。这些理论创立于十九世纪，并开始蓬勃发展。对抽象域概念的兴起有一定影响的还有同余理论和符号代数学。

2、 Galois 理论

在本节中，我们将介绍 Galois 理论，以此引出几何三大问题不可解的证明和四次以上方程无根式解的证明。

域

在上一章我们给出了**环**的定义。进一步的，如果对环 R 中的任一非零元素 a ，都有乘法逆元，即存在 $a^{-1} \in R$ ，满足 $a \cdot a^{-1} = a^{-1} \cdot a = 1$ ，则称它为**除环**。更进一步的，如果除环 R 具有乘法交换律，即对 R 中任意元素 a, b 有 $a \cdot b = b \cdot a$ ，则称 R 是**域**。

一个域 k 的**特征(characteristic)**是最小的正整数 n 使得在 k 中 $n \cdot 1 = 0$，写作 $\mathrm{char}(k)$。若这样的 n 不存在，则 $\mathrm{char}(k) = 0$。

域扩张

类比子群和子环的概念，一个域 K 的子环 k 是一个域，则 k 称作 K 的一个子域，且 K/k 叫做一个**域扩张**。若 K/k 是一个域扩张且 K 的子域 L 包含 k，则称 L 是 K/k 的一个**中间域**。

定义一个域扩张 K/k 的**度数** $[K : k]$ 是 K 作为一个 k-向量空间的维数。若此向量空间是无限维的，则 $[K : k] = \infty$。容易看到 $[K : k] = 1 \Longrightarrow K = k$。

域扩张的度数具有乘法关系$[K : k] = [K : L][L : k]$，其中 L 是域扩张 K/k 的一个中间域。

代数扩张

令 R 为一个环，多项式 f 形如 $f = \sum_{i=0}^{n} a_i x^i$ ，其中 $a_i \in R$, $n \in \mathbb{N}$，$a_n \neq 0$。 n 叫作 f 的**度数(degree)**。令 $R[x]$ 为这样的多项式的集合。若对于 $f = \sum_{i=0}^{n} a_i x^i$ 和 $g = \sum_{i=0}^{m} b_i x^i$ ，这里 $n \geq m$ ，定义 $f + g = \sum_{i=0}^{n} (a_i + b_i) x^i, fg = \sum_{k=0}^{n+m} \left(\sum_{i+j=m} a_i b_j \right) x^m$，其中 $b_i = 0, \forall i > m$ ，则 $R[x]$ 和这两个运算构成一个多项式环。若 $a_n = 1$ 则称 f 是**首一的(monic)**。

若 $a \in K$ 是 $f = \sum_i b_i x^i \in k[x]$ 的一个**根(root)**，即 $f(a) = \sum_i b_i a^i = 0$ ，则 a 在 k 上为**代数的(algebraic)**，否则 a 在 k 上为**超越的(transcendental)**。若 K 中的所有元素在 k 上都是代数的，则 K/k 叫作一个**代数扩张**。

令 $a_1, \cdots, a_l \in K$，K 的所有包含 k 和 $a_1, \cdots, a_l$ 的子域的交集 $k[a_1, \cdots, a_l]$ 叫作**由** $a_1, \cdots, a_l$ **生成的** k **的扩张。**

若 $a \in K$ 在 k 上是代数的，则 $k[a]$ 叫作 k 的一个**简单代数扩张**。此时令 $\mathrm{ev}_a : k[x] \to K, g \mapsto g(a)$ 为**赋值同态(evaluation homomorphism)**。容易注意到 a 是代数的等价于 $\ker(\mathfrak{ev}_a) \neq 0$。

显然 a 在 k 上的极小多项式是唯一的首一多项式，同时也是不可约的，这里不可约指的是不可以被分解为非常数多项式的乘积。

考虑元素 $a \in K$ 在 k 上是代数的，且 f_a 是相应的极小多项式，则 $k[a] \cong k[x]/\langle f_a \rangle$，且 $[k[a]:k] = deg(f_a)$。因此，一个极小多项式可以定义一个简单代数扩张，也可以定义一个域同构扩张。

若 $\phi : k \to k'$ 和 $\Phi : K \to K'$ 是域同构，且 K/k 和 K'/k' 为域扩张，且 $\Phi|_k = \phi$，那么 Φ 叫作 ϕ 的扩张。通过由同构 $\phi : k \to k'$ 定义的另一个同构

$$\phi^* : k[x] \to k'[x], \quad \sum_i a_i x^i \mapsto \sum_i \phi(a_i) x^i$$

可以证明如下结论：

对于具有相同极小多项式的、在k上为代数的$a, a' \in K$存在唯一一个k-同构：

$$\phi : k[a] \to k[a'] \text{使得} \phi(a) = a' \tag{*}$$

分裂域

对于一个非常数的多项式 $f \in k[x]$ 我们想找一个有限域扩张，使得 f 在 K 中有根，甚至能分解成一次因式的乘积。对于一个 $k[x]$ 中的不可约多项式，我们总可以找到一个简单代数扩张 K/k，使得 $[K:k] = \deg(f)$，且 f 在 K 中有根。这里的 K 是由 k 不断添加 f 的根得到，直到可以把 f 分解成线性因式。最小的这样的域叫做 f 在 k 上的分裂域，它在同构意义下唯一。

