伽罗瓦和库默尔对近世代数及代数数论的影响

欧阳毅

中国科学技术大学，数学科学学院

目录

本短课程的主要目的是从数学发展史的观点，对代数思想/概念/方法在数论上的发展给一个简单介绍. 我们的课程将主要集中于介绍两个伟大的问题—五次及以上方程的求根公式和费马大定理, 以及 19 世纪两位伟大的数学家— 埃瓦里斯特 • 伽罗瓦和 恩斯特 • 爱德华 • 库默尔. 伽罗瓦对于一般 $\geq$ 五次方程的根式不可解性的最终证明导致群论的诞生, 而库默尔对于费马大定理的尝试则导致了代数数论和交换环论的诞生. 在这些工具以及其他伟大数学家的更多进展的的武装下，安德鲁 • 怀尔斯 (Andrew Wiles) 最终于 1995 年证明了费马大定理.

本讲义由五个报告 (五章) 组成. 在第 1 章，我们将介绍二次、三次和四次方程的求根公式. 我们将从古巴比伦人于公元前 1900-公元前 1600 年代如何对二次方程求根开始，并谈及 16 世纪意大利人解决 3 次和 4 次方程的传奇故事. 第二个报告我们先介绍尼尔斯 • 阿贝尔和伽罗瓦的生平和工作，然后简单介绍伽罗瓦理论以及阿贝尔和伽罗瓦的不可解定理. 在第三个报告, 我们将谈及库默尔的生平和工作, 特别地, 库默尔关于理想数的理论. 第 4 章是关于代数数论在库默尔的发现后一百年里 (大约 1850 年-1950 年) 的发展史, 至约翰 • 泰特 1950 年的论文为止. 最后一章主要是讲述 1950 年泰特的论文以后的伽罗瓦上同调和伽罗瓦表示的简单发展历程。

CHAPTER 1

二次、三次和四次方程的求解

1. 二次方程

由初中数学熟知二次方程

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

的两个根是

$$x_1, x_2 = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

这个公式其实在古巴比伦时代 (大约公元前 1900 年-前 1600 年) 人们就已经知道了, 这是一个相当了不起的成果，要知道那个时候中国才刚刚进入第一个朝代—夏朝.

自大约公元前 3500 年到公元前 3000 年开始, 美索不达米亚平原上的古苏美尔人就开始使用楔形文字, 古巴比伦人继承了这个方式. 对数学而言, 楔形文字泥板 BM 13901 (即大英博物馆藏品 13901) 可以说是最著名的了. 这套泥板包括 24 个二次方程问题和它们的解答. BM 13901 的秘密最终被法国考古学家 François Thureau-Dangin (1872-1944) 于 1936 年和奥地利数学家 Otto Neugebauer (1899-1990) 于 1937 年解开, 它揭示了古巴比伦人是如何解二次方程的. 我们下面给两个例子.

在举例前, 注意到古巴比伦人使用 60 进制，这个计数方式也是古苏美尔人在公元前 3000 年最初开始使用并传到古巴比伦人手中. 然而, 他们的记录有时候是有歧义的: 数 1 也可能代表 $\frac{1}{60}$ 或者 $\frac{1}{3600}$, 数 30 可以代表 $\frac{1}{2}$, $\frac{1}{120}$, 90 或者 3630 等等. 因此数 $1, 30$ 既可以代表 $1\frac{1}{2}$ 又可以代表 90, 具体数值需要根据上下文判断. 我们将用 $1, 30$ 表示 90 而 $1; 30$ 表示 $1\frac{1}{2}$.

例 1 (BM 13901 问题 2). 我从正方形面积中减掉边长, (得到) $14, 30$.

用现代语言来说, 令 x 是正方形的边长, 注意到 $14, 30 = 870$, 那么这个问题就是求方程

$$x^2 - x = 870$$

的正根. 在泥板里，巴比伦人实际上给出了形如 $x^2 - bx = c$ 的方程的解答. 在本例里，$b = 1$ 而 $c = 14, 30 = 870$. 下面的表格即是巴比伦人的解答:

步骤	方法	结果	结果
1	你写下系数 1	b	1
2	你将 1 分为两半	$\frac{b}{2}$	$\frac{1}{2}=0;30$
3	你将 $0;30$ 乘以 $0;30$	$(\frac{b}{2})^2$	$0;30\cdot 0;30=0;15$
4	你将 $0;15$ 加到 $14,30$, 结果是 $14,30;15$	$(\frac{b}{2})^2+c$	$870\frac{1}{4}=14,30;15$
5	它是 $29;30$ 的平方	$\sqrt{(\frac{b}{2})^2+c}$	$29\frac{1}{2}=29;30$
6	你加上 $0;30$, 结果是 30	$\frac{b}{2}+\sqrt{(\frac{b}{2})^2+c}$	$29;30+0;30=30$

答案: 30.

例 2 (BM 13901 问题 7). 我将 7 乘以正方形的边长加上 11 乘以它的面积: $6;15$.

这就是解方程

$$11x^2+7x=6\frac{1}{4}.$$

在本例的解答中, 古巴比伦人实际上解决了形如 $ax^2+bx=c$ 的方程求解. 此时 $a=11$, $b=7$ 而 $c=\frac{25}{4}$.

步骤	方法	结果	结果
1	你将 11 乘以 $6;15$	ac	$11\cdot\frac{25}{4}=68\frac{3}{4}=1,8;45$
2	你将 $3;30$ 乘以 $3;30$	$(\frac{b}{2})^2$	$(\frac{7}{2})^2=\frac{49}{4}=12;15$
3	你将它加到 $1,8;45$	$\frac{b^2}{4}+ac$	$81=1,21$
4	这是 9 的平方	$\sqrt{\frac{b^2}{4}+ac}$	$\sqrt{81}=9$
5	你减去 $3,30$	$-\frac{b}{2}+\sqrt{\frac{b^2}{4}+ac}$	$\frac{11}{2}=5;30$
6	11 的逆无法计算		
7	什么数乘以 11 得到 $5;30$	$\frac{-\frac{b}{2}+\sqrt{\frac{b^2}{4}+ac}}{a}$	$\frac{11}{2}/11=0;30$

答案: $0;30=\frac{1}{2}$.

BM 13901 出现的其他问题都是这样的形式. 这套泥板看上去是古巴比伦人的教科书或者训练用书.

注记 1. Otto Neugebauer 是奥地利数学家，他在古代数学史和天文史领域做出了杰出贡献. 他坚持认为古巴比伦人发展的数学理论应该比之前人们所认为的更加重要.

Neugebauer 对于数学社区有着并且一直保持着巨大的影响力. 他是 *Zentralblatt für Matematik* (1931-1938), 和 *Mathematical Reviews* (1939-1945) 的创始人和首任编辑, 因此给数学家们提供了数学研究最核心的摘要服务. Neugebauer 对于数学评论的政策非常有趣. 他坚信评论的长短和论文的重要性不是比例关系；事实上, 差文章需要一个长长的评论这样大家就不

会浪费时间到这个文章上了, 而真正重要的文章只需要评论员告知它的重要性即可.

2. 三次和四次方程

2.1. 希腊人. 希腊人, 特别地说欧几里得的巨著《几何原本》，奠定了现代数学的基础. 尽管希腊几何的核心是通过平面方法构造出来的, 但有三个问题：化圆为方问题，三等分角问题和倍方问题, 很多世纪过去人们都无法通过这个方法来得到解答. 这三个问题中, 倍方和三等分角都是关于三次方程的, 前者是 $x^3 = 2$ 而后者是 $4x^3 - 3x = c$.