具体而言，令多项式 $f \in k[x]$ 的度数为 $n > 0$。若一个有限域扩张 K/k 使得 f 在 K 上分解为线性因式，即存在 $a_1, a_2, \ldots, a_n, n \in K$ 使得 $f = b(x - a_1) \ldots (x - a_n)$，且 f 不在任何中间域 $k \subseteq L \subsetneq K$ 上分裂，则 K 叫做 f 在 k 上的分裂域。

若 K 和 K' 是 f 在 k 上的分裂域，则存在同构 $\Phi : K \to K'$，他是自同构 $\phi : k \to k$ 的扩张。

分裂域的存在性是显然的。举例而言，若 a 是 $x^4 + 1$ 在 $\mathbb{Q}$ 的一个扩张里的一个根，那么 $-r, \frac{1}{r}, -\frac{1}{r}$ 也是 $x^4 + 1$ 的根，且这些根都是不同的，于是我们在 $\mathbb{Q}[r]$ 上将 $x^4 + 1$ 分裂成 $(x - r)(x + r)(x - \frac{1}{r})(x + \frac{1}{r})$，即 $\mathbb{Q}[r]$ 是 $\mathbb{Q}$ 的一个分裂域。

正规扩张

若一个域扩张 K/k 是代数的，且任意在 K 中有根的不可约多项式 $f \in k[x]$ 在 K 中分裂为一次因式，则称 K/k 是一个**正规扩张**。

若一个域扩张 K/k 是有限的，K 是 $k[x]$ 中的一个多项式的分裂域当且仅当 K/k 是正规的。

举例而言，$\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ 不是一个正规扩张，因为 $\mathbb{Q}[\sqrt[3]{2}]$ 不是 $\mathbb{Q}$ 的一个分裂域，而 $\mathbb{Q}[\sqrt[3]{2}, e^{2\pi i/3}]/\mathbb{Q}$ 是一个正规扩张，因为 $\mathbb{Q}[\sqrt[3]{2}, e^{2\pi i/3}]$ 是多项式 x^3-2 在 Q 上的分裂域。

可分扩张

为了避免多重根，我们提出了**可分扩张(separable extension)**的概念，而一个正规可分扩张就是我们本章的重点——伽罗瓦扩张。

令 $f \in k[x]$，$f = b(x-a_1)^{m_1}\dots(x-a_l)^{m_l}, m_i > 0, a_1, \dots, a_l \in K$ 两两不同为 f 在域扩张 K/k 上的一个分为一次因式的分裂。若 $m_i = 1$ 则称 a_i 为一个单根，否则称为阶为 m_i 的多重根。若对于一个代数域扩张 K/k，所有在 K 中有根的不可约多项式 $f \in k[x]$ 在它们的分裂域中只有单根，则 K/k 称为一个**可分扩张**。若 k 的所有代数扩张 K/k 都是可分的，则 k 称为**完美的(perfect)**。任意特征为 0 的域都是完美的。

(本原元定理) 若 K/k 是一个有限可分域扩张，那么存在 $a \in K$，使得 $K = k(a)$，这个元素 a 称作一个本原元。

伽罗瓦群

我们可以通过研究 K 的 k-自同构构成的伽罗瓦群 $Gal(K/k)$ 来研究一个有限域扩张 K/k。

令 K/k 为一个域扩张，K 在 k 上的**伽罗瓦群** $\mathrm{Gal}(K/k)$ 是 k-自同构 $\phi : K \to K$ 的集合，即对于任何 $a \in k$有$\phi(a) = a$。这个集合对于映射复合的运算构成一个群。

若 $k[a]/k$ 是一个度数为 n 的一个简单代数扩张，f 是 a 在 k 上的极小多项式，R 为 f 在 $k[a]$ 中的根的集合，且 $S(R) = \{\sigma : R \to R\text{双射}\}$ 为 R 的置换群，那么它的伽罗瓦群 $\mathrm{Gal}(k[a]/k)$ 和 $S(R)$ 的一个阶为 $|R| \le n$ 的子群同构。

伽罗瓦扩张

若一个有限域扩张 K/k 是可分且是正规的，即任意在 K 中有根的不可约多项式 $f \in k[x]$ 在 K 中分解为一次因式，且这样的多项式在其分裂域中只有单根，则 K/k 称作一个**伽罗瓦扩张**

根据本原元定理，我们可以得到推论：若 K/k 为一个度数为 n 的伽罗瓦扩张，那么 $\mathrm{Gal}(K/k)$ 和 $\{1, \dots, n\}$ 的置换群 S_n 的一个子群同构，且 $|\mathrm{Gal}(K/k)| = n$。

通过利用极小多项式构造的域同构的扩张，我们可以得到对于一个伽罗瓦扩张 K/k 和 $a, b \in K$，a, b 有相同的极小多项式当且仅当存在 $\phi \in \mathrm{Gal}(K/k)$ 使得 $\phi(a) = b$。由此我们可以得到如下结论：

$$\textbf{若}K/k\textbf{是一个伽罗瓦扩张，则}k = \{a \in K : \phi(a) = a, \forall \phi \in \mathrm{Gal}(K/k)\} \qquad (**)$$

证明： 根据定义，若 $a \in k$ 且 $\phi \in \mathrm{Gal}(K/k)$，则 $\phi(a) = a$. 现在假设 $\phi \in \mathrm{Gal}(K/k)$，并令 f 为 a 在 k 上的最小多项式。由于 K/k 是正规的，f 在 K 上分裂。令 b 为 f 的一个根，那么存在 $\phi \in \mathrm{Gal}(K/k)$ 使得 $\phi(a) = b$，故 $a = b$。由于 K/k 是可分的，f 没有多重根，故 $f = x - a \in k[x]$，即 $a \in k$。

这个定理说的是，对于一个伽罗瓦扩张 K/k， k 就是这个扩张中被伽罗瓦群 $\mathrm{Gal}(K/k)$ 的元素固定的元素的集合。因此，伽罗瓦群 $\mathrm{Gal}(K/k)$ 的子群与中间域 $K/L/k$ 被联系起来了。我们通常将域扩张视作多项式的分裂域，故我们将一个多项式 $f \in k[x]$ 的伽罗瓦群 $\mathrm{Gal}(f)$ 定义为其分裂域的伽罗瓦群。一个多项式的的伽罗瓦群也可以由它的根的置换群的一个子群界定。

令 $f \in k[x]$ 是一个非常数多项式，并令 K 为 f 在 k 上的分裂域，这里 K 在 k 上是恒等映射的同构下是唯一的，那么，f 的伽罗瓦群是 $\mathrm{Gal}(f) = \mathrm{Gal}(K/k)$。

举例而言，令 $f = x^3 - 2 \in \mathbb{Q}[x]$，那么 $\mathrm{Gal}(f)$ 是 S_3 的一个子群。令 K 是 $\mathbb{Q}$ 的分裂域，$K/\mathbb{Q}$ 是一个伽罗瓦扩张，那么 $K = \mathbb{Q}[\sqrt[3]{2}, e^{2\pi i/3}]$，且 $[K : \mathbb{Q}] = 3 \cdot 2 = 6$，故 $|\mathrm{Gal}(f)| = 6$，又因为 $\mathrm{Gal}(f)$ 是 S_3 的一个子群，故$\mathrm{Gal}(f) = S_3$。

伽罗瓦理论基本定理

伽罗瓦理论基本定理将伽罗瓦扩张 K/k 的中间域和域扩张的伽罗瓦群 $\mathrm{Gal}(K/k)$ 联系在一起，因此它可以将域论中的问题转化为群论的问题，使得它们更容易解决。在介绍伽罗瓦理论基本定理的证明之前，我们需要引入**固定域 (fixed field)**的概念。

若 K/k 是一个域扩张，那么对于伽罗瓦群的子群 $H \subseteq \mathrm{Gal}(K/k)$，$H$ 的**固定域** 是 $\mathrm{Fix}(H) = \{\phi(a) = a, \forall \phi \in H\}$。

$\mathrm{Fix}(H)$ 显然是 K 的一个子域。此外，我们已经在(**)中证明了，对于一个伽罗瓦扩张 K/k，$\mathrm{Fix}(\mathrm{Gal}(K/k)) = k$。还有，对于 K/k 的一个中间域 L，$\mathrm{Gal}(K/L) = \{\phi \in \mathrm{Gal}(K/k) : \phi|_L = \mathrm{id}\}$ 是 $\mathrm{Gal}(K/k)$ 的一个子群。下面的定理就是伽罗瓦理论基本定理，它由三部分构成。

(伽罗瓦理论基本定理)令 K/k 为一个伽罗瓦扩张，L 为 K/k 的一个中间域，并令 H 为 $\mathrm{Gal}(K/k)$ 的一个子群。

1.映射 $H \mapsto \mathrm{Fix}(H)$ 和 $L \mapsto \mathrm{Gal}(K/L)$ 是

$$\{\mathrm{Gal}(K/k) \text{ 的子群}\} \longleftrightarrow \{K/k \text{ 的中间域}\}$$

之间互为逆的双射。换句话说，$\mathrm{Fix}(\mathrm{Gal}(K/L)) = L$，且 $\mathrm{Gal}(K/\mathrm{Fix}(H)) = H$。

2.对于 $\mathrm{Gal}(K/k)$ 的子群 H，$[K : \mathrm{Fix}(H)] = |H|$，且 $[\mathrm{Fix}(H) : k] = [\mathrm{Gal}(K/k) : H]$。

3.对于中间域 $k \subseteq L \subseteq K$，$[K : L] = |\mathrm{Gal}(K/L)|$，且 $[L : k] = [\mathrm{Gal}(K/k) : \mathrm{Gal}(K/L)]$。

证明： 1.令 L 为 K/k 的一个中间域，则 K/L 是一个伽罗瓦扩张。由于 K 是一个多项式在 k 上的分裂域，故也是在 L 上的分裂域，因此 K/L 是一个正规扩张。令 f 为 a 在 L 上的最小多项式，并令 g 为 a 在 k 上的最小多项式。由于 K/k 是可分的，g 在其分裂域中没有多重根。由于 f 是 g的因式，f 在其分裂域中没有多重根，故 K/L 是可分的。根据$(**)$，$\mathrm{Fix}(\mathrm{Gal}(K/L)) = L$。