希腊数学家丢番图 (Diophantus, 约 200 年-284 年) 有时候被称为 代数之父. 他由于巨著《算术》而闻名于世. 这本书对数论发展有巨大的影响力. 在《算术》里，丢番图解决了数百个代数方程, 他是最先使用代数记号和符号的数学家. 现在人们称求解不定方程的方法为丢番图分析.

2.2. 阿拉伯人：阿尔-花拉子密, 代数和算法. 古希腊人的很多数数学著作, 包括《几何原本》和《算术》等，在中世纪被翻译为阿拉伯语，由阿拉伯人保存了下来. 阿拉伯数学家, 特别地说, 阿尔-花拉子密和阿尔-卡拉吉, 学习希腊人的著作, 在代数上做出了自己的贡献.

阿尔-花拉子密 (Al-Khwārizmī, 约 780 年- 约 850 年), 全名穆罕默德 • 本 • 穆萨 • 阿尔-花拉子密 (Muḥammad ibn Mūsā al-Khwārizmī), 是波斯数学家，航海学家，星象学家和地理学家，巴格达智慧宫 (House of Wisdom) 学者, 代数之父的另一位候选人. 他将印度-阿拉伯数字和代数的概念引入到欧洲数学界. 他最伟大的数学工作 *Hisab al-Jabr wa-al-Muqabala*, 简称为 al-Jabr, 被认为是现代科学的基础和基石。这本书在 12 世纪中叶被翻译为拉丁文, 题为 *Liber Algebrae et Almucabola*. 今天代数 (algebra) 这个名字就是来自这本书的书名 al-jabr 或者 al-ğabr. 在书中, 阿尔-花拉子密给出如何去解线性和二次方程, 如何去计算一些几何图形的面积和体积，他还为了解方程引入了 “平衡” 的概念. 在 12 世纪，阿尔-花拉子密的另一部著作被介绍到西方, 书中他引入了印度-阿拉伯数字和算术. 这本书 *Algoritmi de numero Indorum* (《阿尔-花拉子密印度算术》), 只有拉丁文译本还保存下来了. 书的名字, 拉丁文缩写即 Algoritmi, 是算法 (algorithm) 这个词的起源.

阿尔-卡拉吉 (Al-Karagi, 约 953 年 - 约 1029 年), 全名阿布 • 巴克尔 • 本 • 穆罕默德 • 本 • 阿尔-侯赛因 • 阿尔-卡拉吉 (Abū Bakr ibn Muḥammad ibn al-Ḥusayn al-Karajī), 是另一位波斯数学家. 他被认为是将代数从几何图形运算中解放出来，而使用现代通用的代数符号计算的第一人. 他也可能

是第一位明确提出同余数问题的数学家, 尽管丢番图在他的《算术》里提过类似问题. 一个整数称为同余数如果它是有理系数边长的直角三角形的面积. 阿尔-卡拉吉提了一个等价的问题: 对于哪些正整数 n, 存在有理平方数 a^2 使得 a^2-n 和 a^2+n 也是有理平方数? 我们现在知道 n 是同余数当且仅当 3 次方程 $y^3=x^3-n^2x$ 有非平凡的有理数解.

2.3. 16 世纪的意大利人 (文艺复兴时代). 意大利人在 16 世纪发现三次和四次方程的代数解充满了戏剧性. 那时候文艺复兴进入末期, 意大利分裂为一些城邦国家.

我们首先从三次方程的求解开始. 注意到在 16 世纪的欧洲负数还不被使用, 因此一般三次方程被当时的数学家约化到两种形式: (I) 立方加上一个东西等于一个数, 即 $x^3+px=q$ 和 (II) 立方等于东西加上数, 即 $x^3=px+q$, 这里 p 和 q 都是正数.

2.3.1. 德尔•费罗. 希皮奥内•德尔•费罗 (Scipione del Ferro, 1465-1526) 是博洛尼亚大学教授. 博洛尼亚大学始建于 11 世纪, 是欧洲最古老的大学, 也是德尔•费罗那个时代世界最好的大学. 大约在 1515 年，费罗发现了求解三次方程的方法. 不过他并没有发表他的成果, 只是在 1525 年他快要过世的时候将这个秘密告诉了他的学生安东尼奥•菲奥尔 (Antonio Fior), 此人并不擅长数学，和他的女婿和他在博洛尼亚大学的继承人汉尼拔•德拉•奈维 (Annibale della Nave). 他还给奈维留下一个笔记本，里面记录有他的解法. 菲奥尔则只知道如何解类型 (I) 的三次方程.

2.3.2. 塔塔利亚. 尼科洛•塔塔利亚 (Niccolò Tartaglia, 1500-1557) 生于威尼斯共和国的布雷西亚. 1512 年法军攻占并抢掠布雷西亚时, 他受到严重的伤害, 从此以后他说话都很困难, 因此得到了塔塔利亚 (口吃者) 的绰号.

塔塔利亚的数学知识是自学而来的，他以教授科学和数学课程为生, 最初是在维罗纳, 1534 年搬到威尼斯, 在那里定居直到去世. 尽管他一生潦倒, 他还是将赚到的微博薪水投到军事科学的爱好上, 特别地, 投入到他在火炮领域的发明上面.

自导师过世以后，菲奥尔自己也渴望得到会求解三次方程的荣耀. 他从别人那里听到塔塔利亚会解三次方程, 认为塔塔利亚只是个骗子, 于是向塔塔利亚发起公众挑战. 他们约定挑战双方在 1535 年 2 月 22 日给对方出 30 道数学题, 每人有两个月时间来解答这些问题. 失败者需要给胜利者和他的朋友们付 30 顿大餐的费用.

塔塔利亚意识到菲奥尔的问题会是类型 (I) 的, 但他并不知道如何去解. 经过一番辛勤钻研, 1535 年 2 月 12 日至 13 日的晚上, 也就是比试开始前八

天, 他发现了求解所有类型三次方程的方法. 挑战时他给菲奥尔出了三次方程的问题还有一些其他问题, 而菲奥尔给的 30 个问题的确全是 $x^3+px=q$ 型的. 塔塔利亚在两个小时内就迅速解决了菲奥尔的所有问题，轻易赢得了比赛. 他没有让菲奥尔支付 30 顿大餐的费用, 对他而言，获胜的荣誉就足够了.

我们列举一些菲奥尔的问题:

(1) $x^3+x=6$,
(2) $4x^3+3x=40$,
(3) $x^3+x=5$,
(15) $x^3+x=500$,
(30) $x^3+x=700$.