令 H 为 $\mathrm{Gal}(K/k)$ 的一个子群。我们想要证明 $\mathrm{Gal}(K/\mathrm{Fix}(H)) = H$。根据本原元定理，$K = k[a]$，其中 $a \in K$。定义 $f = \prod_{h\in H}(x - h(a))$，故 $\deg(f) = |H|$. 由于 $k[a]/k$是一个简单扩张， $h_1(a) = h_2(a)$ 意味着 $h_1 = h_2$，故 f 的根是不同的。将 f 写作 $f = \sum_i b_i x^i$，其中 $b_i \in k[a]$。我们要证明 $b_i \in \mathrm{Fix}(H)$。对于 $l \in H$，令 $l_*(f) = \sum_i l(b_i)\, x^i$。由于 $l, h \in H$，$l_*(f) = \prod_{h\in H}(x - l(h(a))) = \prod_{h\in H}(x - h(a)) = f$。因此，$b_i \in \mathrm{Fix}(H)$，即 $f \in \mathrm{Fix}(H)[x]$。这样，$f(a) = 0$，故 a 在 $\mathrm{Fix}(H)$ 上的最小多项式 g 是 f 的因式。由于 $K = k[a] = F[a]$，我们有

$$|\,\mathrm{Gal}(K/\,\mathrm{Fix}(H))| = [K : \mathrm{Fix}(H)] = \deg(g) \le \deg(f) = |H|$$

由于 H 是 $\mathrm{Gal}(K/\mathrm{Fix}(H))$ 的一个子群，我们有 $|\mathrm{Gal}(K/\mathrm{Fix}(H))| = |H|$，即 $\mathrm{Gal}(K/\,\mathrm{Fix}(H)) = H$。

2.由于 $\mathrm{Fix}(H)$ 是 K/k 的一个中间域，$K/\,\mathrm{Fix}(H)$ 是一个伽罗瓦扩张。因此，$[K : \mathrm{Fix}(H)] = |\,\mathrm{Gal}(\mathrm{K}/\,\mathrm{Fix}(\mathrm{H}))| = |H|$。根据度数定理和拉格朗日定理，

$$[\mathrm{Fix}(H) : k] = [K : k]/[\mathrm{Fix}(H) : k] = |\,\mathrm{Gal}(K/k)|/|H| = [\mathrm{Gal}(K/k) : H]$$

3.由于 K/L 是一个伽罗瓦扩张，$[K : L] = |\mathrm{Gal}(K/L)|$。那么

$$[L : k] = [K : k]/[K : L] = |\,\mathrm{Gal}(K/k)|/|\,\mathrm{Gal}(K/L)| = [\mathrm{Gal}(K/k) : \mathrm{Gal}(K/L)]$$

由上面的伽罗瓦理论基本定理，我们知道，通过伽罗瓦群和固定域可以在伽罗瓦扩张 K/k 的中间域和此域扩张的伽罗瓦群的子群之间构造一个双射——中间域 L/k 对应 $\mathrm{Gal}(K/k)$ 的子群 $\mathrm{Gal}(K/L)$。另外一个重要结论是，当且仅当 L/k 是一个正规扩张，$\mathrm{Gal}(K/L)$ 是 $\mathrm{Gal}(K/k)$ 的一个正规子群，且

$$\mathrm{Gal}(L/k) = \mathrm{Gal}(K/k)/\,\mathrm{Gal}(K/L)$$

令 K/k 为一个伽罗瓦扩张，并令 L 为 K/k 的一个中间域。令 $\alpha \in \mathrm{Gal}(K/k)$，并令 $\alpha(L) = \{\alpha(a) : a \in L\}$。显然 $\alpha(L)$ 是 K/k 的一个中间域。那么，下面的陈述是等价的:

1. L/k 是一个正规扩张。
2. $\alpha(L) = L, \forall \alpha \in \mathrm{Gal}(K/k)$。
3. $\mathrm{Gal}(K/L)$ 是 $\mathrm{Gal}(K/k)$ 的一个正规子群。

证明： $(1 \Rightarrow 2)$ 令 $a \in L$，并令 f 为 a 在 k 上的最小多项式。由于 L/k 是一个正规扩张，f 的所有根都在 L 中。令 $\alpha \in \mathrm{Gal}(K/k)$。由于 $f(\alpha(a)) = \alpha(f(a)) = 0, \alpha(a) \in L$，故 $\alpha(L) \subseteq L$。类似地，我们可以证明 $\alpha(L)^{-1} \subseteq L$，即 $L \subseteq \alpha(L)$。

$(2 \Rightarrow 3)$ 令 $\alpha, \beta \in \mathrm{Gal}(K/k)$. $\beta \in \mathrm{Gal}(K/\alpha(L))$ 等价于 $\beta(\alpha(a)) = \alpha(a), \forall a \in L$。这等价于 $\alpha^{-1}(\beta(\alpha(a))) = a, \forall a \in L$，而这等价于 $\alpha^{-1}\beta\alpha \in \mathrm{Gal}(K/L)$，即 $\beta \in \alpha\mathrm{Gal}(K/L)\alpha^{-1}$。那么，

$$\mathrm{Gal}(K/L) = \mathrm{Gal}(K/\alpha(L)) = \alpha\,\mathrm{Gal}(K/L)\alpha^{-1}$$