现在我们介绍一下塔塔利亚解三次方程的方法. 设三次方程为

$$x^3+px+q=0.$$

令 $x=u+v$, 则

$$(u+v)^3+p(u+v)+q=(u^3+v^3)+(u+v)(3uv+p)+q=0.$$

令 $3uv=-p$, $U=u^3$, $V=v^3$, 则

$$\begin{cases} U+V=-q, \\ UV=-\frac{p^3}{27}. \end{cases}$$

于是

$$U,V=-\frac{q}{2}\pm\sqrt{\frac{q^2}{4}+\frac{p^3}{27}},$$

因而方程的一个解是

$$x=u+v=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}. \tag{1}$$

令 j 是 3 次本原单位根 (即 $j^3=1$ 但 $j\neq 1$), 则其他两个根是 $x=ju+j^2v$ 和 $x=j^2u+jv$, 即

$$x=j\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+j^2\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}. \tag{2}$$

$$x=j^2\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+j\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}. \tag{3}$$

2.3.3. 卡尔达诺. 吉罗拉莫 • 卡尔达诺 (Girolano Cardano, 1501-1576), 又称卡丹 (Cardan), 是文艺复兴时代一位多姿多彩、非常有趣的学者. 他是名满全欧的医生, 甚至被请到苏格兰去给圣安德鲁斯大主教治病. 他是非常有名的星象学家. 他还是一位多产的作家, 著作包含医药，数学，物理，航海和赌博 (包括如何出老千) 等等. 他甚至预测了自己的死期, 并且将自己饿死, 以确保预言准确.

卡尔达诺听说了菲奥尔和塔塔利亚的挑战赛, 特别想知道塔塔利亚是如何解三次方程的. 数次联络塔塔利亚失败以后, 卡尔达诺写信承诺会将塔塔利亚介绍给米兰的西班牙总督, 帮助他从总督那里获得经费来支持他的军事科学研究. 塔塔利亚告诉了卡尔达诺他的秘密，但要求卡尔达诺发誓他永远不会发表这个方法. 卡尔达诺的学生费拉里是唯一在现场的第三者, 我们将在后面讲他的故事.

获悉塔塔利亚的秘密后，费拉里很快就在 1540 年找到了解四次方程的方法. 卡尔达诺开始写作 *Ars Magna* (《大术》，The Great Arts), 书里包括求解三次和四次方程的方法. 他自然知道这将会是一部流芳百世的著作. 然而, 由于他的誓言卡尔达诺不能出版这本书. 1543 年德拉 • 奈维告诉了卡尔达诺和费拉里他们俩费罗的工作, 证明塔塔利亚并不是最先发现解三次方程的人. 卡尔达诺在 1545 年出版了 Ars Magna, 确信自己可以打破誓言, 因为塔塔利亚不是三次方程求解方法的发现人. Ars Magna 是第一部完全讲授代数学的拉丁文著作, 可能是文艺复兴时期出版的最重要的数学著作.

当他发现卡尔达诺违背誓言后, 塔塔利亚十分愤怒. 次年塔塔利亚出版了自己的著作 *New Problems and Inventions*, 书中他清楚讲述了他那个方面的故事, 并坚信卡尔达诺的行为十分卑鄙. 此后塔塔利亚和费拉里恶斗多年, 双方均不吝人身攻击对方, 直到 1557 年塔塔利亚去世.

2.3.4. 费拉里. 路德维可 • 费拉里 (Lodovico Ferrari, 1522-1565), 在 1536 年 14 岁时成为卡尔达诺的学生。自从他对四次方程的求解在 Ars Magna 发表, 并且在与塔塔利亚的论战中占据上风以后, 他自己也变得非常有名了. 后来他成为博洛尼亚大学的教授, 但很年轻就去世了, 死因很可疑, 可能是他妹妹谋杀了他. 卡尔达诺对费拉里的悼文是如此说的:

> “生命如此短暂, 长寿者非常稀少, 不管你爱的是谁, 不要期望他们会取悦于你.”

我们来介绍一下费拉里是如何解四次方程

$$x^4 + px^2 + sx + r = 0.$$

令 $z = x^2 + y$, 则

$$z^2 = x^4 + 2x^2y + y^2 = (2y - p)x^2 + qx + (y^2 - r).$$

考虑

$$\Delta = q^2 - 4(y^2 - r)(2y - p) = 0.$$

这是关于 y 的三次方程, 因此是可解的.

- 如果存在 $y \neq \frac{p}{2}$ 使得 $\Delta(y) = 0$, 那么 $z^2 = (Ax + B)^2$ 对于某 A 与 B 成立, 故
$$x = \pm\sqrt{-y \pm (Ax + B)}.$$
- 如果 $y = \frac{p}{2}$ 是 $\Delta = 0$ 的一个根, 那么 $q = 0$ 且 $z^2 = \frac{p^2}{4} - r$. 因此
$$x = \pm\sqrt{-\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - r}}.$$

2.3.5. *求解三次和四次方程取得的进一步数学进展*. 第一个进展是复数概念的引入. 使用三次方程的求根公式, 即使这个根本身是实的, 也可能会遇到负数的平方根. 卡尔达诺在 Ars Magna 第一次给出了复数的计算. 为解决一个特别的三次方程，他写道:

> 不考虑 (这样做引起的) 精神折磨, 将 $5 + \sqrt{-15}$ 与 $5 - \sqrt{-15}$ 相乘, 我们就得到 $25 - (-15)$. 因此这个乘积是 40. .... 如此以来算术的精妙性将得到保持. 这个极端情形, 如我所说, 是如此的精细而无用.

拉斐尔 • 邦贝利 (Rafael Bombelli, 1526-1572) 在 1572 年出版了他影响深远的教科书《代数》(Algebra), 在书中他对于复数和它们的运算法则进行了详细讨论. 从此以后复数正式进入了数学世界.

另一个进展是关于根与系数的关系的韦达定理. 弗朗索瓦 • 韦达 (François Viète, 1540-1603), 与我们本节提到的其他数学家不同是法国人. 韦达第一个引入了系统的代数记号并给出 2 次，3 次和 4 次方程的求解方法，韦达被称为 *现代代数记号之父*, 他的 *In artem analyticem isagoge* (1591; 《解析艺术引论》) 和现代的初等代数教科书十分相似. 他清楚方程的正根的幂次和系数的关系, 这个关系的一般形式即现在所谓的韦达定理:

定理 1. *设方程* $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = (x - x_1)\cdots(x - x_n)$, 则

$$a_{n-k} = (-1)^k \sum_{1 \le i_1 < \cdots < i_k \le n} x_{i_1} \cdots x_{i_k} = (-1)^k S_k(x_1, \cdots, x_n)$$

此处 $S_k(x_1,\cdots,x_n)$ 是 $x_1,\cdots,x_n$ 的 k-次初等对称多项式.

CHAPTER 2

伽罗瓦理论

1. 阿贝尔和伽罗瓦的生平

大于等于五次的一般方程的代数不可解性是两个杰出的年轻数学家：阿贝尔和伽罗瓦解决的. 我们首先简略介绍一下他们的生平.

1.1. 阿贝尔. 尼尔斯•阿贝尔 (Niels Abel, 1802-1829) 是挪威数学家. 在他出生时, 挪威是丹麦的一部分. 法国 (由拿破仑领导) 与欧洲其他强国的战争对挪威人民造成了巨大的政治和经济破坏. 1814 年, 拿破仑失败后挪威被划归瑞典. 就是在这个困难时代阿贝尔在挪威东南部的 Gjerstad 长大.

1815 年阿贝尔去克里斯蒂安尼亚 (即现在的首都奥斯陆) 的天主教会学校学习. 最开始的时候, 阿贝尔在学校的成绩并不出色. 1817 年一位名叫 Bernt Holmboë 的新数学老师的到来让阿贝尔发生了巨大变化. 他开始学习大学阶段的数学教材, 并在 Holmboë 到来 1 年内, 阿贝尔开始阅读欧拉, 牛顿, 拉朗德 (法国天文学家, 1732-1807) 和达朗贝尔的著作. Holmboë 坚信阿贝尔的潜力巨大, 极大鼓舞了阿贝尔的信心，指导他阅读拉格朗日和拉普拉斯的著作. 1820 年, Holmboë 是如此评价阿贝尔的:

> “作为令人难以置信的天才, 他将对数学的狂热和兴趣结合起来，这样他很可能，如果能活下去的话，将成为最伟大的数学家之一”.

1820 年阿贝尔的父亲去世以后, 家里没有钱让阿贝尔继续学校的学业, 也没有钱让他入大学读书. Holmboë 帮助阿贝尔得到一笔奖学金, 让他得以留在学校, 并在 1821 年进入克里斯蒂安尼亚大学学习. 他在 1822 年毕业, 1823 年发表了自己的第一篇文章.

1824 年, 阿贝尔证明了 5 次一般方程的根式不可解性. 他自费用法语出版了他的论文, 并将小册子寄给了一些数学家, 包括高斯, 他打算去哥廷根拜访高斯.

1825 年阿贝尔得到挪威政府一笔基金, 让他可以去国外游学. 1825 年/26 年冬天, 阿贝尔在柏林认识了克雷尔（August Leopold Crelle, 1780-1855), 他们俩很快成为亲密朋友. 在阿贝尔的强烈鼓励下, 克雷尔于 1826 年

创办了 *Journal für die reine und angewandte Mathematik* (现在就叫做克雷尔杂志). 阿贝尔则受克雷尔的鼓舞写作了他关于五次方程不可解的文章的更清楚版本 *Recherches sur les fonctions elliptiques*, 发表在 1827 年克雷尔杂志第 1 卷, 该卷还有阿贝尔另外 6 篇文章. 在柏林阿贝尔开始进行对数学分析严格奠基的工作. 也是在柏林的时候, 阿贝尔获知克里斯蒂安尼亚大学 (挪威此时唯一的大学) 数学教授的位置给了他的老师 Holmboë.

阿贝尔计划与克雷尔一起旅行去巴黎, 并顺道去哥廷根拜访高斯. 但由于克雷尔有事不能分身, 而阿贝尔得到消息说高斯对于他关于五次方程不可解的工作不太高兴 (事实上高斯从来就没有打开过阿贝尔的信). 阿贝尔自己于 1826 年访问了巴黎, 但未能获得他想要的承认. 他于冬天回到柏林, 十分失望又穷困潦倒, 1827 年 5 月他回到克里斯蒂安尼亚.

此时阿贝尔贫病交加, 他先是在克里斯蒂安尼亚大学当助教, 然后获得了一个临时位置. 他开始与雅可比在椭圆函数领域的竞赛，持续出产高水平的数学成果, 而他的健康状况则持续恶化. 他在数学界声名鹊起, 在克雷尔和法国科学院的帮助下获得了柏林的教授职位. 但他未能赴任, 在 1828 年冬天病情加重, 于 1829 年 4 月 6 日去世. 阿贝尔去世后, 人们发现了他关于方程的代数解的未发表工作:

> “如果素数次不可约多项式的某三个根中有一个可以由另外两个的有理函数表示, 则方程根式可解.”

由于他们的杰出工作, 1830 年巴黎科学院将科学院大奖授予阿贝尔和雅可比.

今天在分析和代数教科书中, 我们到处可以看到阿贝尔的贡献: 阿贝尔群, 阿贝尔范畴, 阿贝尔引理等等. 如他的老师在 1820 年所说, 他毫无疑问是 “最伟大的数学家之一”. 2002 年 1 月 1 日, 挪威政府设立了阿贝尔奖, 每年颁发给数学领域的杰出工作. 它是数学界的最高荣誉之一，常被认为是数学界的诺贝尔奖.

1.2. 伽罗瓦. 埃瓦里斯特 • 伽罗瓦 (Évariste Galois, 1811-1832) 于 1811 年 10 月 25 日生于法国巴黎南郊的王后镇 (Bourg-la-Reine). 12 岁之前他在家由母亲 Adelaide Marie Demante 亲自教导. 伽罗瓦的父亲尼古拉 • 加布里埃 • 伽罗瓦是社区名人，1815 年被选为王后镇的市长.

首先我们解释一下伽罗瓦时代法国的政治形势. 1811 年当伽罗瓦出生时, 拿破仑正处于他权力的顶峰. 1812 年拿破仑远征俄国失败, 之后又经受一连串失败, 反法同盟于 1814 年 3 月 31 日进入巴黎, 拿破仑于 4 月 13 日第一次退位, 波旁王朝复辟, 路易十八成为法国国王. 1815 年是著名的百日

王朝时期. 拿破仑从软禁地厄尔巴岛逃出, 3 月 20 日进入巴黎, 6 月 18 日在滑铁卢失败, 6 月 22 日再次退位. 路易十八再次成为法国国王, 他于 1824 年 9 月去世, 他的弟弟查理十世成为新国王. 1830 年, 爆发七月革命, 查理十世逃跑, 复辟的波旁王朝被推翻. 路易 • 菲利浦登上王位, 新王朝也就是七月王朝. 从 1815 年到 1830 年, 法国的政治主题是共和党人/波拿巴派和保皇党人/极端保皇党人的激烈斗争. 伽罗瓦的父母和他自己都是狂热的共和党人.

1823 年 10 月 6 日伽罗瓦入巴黎的路易大帝中学 (Lycée Louis le Grand) 学习. 这座历史悠久的中学是法国最富盛名的中学，现在大名鼎鼎的巴黎高师 (Écloe Normale Supérieure) 在伽罗瓦时代是坐落在路易大帝中学校园内的教师预备学校 (École Préparatoire). 1827 年 2 月伽罗瓦第一次上数学课程, 很快就被数学吸引住了. 伽罗瓦在学校的记录描述他是 “奇异、怪诞、有独创性、封闭”, 而他的老师说他 “聪明、进步很大但方法不够”. 1828 年伽罗瓦第一次参加巴黎综合理工学院 (École Polytechnique) 的入学考试但未被录取，那时巴黎综合理工学院是法国的头号学府.

伽罗瓦回到路易大帝中学继续上学, 他上了路易 • 理查的课, 但大部分时间还是自己自学数学. 1829 年 4 月他的第一篇数学论文在 Annales de mathématiques 上发表, 论文是讨论连分数的. 1829 年 5 月 25 日和 6 月 1 日, 他向法国科学院提交了方程的代数解的问题. 柯西是伽罗瓦论文的审稿人. 柯西拒了伽罗瓦的文章, 部分原因是这个工作部分与阿贝尔的工作重合, 但建议他修改文章, 再次提交.

1829 年 7 月, 由于一位保皇党人牧师在很多封信件中伪造他的签名攻击他的亲戚, 伽罗瓦的父亲自杀. 父亲的去世极大影响了伽罗瓦后来的举动. 不久以后他再次参加巴黎综合理工的考试, 并又一次失败. 伽罗瓦通过中学毕业会考, 于 1829 年 12 月 29 日获得学位. 他的数学老师是这样报告的:

> 这个学生有时候表达自己的思想不清楚, 但他很聪明，对研究有非凡的热情.

他的文学老师则这样报告:

> 他是唯一一位回答我的问题十分糟糕的学生, 他什么也不懂. 我听说这个学生在数学上有杰出的才能, 这让我十分惊讶, 因为从考试来看, 我认为他愚不可及.