因此，$\mathrm{Gal}(K/L)$ 是 $\mathrm{Gal}(K/k)$ 的一个正规子群。

$(3 \Rightarrow 1)$ 令 $\alpha \in \mathrm{Gal}(K/k)$. 由于 $\mathrm{Gal}(K/L) = \alpha\,\mathrm{Gal}(K/L)\alpha^{-1} = \mathrm{Gal}(K/\alpha(L))$， 根据伽罗瓦理论基本定理，$L = \alpha(L)$。令 $f \in k[x]$ 为有根 $a \in L$ 的不可约多项式，并令 b 为 f 在 K 中的另一个根. 由于 a, b 在 k 上的最小多项式都是 f，根据$(*)$，存在 $\alpha \in \mathrm{Gal}(K/k)$ 使得 $\alpha(a) = b$。那么，$b \in \alpha(L) = L$，故 K/k 是一个正规扩张。

一个推论是，我们可以用 K/L 和 K/L 的伽罗瓦群的商群来界定中 L/k 的伽罗瓦群，即

$$\mathrm{Gal}(L/k) \cong \mathrm{Gal}(K/k)/\,\mathrm{Gal}(K/L)$$

这是因为 $\mathrm{Gal}(K/k)/\mathrm{Gal}(K/L)$ 和 $\mathrm{Gal}(L/k)$ 的一个子群，且 $|\mathrm{Gal}(L/k)| = |\mathrm{Gal}(K/k)/\mathrm{Gal}(K/L)|$。

至此，我们已经叙述了伽罗瓦理论的基本内容，在下两节中我们将完成几何三大问题不可解的证明和四次以上方程无根式解的证明。

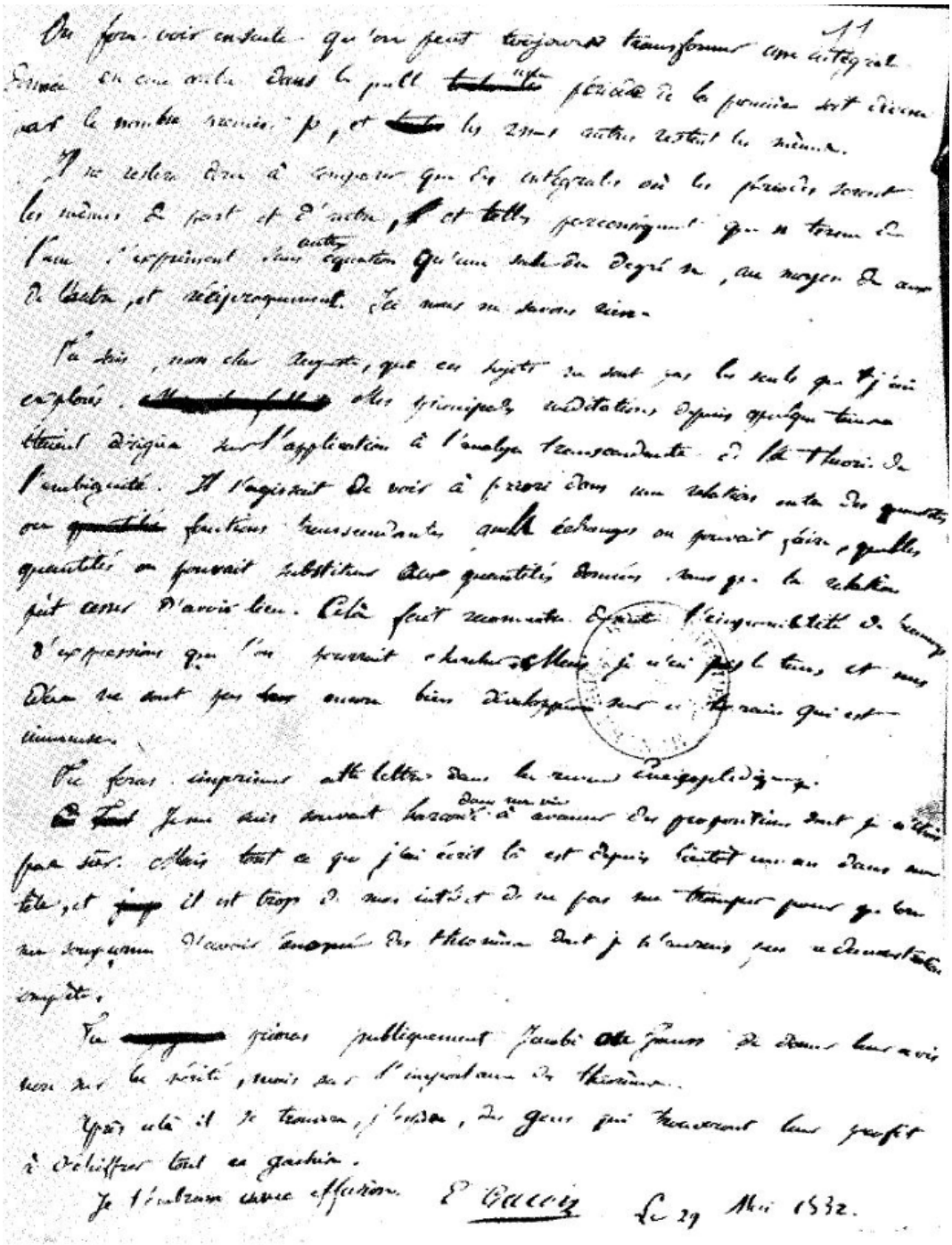


图 18: Galois的手稿

3、 对于几何三大问题不可解的证明

我们先来公理化定义尺规作图。

记 $L(x,y)$ 为过两点 x 和 y 的直线，$C(x,r)$ 为以点 x 为圆心，长度 r 为半径的圆。

开始尺规作图之前，我们在平面上有 n 个点 $z_1,z_2,\ldots,z_n\in\mathbb{R}^2\cong\mathbb{C}$，其中 $z_1=(0,0),z_2=(0,1)$，即我们有了原点和单位长度。

令 $S_1=\{z_1,\ldots,z_n\}$。我们在 S_i 上通过如下规则作出 S_{i+1}：

(i)添加两直线的交点 $L(x,y)\cap L(x',y')$；

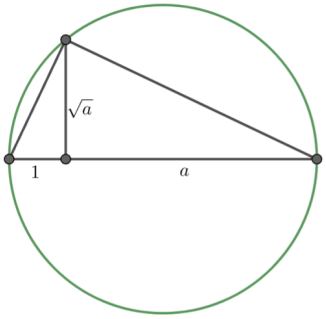
(ii)添加两圆的交点 $C(x,|y-z|)\cap C(x',|y'-z'|)$；

(iii)添加直线与圆的交点 $L(x,y)\cap C(x',|y'-z'|)$。

于是我们有 $S_1\subset S_2\subset\ldots$ 并且 $S=\bigcup_{i=1}^{\infty}S_i$ 是所有能用尺规作图作出来的点构成的集合。

我们已经熟知如何用尺规作图对线段长度进行加减乘除，以及对角进行加减，于是对于 $x,y\in S$，可以通过尺规作图构造 $x+y,x-y,xy,\dfrac{x}{y}$。由此我们可以推得 S 是 $\mathbb{C}$ 的一个子域。

对 $a\in S$，我们可以做出 a 的共轭 $\bar{a}$，同样可以如下图构造 $\sqrt{|a|}$ 的长度，并利用等分角来作出 $\sqrt{a}$(注意这里的 a 是复数)。这表明 $\bar{a},\sqrt{a}\in S$。



通过 S 的定义我们可以看到，S 是 $\mathbb{C}$ 的满足如上条件的最小子域。

我们称 S 中的点是$z_1,\ldots,z_n$ **尺规导出的(constructible from $z_1,\ldots,z_n$)**

对于 $\mathbb{C}$ 的子域 F，一个域扩张 E/F 称为F **上的平方根塔(square root tower over F)**，如果 E 形如 $F(u_1,\ldots,u_n)$ 并且 $u_i^2\in F(u_1,\ldots,u_{i-1})$。

进而我们可以看到 $[F(u_1,\ldots,u_i):F(u_1,\ldots,u_{i-1})]=1or2$，所以 $[E:F]=2^k$ 对于某个正整数 k。

接下来我们证明这样一个结论：**给定 n 个点 $z_1,\ldots,z_n\in\mathbb{C}$，$F=\mathbb{Q}(z_1,\ldots,z_n,\bar{z_1},\ldots,\bar{z_n})$。则 $z\in\mathbb{C}$ 是尺规导出的当且仅当 z 被包含在 F 上的一个平方根塔里。**

证明： 设 T 是平方根塔的集合。

一方面，容易验证 T 同 S 一样满足上述条件，故 $S \subset T$。

另一方面，通过归纳容易验证 T 中的点都是尺规导出的，故 $T \subset S$。

因此 $S = T$，得证。

由此我们可以得到推论如下：**若 z 是尺规导出的，那么 z 是代数数，且若 $g(x)$ 是 z 在 F 上的极小多项式，则 $\deg g(x) = 2^k$，对于某个正整数 k。**

接下来几何三大问题的不可解证明就呼之欲出了。

倍立方问题： 取 $F = Q, z = \sqrt[3]{2}$，z 在 F 上的极小多项式是 $g(x) = x^3 - 2$，$\deg g(x) = 3 \neq 2^k$，故不是尺规导出的。

三等分角问题： 取 $F = Q, z = e^{i\pi/9}$，z 在 F 上的极小多项式是 $g(x) = x^3 - \frac{3}{4}x - \frac{1}{8}$，$\deg g(x) = 3 \neq 2^k$，故 $\frac{\pi}{3}$ 不能被三等分，更不用说一般的角了。

倍立方问题： 取 $F = Q, z = \pi$，z 在 F 上不是代数数，自然不是尺规导出的。

至此我们正式解决了几何三大问题这世纪难题，从此可以窥得 Galois 理论的强大。

4、 对于四次以上方程无根式解的证明

由上述 Galois 理论可以得到：

域 F 上的多项式 $f(x)$ 有根式解$\Longleftrightarrow$ $f(x)$ 的分裂域 K 在 F 上的 **Galois** 群是可解群。

与：

对于一个度数为 n 的伽罗瓦扩张 K/k，$Gal(K/k)$ 和置换群 S_n 同构。

且我们熟知：

$n > 4$ 时，S_n 不是可解群。

综上，五次方程无根式解。

六、 线性代数的历史

1、 线性代数的由来

线性代数是一门非常有用的学科，该学科起源于数论、几何、抽象代数、分析和物理学等不同领域。

线性代数的基本概念包括线性方程、矩阵、行列式、线性变换、线性独立性、维度、双线性形式、二次形式和向量空间。到 1880 年，线性代数的许多基本结果已经建立，但它们不是一般理论的一部分。特别是，不存在这种理论所构成的向量空间的基本概念。这是皮亚诺在 1888 年才引入的。即便如此，它在很大程度上被忽视了。因此，主体的历史发展与其逻辑顺序相反。