由于通过了毕业会考, 伽罗瓦被录取到预备学校 (巴黎高师) 学习.

伽罗瓦接受了柯西的建议, 改写了论文并重新提交, 打算竞争科学院的数学大奖. 论文邮寄给了傅里叶, 当时他是科学院的秘书. 然而傅里叶于

1830 年去世，伽罗瓦的文章被永远丢失了. 我们知道阿贝尔和雅可比于 1830 年 6 月赢得了此次大奖.

1831 年 1 月 17 日，伽罗瓦在泊松的建议下第三次向科学院提交了论文. 泊松和 Lacroix 于 1831 年 7 月 4 日拒绝了他的论文, 说 “他的论述既不充分清楚也没有充分展开让我们不能判定他的严格性, 我们在这个报告中无法给出确定的意见”.

自傅里叶丢失他的文章后, 伽罗瓦就将精力越来越投入到政治活动上去. 1830 年 7 月, 校长 Guigniault 将预备学校的大门锁了，以阻止学生们跑出去加入外面的七月革命. 1830 年 12 月伽罗瓦嘲讽性地回应了 Guigniault 在学生报纸上发表的一封信, 这导致他于 1831 年 1 月 4 日被学校开除. 此后伽罗瓦尝试以教数学课或者辅导低年级数学来谋生. 他于 1831 年 5 月 9 日被捕，于 6 月 15 日被无罪释放，在巴士底日 (1831 年 7 月 14 日) 再次被捕, 于 1832 年 4 月 29 日从狱中释放. 1832 年 5 月 30 日他参与了那场命运的决斗, 次日逝世于医院, 只有他的弟弟阿尔弗雷德 (Alfred) 陪伴在身旁. “再见! 我还大有作为来有益公众.” 他给弟弟的最后遗言说, “别哭! 我需要所有的勇气在 20 岁时死去.”

在决斗前的那天夜里 (1832 年 5 月 29 日), 伽罗瓦坚信他即将到来的死亡, 整夜里他一直在写信，最重要的信是写给他的忠实好友舍瓦利耶 (Auguste Chevalier) 的, 里面叙述了他的数学贡献. 在信中伽罗瓦说:

> “我在分析方面做了一些新东西, 其中一些关于方程理论而另外一些与积分函数有关.
>
> 在方程理论方面, 我寻找方程根式可解的条件, ...
>
> 我最近一段时间考虑的主要问题是将含糊的理论 (theory of ambiguity) 应用到超越分析上去. 但我没有时间了，我处理这片巨大地形的思想还没有发展完好.
>
> 你可以公开请求雅可比或者高斯给出他们的意见, 不是为了它的正确性而是这些定理的重要性.
>
> 此后, 我希望有人会从破解这片混乱的行动中受益.”

赫尔曼外尔 (Hermann Weyl, 1885–1955) 这样评价

> “这封信, 如果从思想的创新性和深刻性来判断, 可能是人类所有文献中最有价值的一篇.”

伽罗瓦死后, 舍瓦利耶和阿尔弗雷德 • 伽罗瓦复制了他的论文并邮寄给高斯, 雅可比和其他人. 他们没有收到高斯和雅可比的回应. 然而, 这些文章传到了约瑟夫 • 刘维尔 (Joseph Liouville, 1809-1882) 手里, 他于 1843 年 9

月 4 日在法国科学院宣布伽罗瓦的文章的确给出了 5 次以上方程不可解的简洁证明.

> ...(他的论文) 完全正确且十分深刻地解决了下面这个可爱问题: 给定一个素数次不可约方程, 判断它是否根式可解.

1846 年, 刘维尔在 Journal de Mathématiques Pures et Aplliquées (现在称刘维尔杂志, 刘维尔于 1836 年创办, 是至今还在连续出版的数学杂志中第二古老的, 仅次于克雷尔杂志) 原封不动地发表了伽罗瓦的论文 (没有如之前计划的那样编辑文章并给以评论).

2. 群和域扩张的基本理论

伽罗瓦理论是联系群和域扩张的理论，这些是近世代数的基本研究对象. 我们首先回顾这些概念的基本性质.

2.1. 群论基础.

2.1.1. *群*. 在数学上，群是非空集合并配备有一个二元运算 (称为乘法运算或者简称乘法), 也就是说任何两个元素通过乘法对应到第三个元素且满足三个条件 (即群的三条公理): 结合律, 单位元和逆元. 我们将群 G 的单位元记为 1. 下面是群的一些例子:

- $\mathbb{Z}$, 整数集合在加法运算下构成群, 这是最为熟知的群的例子之一.
- 循环群, 即由一个元素生成的群. 阶为 n (或者无限) 的循环群都同构于加法群 $\mathbb{Z}/n\mathbb{Z}$ (或者 $\mathbb{Z}$).
- 阿贝尔群, 就是乘法交换的群. 这个名字是纪念尼尔斯 • 阿贝尔的. 通常阿贝尔群的乘法用加法表示，单位元则记为 0. 有限生成阿贝尔群总是有限个循环群的直积.
- S_n: 对称群, 包括 n 个物体的所有置换 (排列), 阶为 $n!$.
- $A_n \subseteq S_n$: 交错群, 由 n 个物体的所有偶置换构成, 是 S_n 的子群, 阶为 $\frac{n|}{2}$.
- 典型群: 从线性代数和矩阵理论得到的群, 如一般线性群 GL_n, 特殊线性群 SL_n，正交群，酉群和辛群.

2.1.2. *子群*. 群 G 的子群 H, 记为 $H \leq G$，是 G 的子集合并且对乘法和求逆封闭. $\{1\}$ 和 G 是 G 的平凡子群. 阶为 n 的有限群都是对称群 S_n 的子群 (Cayley 定理). 对于 $H \leq G$, 左 (右)a 陪集是指集合 $gH = \{gh \mid h \in H\}$ (或 Hg). 群 G 是子群 H 的不相交左陪集 (或右陪集) 的并. 特别地, 如果 G 是有限群, 那么子群 H 的阶总是 G 的阶的因子 (拉格朗日定理).

2.1.3. *正规子群*. 1 子群 N 称为群 G 的正规子群是, 记为 $N \triangleleft G$, 是指它对于共轭封闭, 即若 $x \in N$ 则 $g^{-1}xg \in N$ 对所有 $g \in G$ 成立. 我们有

$$\mathrm{SL}_n(\mathbb{F}) \triangleleft \mathrm{GL}_n(\mathbb{F}), \quad A_n \triangleleft S_n.$$

更进一步地,

- $\{1\}$ 和 G 是 G 的平凡正规子群, 而 G 称为单群是指 G 没有非平凡正规子群.
- 若 $N \triangleleft G$, 则 G/N 还是群, 称为 G 的商群.

2.1.4. *群同态*. 群同态 $\varphi : G \to G'$ 是指群之间保持乘法运算的映射, 即 $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$, 它的像 $\mathrm{im}(\varphi)$ 是 G' 的子群, 它的核 $\ker(\varphi)$ 是 G 的正规子群, 且诱导映射 $G/\ker(\varphi) \to \mathrm{im}(\varphi)$ 是典范同构 (同态基本定理).

2.1.5. *可解群*. 有限群 G 称为可解群是指存在有限序列

$$G_0 = \{1\} \triangleleft G_1 \triangleleft \cdots \triangleleft G_r = G,$$

使得 G_{i+1}/G_i 是阿贝尔群 (或循环群) 对所有 $0 \le i \le r-1$ 成立.

- 有限阿贝尔群都是可解群.
- S_3, S_4 和 A_4 是可解的. 例如,

$$\{1\} \triangleleft K_2 = \{(12)(34), (14)(23), (13)(24)\} \triangleleft A_4 \triangleleft S_4.$$

- 伯恩赛德定理: 若 $|G| = p^aq^b$, 其中 p, q 是素数, 则 G 是可解群.

定理 2 (Galois). *若 $n \ge 5$, 则 A_n 是单群因此不是可解群, 故 S_n 不是可解群.*

2.2. 域扩张基本理论.

2.2.1. *域*. 域 F 是配备有两种二元运算: 加法 $+$ 和乘法 $\times$, 的集合, 且满足条件: $(F, +)$ 是阿贝尔群其单位元是 0, $(F - \{0\}, \times)$ 是阿贝尔群其单位元 1, 且加法与乘法满足分配律. 下面是一些熟知的域的例子:

- 有理数域 $\mathbb{Q}$, 实数域 $\mathbb{R}$ 和复数域 $\mathbb{C}$.
- 设 p 是素数, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ 是 p 元有限域.

2.2.2. *域扩张*. 如果 F 是 E 的子域, 那么我们称 E/F 是域扩张. 此时 E 是典范 F-向量空间. 域扩张 E/F 的扩张次数定义为 $[E : F] = \dim_F E$, 即 E 作为典范 F-向量空间的维数.

- $\mathbb{C}/\mathbb{R}$ 是扩张次数为 2 的扩张, $\mathbb{R}/\mathbb{Q}$ 是无限扩张.
- 令 $q = p^f$, 则 $\mathbb{F}_q/\mathbb{F}_p$ 是次数 f 的域扩张.

定理 3. *若 $K/E/F$ 是域扩张, 则 $[K : F] = [K : E] \cdot [E : F]$.*

2.2.3. 域的构造. 构造新的域和域扩张一个通用办法如下: 设 R 是交换环而 $\mathfrak{m}$ 是它的一个极大理想, 那么商环 $R/\mathfrak{m}$ 是一个域.

- 取 $R=\mathbb{Z}$ 而 $\mathfrak{m}-p\mathbb{Z}$, 我们就得到 $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$.
- 设 F 是域, $p(x)$ 是 F 上次数 n 的不可约多项式. 那么 $F[x]/(p(x))$ 是 F 的一个次数 n 的有限扩张.

2.2.4. 代数与超越扩张. 设 E/F 是域扩张而 $\alpha\in E$. 域

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

是 F 的一个扩张. α 称为代数元或者在 F 上代数如果 $[F(\alpha):F]$ 有限, 而称为超越元或者在 F 上超越如果 $[F(\alpha):F]$ 无限. E/F 称为代数扩张如果 E 中每个元素都在 F 上代数，称为超越扩张如果 E 中存在在 F 上超越的元素.

- 有限扩张都是代数扩张.
- $\mathbb{R}/\mathbb{Q}$ 是超越扩张.
- $F(x)$, 即 F 的一元有理函数域, 是 F 的超越扩张. 同样 n 元有理函数域 $F(x_1,\cdots,x_n)$ 也是.

设 $\alpha_1,\cdots,\alpha_n$ 在 F 的某个扩域里. 那么

$$F(\alpha_1,\cdots,\alpha_n)=\left\{\frac{f(\alpha_1,\cdots,\alpha_n)}{g(\alpha_1,\cdots,\alpha_n)}\,\middle|\, f,g\in F[x_1,\cdots,x_n],g(\alpha_1,\cdots,\alpha_n)\neq 0\right\}$$

是 F 的 $\alpha_1,\cdots,\alpha_n$ 生成的扩域. 域扩张 E/F 称为有限生成扩张是指存在 $\alpha_1,\cdots,\alpha_n$，使得 $E=F(\alpha_1,\cdots,\alpha_n)$. 若 $E=F(\alpha)$ 对某个 α 成立, 则 E 被称为是 F 的单扩张.

命题 1. (1) 有限扩张和有限生成代数扩张是同一个意思.

(2) 素数次扩张都是但扩张.

定理 4. 设 E/F 是域扩张, $\alpha\in E$. 令 $\mathrm{ev}:F[x]\to F[\alpha]$, $x\mapsto\alpha$ 是赋值映射.

(1) 若 α 在 F 上超越, 则 ev 扩充为域同构 $F(x)\cong F(\alpha)$.

(2) 若 α 在 F 上代数, 则存在唯一首一不可约多项式 $p(x)$, 使得赋值映射诱导域同构 $F[x]/(p(x))\cong F(\alpha)=F[\alpha]$. 此时, $F(\alpha):F]=\deg p(x)$ 而 $\{\alpha^i\mid 0\leq i<\deg p(x)\}$ 是 $F(\alpha)$ 作为 F-向量空间的一组基, 即 $F(\alpha)$ 中任意元素可以唯一写为 $\sum_{i=0}^{\deg p-1}a_i\alpha^i$ 的形式，其中 $a_i\in F$.

上述定理的多项式 $p(x)$ 称为 α 的最小多项式.

2.2.5. 代数闭域和代数闭包. 域 F 称为代数封闭域是指所有非常值多项式 $f(x) \in F[x]$ 在 F 中均有根. 代数基本定理就是说 $\mathbb{C}$ 是代数闭域.

设 F 为域. 域扩张 E 称为 F 的代数闭包是指 E 是 F 的代数扩张且每个非常值多项式 $f(x) \in F[x]$ 在 E 中均有根. 对于任何域, (在同构意义下) 存在唯一的代数闭包, 闭包本身是代数闭域.

注记 2. 此后, 域 F 的代数扩张均假设是包含在 F 的某个确定的代数闭包 $\overline{F}$ 里.

例 3. 有限域 $\mathbb{F}_p$ 的代数闭包 $\overline{\mathbb{F}}_p = \bigcup_m \mathbb{F}_{p^m}$.

设 α 是 F 的代数闭包里面的元素, 设 $p(x)$ 是它在 F 上的最小多项式, $p(x)$ 的根称为 α 的共轭元或者 F-共轭元. 注意到对于非零多项式 $f(x) \in F[x]$, F 的任何域扩张中最多存在 $\deg(f)$ 个根 (拉格朗日定理).

2.2.6. 域的同态. 设 E 和 F 是域, $\sigma : F \to E$ 是同态 (因此 $\sigma(0) = 0$ 且 $\sigma(1) = 1$), 故 $\ker\sigma = 0$, σ 一定是域的嵌入.

设 E 和 E' 是域 F 的扩张, 同态 $\sigma : E \to E'$ 称为 F-同态是指 $\sigma|_F$=id, 即 $\sigma(x) = x$ 对所有 $x \in F$ 成立. 对于 F-同态有个值得注意的关键事实: 若 $\alpha \in E$ 而 $p(x) \in F[x]$ 使得 $p(\sigma) = 0$, 则 $\sigma(p(\alpha)) = p(\sigma(\alpha)) = 0$, 因此 α 的像 $\sigma(\alpha) \in E'$ 也一定是 $p(x)$ 的根.