大约 4000 年前，巴比伦人知道如何在两个线性方程组中求解两个未知数。同样在我国古代著名的《九章算术》中，仅通过使用它们的系数来解决三个三元线性方程组。这些是矩阵的原型，解法与高斯和其他人在大约 2000 年后引入的“消除法”没有什么不同。

线性方程组的现代研究可以说起源于莱布尼茨，莱布尼茨在 1693 年为此发明了行列式的概念。但他的研究在当时仍然未知。在 1750 年的《代数曲线分析导论》中，克莱默发表了以他的名字命名的求解 $n \times n$ 方程组的的规则，但他没有提供任何证明。他被引导研究线性方程组，同时试图解决一个几何问题：确定一条经过 $\frac{1}{2}n^2 + \frac{3}{2}n$ 个不动点的 n 次代数曲线。

欧拉可能是第一个观察到 n 个未知数组成的 n 个方程组不一定具有唯一解的人。他指出，为了获得唯一性，有必要添加条件。他想到了一个方程对其他方程的依赖性，尽管他没有给出确切的条件。在 18 世纪，线性方程的研究通常被归入行列式的研究，因此没有考虑方程数与未知数不同的系统。

关于他发明的最小二乘法，高斯引入了现在称为高斯消元法的方法，用于线性方程组的求解，尽管他没有使用矩阵符号。他处理了方程和未知数的数量可能不同的情况。线性方程组的理论性质，包括它们的一致性问题，在十九世纪下半叶得到了处理。

2、 线性方程和行列式

尽管现在人们谈论矩阵的行列式，但这两个概念有不同的起源。特别是，行列式出现在矩阵之前，其历史的早期阶段与线性方程密切相关。随后引起行列式新用途的问题包括消除理论——寻找两个多项式具有共同根的条件、坐标变换以简化代数表达式（例如，二次形式）、多重积分变量的变化、微分方程组的解和天体力学。

上一节已述，莱布尼茨发明了行列式。他实质上已经知道了行列式的现代组合定义，并用来研究线性方程组和elimination theory. 他写了很多关于行列式的论文，但直到近些年才得到发表。

最早的关于行列式的出版物是麦克劳林的《Treatise of algebra》，其中用来解 2×2 和 3×3 方程组。不久就有了克莱姆法则。

行列式独立于解线性方程组的阐述最早由范德蒙在 1772 年的《Memoir on elimination》中给出。行列式的名字最早由高斯在 1801 年给出，用于表示二次型的判别式。拉普拉斯在 1772 年的《Researches on the integral calculus and the system of the world》中拓展了范德蒙的工作，指出如何利用代数余子式展开 $n\times n$ 行列式。

第一处系统阐述行列式的是柯西在 1815 年发表的论文，他是我们今天所谓的行列式理论的创立者。他证明了许多关于行列式的结果，例如乘法公式：$\det(AB)=\det A\times\det B$。他的工作为数学家提供了有力的代数工具，用于研究 n 维代数、几何和分析。例如，1843 年凯莱以行列式为基本工具建立 n 维解析几何的理论，1870 年戴德金用来证明代数数的和与积仍然是代数数。

魏尔斯特拉斯和克罗内克大概在 19 世纪 60 年代给出了行列式的公理化定义。魏尔斯特拉斯定义行列式为赋范线性齐次函数。他们的工作在 1903 年为人所知，这一年魏尔斯特拉斯的《On determinant theory》和克罗内克的《Lectures on determinant theory》得到发表。

行列式理论在19世纪是一个充满活力又富有独立性的主题，有 2000 余篇论文。但 20 世纪之后行列式不再那么时髦，因为线性代数主要结果的证明不再依赖于行列式。

3、 矩阵和线性变换

矩阵是“自然”的数学对象：它们与线性方程、线性变换以及双线性型和二次型一起出现，这在几何、分析、数论和物理学中都很重要。矩阵作为数字数组的矩阵出现在公元前 200 年左右的我国数学中，但它们只是线性方程组的缩写。矩阵只有在被运算时才变得重要——加法、减法，特别是乘法；更重要的是，当它被写出来时，它们将被用于什么用途。

矩阵是高斯在前面提到的《Disquisitiones》中隐含地作为线性变换的缩写引入的，但现在以一种重要的方式引入。高斯对二元二次型 $f(x,y)=ax^2+bxy+cy^2$ 的算术理论进行了深入研究。他将两种形式 $f(x,y)$ 和 $F(X,Y)=AX^2+BXY+CY^2$ 称为“等价”，如果当 x、y、X 和 Y 取遍所有整数时，它们生成相同的整数集(a、b、c 和 A、B、C 是整数)。他证明，这等价于存在坐标系 (x,y) 到 (X,Y) 的线性变换 T 将 $f(x,y)$ 转换为 $F(X,Y)$，且行列式$=1$。线性变换被表示为矩形数组——矩阵，尽管高斯没有使用矩阵术语。他还隐含地定义了矩阵的乘积(仅适用于 2×2 和 3×3)。