命题 2. *设 E 是 F 上次数为 n 的单扩张. 则对于任意域扩张 E'/F, 从 E 到 E' 最多存在 n 个 F-同态.*

证明. 设 $E = F(\alpha)$. α 的最小多项式 $p(x)$ 次数为 n, 它 • 在 E' 中最多有 n 个根, 故 α 的像最多有 n 种可能, 但 F-同态完全由 α 的像决定. □

若 $E = E'$ 是 F 的有限扩张, 那么任意 F-同态 $\sigma : E \to E$ 是有限维线性空间的单 F-线性映射，因此也必须是满映射, 也就是说任何 F-同态 $E \to E$ 一定是 F-自同构. 那么命题 2 告诉我们次数 n 的单扩张最多有 n 个 F-自同构, 这个事实可以推广到一般情形：

命题 3. *对于任意有限域扩张 E/F, 存在最多 $[E : F]$ 个 F-自同构.*

3. 伽罗瓦理论

3.1. 伽罗瓦群和伽罗瓦扩张.

3.1.1. *伽罗瓦群*. 设 E/F 是域的有限扩张, E/F 的伽罗瓦群是群

$$\mathrm{Gal}(E/F) := \mathrm{Aut}_F(E) = \{\sigma : E \to E, \sigma \text{ 是}F\text{-自同构}\},$$

其中群的乘法运算是映射的复合. 则命题 3 说明 $\mathrm{Gal}(E/F)$ 是阶 $\leq [E:F]$ 的有限群.

定义 1. 若 $|\mathrm{Gal}(E/F)| = [E:F]$, 则称 E/F 为伽罗瓦扩张,.

例 4. 令 $E = \mathbb{Q}(\sqrt[3]{2})$. $\sqrt[3]{2}$ 在 E 中唯一的 $\mathbb{Q}$-共轭元是它自己, 故 $\mathrm{Gal}(E/Q) = 1$, 因此 $E/\mathbb{Q}$ 不是伽罗瓦扩张.

例 5. 令 $F = \mathbb{F}_p(x)$, $E = F(\alpha)$ 其中 α 满足条件 $\alpha^p = x$. 由于 α 的最小多项式是 $X^p - x = (X-\alpha)^p$, 故 $\mathrm{Gal}(E/F) = 1$, E/F 不是伽罗瓦扩张.

例 6. 设 $F = \mathbb{F}_q$ 而 $E = \mathbb{F}_{q^m}$, 则:

(1). $[E:F] = m$.

(2). $E^\times = \mathbb{F}_{q^m}^\times$ 是阶为 $q^m - 1$ 的循环群, 令 α 是 $E^\times$ 的一个生成元而 $p(x)$ 是 α 在 $F = \mathbb{F}_q$ 上的最小多项式, 则 $\deg p(x) = m$.

(3). 对于 $c \in \mathbb{F}_q, c^q = c^{q-1} \cdot c = c$, 因此 $p(\alpha^q) = p(\alpha)^q = 0$, 故 $\alpha, \alpha^q, \cdots, \alpha^{q^{m-1}}$ 是 $p(x)$ 的不同根, 所以

$$p(x) = (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{m-1}}).$$

(4). 可以验证 $\sigma_q : E \to E, t \mapsto t^q$ 是 E 的 F-自同构 (q-Frobenius). 因此 $\sigma_q \in \mathrm{Gal}(E/F)$, 并且由于 $\sigma_q^m = 1$ 而 $\sigma_q^i \neq 1$ for $i < m$, 故子群 $\langle \sigma_q \rangle$ 的阶为 $m = [E:F] \geq |\mathrm{Gal}(E/F)|$. 所以 E/F 是伽罗瓦扩张且

$$\mathrm{Gal}(E/F) = \langle \sigma_q \rangle \cong \mathbb{Z}/m\mathbb{Z}$$

是阶为 m 的循环群.

3.1.2. *分裂域和正规扩张*.

定义 2. 设 F 是域, $f(x) \in F[x]$.

(1) $f(x)$ 在域扩张 E/F 分裂是指它在 E 中可分解为线性因子的乘积, 即

$$f(x) = a(x-\alpha_1)\cdots(x-\alpha_n), \quad \alpha_i \in E.$$

(2) $f(x)$ 在 F 上的分裂域是 F 的代数闭包内使得 $f(x)$ 分裂的最小子扩张 E_f. 换言之, 分裂域 $E_f = F(\alpha_1, \cdots, \alpha_n)$, 这里 $\alpha_i (1 \leq i \leq n)$ 是 $f(x)$ 在代数闭包内的所有根.

例 7. (1) $f(x)=(x^2-2)(x^2-3)$ 在 $\mathbb{Q}$ 上的分裂域是 $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

(2) $f(x)=x^3-2$ 在 $\mathbb{Q}$ 上的分裂域是 $\mathbb{Q}(\sqrt[3]{2},\sqrt{-3})$.

(3) $f(x)=x^{q^n}-x$ 或者任何 $\mathbb{F}_q$ 上的 n 次不可约首一多项式在 $\mathbb{F}_q$ 上的分裂域都是 $\mathbb{F}_{q^n}$.

(4) F 的代数闭包 $\overline{F}$ 即 F 上的所有非常值多项式均分裂的域.

定义 3. (1) 代数扩张 E/F 称为正规扩张是指对任意 $\alpha\in E$, 它的最小多项式 $p(x)$ 在 E 中分裂, 即 α 的所有共轭元均在 E 中.

(2) 代数扩张 L/F 的正规闭包是包含 L 的 F 的最小正规扩张 (代数闭包内).

如果 L/F 是有限扩张, 记 $L=F(\alpha_1,\cdots,\alpha_t)$, 令 E 是 $\alpha_1,\cdots,\alpha_t$ 的所有共轭元生成的域. 则 E 是 L/F 的正规闭包.

例 8. $L=\mathbb{Q}(\sqrt[3]{2})$ 在 $\mathbb{Q}$ 上的正规闭包是 $\mathbb{Q}(\sqrt[3]{2},\sqrt{-3})$.

3.1.3. 可分扩张.

定义 4. (1) 不可约多项式 $f(x)\in F[x]$ 称为可分的是指它在 F 的代数闭包里没有重根, 等价地，即指 $\gcd(f(x),f'(x))=1$.

(2) 一般多项式 $f(x)$ 称为可分多项式是指它的不可约因子都是可分的, 否则称 $f(x)$ 是不可分的.

定义 5. 设 E/F 是代数扩张.

(1) 元素 $\alpha\in E$ 称为在 F 上可分是指它在 F 上的最小多项式 $p(x)\in F[x]$ 可分.

(2) E/F 称为可分扩张是指 E 的所有元素在 F 上均可分，否则, 它称为不可分扩张. E/F 称为纯不可分扩张是指 $E\backslash F$ 中没有可分元.

设 E/F 是代数扩张. 则在 F 上代数的所有元素集合构成 E 的子域. F 的可分闭包是 F 的可分扩张使得所有可分多项式均分裂, 即代数闭包 $\overline{F}$ 的可分元构成的子域.

例 9. (1) 有限域的代数扩张均是可分扩张.

(2) 如果 F 是特征 0 的域 (比如说 $\mathbb{C}$ 的子域), 那么 F 的任何代数扩张均是可分扩张, 因此代数闭包和可分闭包是同一个域.

(3) 设 $F=\mathbb{F}_p(x)$ 而 $E=\mathbb{F}_p(x,\sqrt[p]{x})=\mathbb{F}_p(\sqrt[p]{x})$, 则 $\sqrt[p]{x}$ 在 F 上是不可分的, 故 E/F 是不可分扩张.