坐标的线性变换，$y_j=\sum_{k=1}^{n}a_{jk}x_k(1\le j\le m)$，在 17 世纪和 18 世纪的解析几何中占有重要地位主要为($m=n\le 3$)。这自然导致了对矩形数组 (a_{jk}) 的计算。线性变换也出现在射影几何中，它成立于 17 世纪，并在 19 世纪初进行了分析的描述。

Cayley 在 1850 年和 1858 年的两篇论文中正式引入了 $m\times n$ 矩阵(“矩阵”一词是由西尔维斯特在 1850 年创造的)。他指出，将它们视为整体，并认识到它们在简化线性方程组和线性变换组合方面的实用性。他定义了合适的矩形进行矩阵对矩阵的和和乘积。他还介绍了单位矩阵和逆矩阵，并展示了如何在特定条件下使用后者求解 $n\times n$ 的线性方程组。

Cayley 提出了将矩阵视为构成符号代数的重要思想。特别是，他使用单个字母来表示矩阵是矩阵代数发展的重要一步。但他 1850 年代的论文直到 1880 年代才在英国以外的地方引起注意。

在此期间，Cauchy、Jacobi、Jordan、Weierstrass 等人对矩阵进行了深入的研究。他们创造了所谓的矩阵谱理论：将它们分类为对称、正交和酉矩阵等类型，各种类型矩阵的特征值性质的结果，最重要的是，矩阵的规范形式理论——在某种类型的所有矩阵中确定那些在某种意义上是规范的矩阵。一个重要的例子是 Jordan 型，由 Weierstrass 引入(独立于 Jordan)，他表明当且仅当两个矩阵具有相同的 Jordan 型时，它们是相似的。

Frobenius 将他的矩阵理论应用于群表示和四元数，为后者表明，作为可除代数的实数的唯一 n 元组是实数、复数和四元数，这一结果由 C. S. Peirce 独立证明。Cayley 在他 1858 年的论文中，也通过证明四元数与复数上的 2×2 个矩阵的代数的子代数同构，将矩阵与四元数联系起来。

在该世纪内，线性相关性、基、维数等概念被逐渐提出并完善，逐渐发展成如今我们熟知的线性代数。

图 19: Frobenius

4、 向量空间

正如我们所提到的，到 1880 年，线性代数的许多基本结果已经确立，但它们并没有被视为一般理论的一部分。特别是，不存在这种理论所构成的向量空间的基本概念。它是由皮亚诺于 1888 年推出的。

向量最早的概念来自物理学，它意味着同时具有大小和方向的量。这个想法在 17 世纪末已经确立，向量平行四边形也是如此，向量平行四边形是由两个向量确定的相邻边。在这种情况下，向量的相加及其乘以标量具有明确的物理意义。

向量的数学概念起源于复数的几何表示。1835 年，Hamilton 以代数方式将复数定义为有序的实数对，通常的运算是加法和乘法，以及数乘。他指出，这些元素满足封闭律、交换律和分配律，具有零元素，并且具有加法和乘法逆。

一个重要的发展是将向量思想扩展到三维空间。Hamilton 在他的四元数系统中构造了一个向量代数：以 $ai + bj + ck$ 的形式表示，其中 a、b、c 是实数，i、j、k 是四元数单位——这是三维欧几里得空间基础的明确前身。正是在这里，他为这些对象引入了“向量”一词。

向量空间理论的一个关键发展是将三维空间的概念进一步扩展到更高维度的空间。Hamilton 将三维空间扩展到四维空间称为“想象力的飞跃”。当然，他想到了四元数，一个四维向量空间(也是一个可除代数)。

皮亚诺定义了线性代数的许多概念，包括维数和线性变换，并证明了许多定理。皮亚诺的工作在很大程度上被忽略了，可能是因为公理学还处于起步阶段，也许是因为这项工作与几何学密切相关，而忽略了我们上面描述的线性代数思想的其他重要背景。

关于公理化方法的一句话。虽然它只是在二十世纪初才建立起来，但它在十九世纪的最后二十年里“在空中”。例如，出现了群和域的公理化定义、正整数(参见皮亚诺公理)和射影几何。

Banach 在 1920 年的博士论文中将实数上的赋范线性空间(现在称为 Banach 空间)公理化，非常具有现代精神。

Emmy Noether 在 1921 年的论文《Ideal theory in rings》中，Emmy Noether 引入了模，并将向量空间视为特例。因此，我们看到向量空间在三种不同的环境中出现：几何、分析和代数。van der Waerden 在他 1930 年的经典著作《Modern Algebra》中，有一章题为《线性代数(Linear Algebra)》。**在这里，该术语首次以我们今天的意义使用，线性代数登上了历史舞台。**

A 参考文献

[1] Israel Kleiner, A History of Abstract Algebra

[2] V. Katz, Algebra and its teaching: An historical survey

[3] N. Bourbaki, Elements of the History of Mathematics

[4] N. Jacobson, Basic Algebra

[5] M. J. Crowe, A History of Vector Analysis

[6] L. Corry, Modern Algebra and the Rise of Mathematical Structures

[7] E. Galois, Sur la théorie des nombres

[8] 王淑红，环论源流

[9] 李文林，数学史概论

[10] 冯克勤，代数数论简史

[11] 华罗庚，苏步青，中国大百科全书

[12] 汪明义，环论若干研究方向概述