下面定理在伽罗瓦理论中起着很重要的作用:

定理 5 (单扩张定理). *有限可分扩张是单扩张.*

3.1.4. *伽罗瓦扩张的等价定义.* 如下定理给出伽罗瓦扩张的等价定义:

定理 6. *设 E/F 是域的有限扩张. 则下列条件等价:*
(1) *E/F 是伽罗瓦扩张.*
(2) *E/F 是正规可分扩张.*
(3) *E 是某可分多项式 $f(x) \in F[x]$ 的分裂域.*

由此可知, 如果 L/F 是有限可分扩张, 则 L 的正规闭包 E 在 F 上是伽罗瓦扩张, 称为 L/F 的伽罗瓦闭包; 如果 f 是可分不可约多项式, 则 E_f/F 是伽罗瓦扩张, $\mathrm{Gal}(E_f/F)$ 的阶是 $\deg(f)$.

例 10. 设 $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ 而 $F = \mathbb{Q}$, 则 E 是 $(x^2-2)(x^2-3)$ 的分裂域, 故 $E/\mathbb{Q}$ 是伽罗瓦扩张. 注意到
(1). $[E : \mathbb{Q}] = 4 \Longrightarrow |\mathrm{Gal}(E/\mathbb{Q})| = 4$.
(2). 对于 $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$, σ 由 $\sigma(\sqrt{2})$ 和 $\sigma(\sqrt{3})$ 决定, 但 $\sigma(\sqrt{2}) = \pm\sqrt{2}$, $\sigma(\sqrt{3}) = \pm\sqrt{3}$. 因此 $\mathrm{Gal}(E/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\} \cong K_2$, 这里

$$\sigma(\sqrt{2}) = -\sqrt{2},\ \sigma(\sqrt{3}) = \sqrt{3};$$
$$\tau(\sqrt{2}) = \sqrt{2},\ \tau(\sqrt{3}) = -\sqrt{3}.$$

例 11. 设 $p > 2$ 是素数, p 次分圆多项式 $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p-1}{x-1}$ 是不可约多项式, 它是 ζ_p 的最小多项式, 因此 $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$. 对于 $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, $\sigma(\zeta_p) = \zeta_p^a$, 这给出单同态: $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to (\mathbb{Z}/p\mathbb{Z})^\times, \sigma \mapsto a$. 由于两边的阶都是 $p-1$，我们知道 $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ 是阶为 $p-1$ 的循环群.

3.2. 伽罗瓦理论基本定理. 设 E/F 是有限伽罗瓦扩张, $G = \mathrm{Gal}(E/F)$. 则很清楚 G 作用在域 E 上且 F 被 G-作用固定. 更进一步地, 对于子群 $H \leq G$, 记 $E^H := \{x \in E \mid h(x) = x, \text{ 对所有 } h \in H \text{ 成立}\}$, 它是 E 的子域, 称为 H 的不变域.

定理 7. *设 E/F 是有限伽罗瓦扩张, $G = \mathrm{Gal}(E/F)$. 则存在一一对应, 将 E/F 的中间域集合映射到 G 的子群集合:*

$$\begin{array}{ccc} L & \longrightarrow & \mathrm{Gal}(E/L) \\ E^H & \longleftarrow & H \end{array}$$

使得

(1) 对所有的 E 的中间域 L, E/L 是伽罗瓦扩张, 即 $[E:L]=\mathrm{Gal}(E/L)$.

(2) 对所有 G 的子群 H, $|H|=[E:E^H]$.

(3) L/F 是伽罗瓦扩张当且仅当 $H=\mathrm{Gal}(E/L)$ 是 G 的正规子群, 此时同构 $G/H\cong\mathrm{Gal}(L/F)$ 由 $g\mapsto g|_L$ 诱导给出.

例 12. 设 $E=\mathbb{Q}(\sqrt{2},\sqrt{3})$, 则 $G=\mathrm{Gal}(E/\mathbb{Q})=\{1,\sigma,\tau,\sigma\tau\}$, 其中 $\sigma:\sqrt{2}\mapsto-\sqrt{2},\ \sqrt{3}\mapsto\sqrt{3}$ and $\tau:\sqrt{2}\mapsto\sqrt{2},\ \sqrt{3}\mapsto-\sqrt{3}$.

G 有 5 个子群: $\{1\},\{1,\sigma\},\{1,\tau\},\{1,\sigma\tau\}$ 和 G, 分别对应 E 的 5 个子域: $E,\mathbb{Q}(\sqrt{3}),\mathbb{Q}(\sqrt{2}),\mathbb{Q}(\sqrt{6})$ 和 $\mathbb{Q}$.

由基本定理, 立刻可以看出 $E^G=F$. 事实上我们有

定理 8. 设 G 是有限群, 作用于域 E 上. 则 E/E^G 是伽罗瓦扩张, 它的伽罗瓦群是 G.

例 13. 设 K 是域, $E=K(x_1,\cdots,x_n)$ 是 K 的 n 元有理函数域. 设 s_i 是 $x_1,\cdots,x_n$ 的 i 次基本对称多项式:

$$s_i=\sum_{1\le k_1<\cdots<k_i\le n}x_{k_1}\cdots x_{k_n}.$$

对称群 S_n 通过 $\sigma(x_i)=x_{\sigma(i)}$ 作用于 E, 且 $E^{S_n}=K(s_1,\cdots,s_n)$. 故 E/E^{S_n} 是伽罗瓦扩张，它的伽罗瓦群是 S_n.

4. 伽罗瓦理论的应用

4.1. 根式扩张.

定义 6. 有限扩张 E/F 称为根式扩张是指存在域扩张序列

$$F=F_0\subseteq F_1\subseteq\cdots\subseteq F_r=E$$

使得 $F_{i+1}=F_i(\sqrt[k_i]{a_i})$ 对于某 $a_i\in F_i$ 和 $k_i\in\mathbb{Z}_+$ 成立. 换言之, E/F 是根式扩张是指 E 的任何元素均可以通过对 F 的元素经过有限步加、减、乘、除和开方运算得来.

下面这些定理给出次数 ≥5 的一般多项式根式不可解:

定理 9 (伽罗瓦). 设 F 是 $\mathbb{C}$ 的子域, 令 a_i $(0\le i\le n-1)$ 是 F 上的未定元, $K=F(a_0,a_1,\cdots,a_{n-1})$. 设 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0=(x-r_1)\cdots(x-r_n)$. 则 $N=F(r_1,\cdots,r_n)$ 是 K 的伽罗瓦扩张且 $\mathrm{Gal}(N/K)\cong S_n$.

注记 3. 若 $\sigma \in \mathrm{Gal}(N/K)$, 则 $\sigma : r_i \mapsto r_j$, 因此 σ 诱导了 $\{r_1, \cdots, r_n\}$ 的置换, 这定义了群的单同态 $\mathrm{Gal}(N/K) \hookrightarrow S_n$. 伽罗瓦的结果告诉我们这个单同态其实是同构.

定理 10 (阿贝尔-伽罗瓦). 设 F 是 $\mathbb{C}$ 的子域, $f(x) \in F[x]$ 而 E_f 是 $f(x)$ 在 F 上的分裂域. 则

(1) E_f 是 F 的根式扩张当且仅当 $G_f = \mathrm{Gal}(E_f/F)$ 是可解群.

(2) 若 f 不可约, $\deg f = n \geq 5$ 且 f 处于一般位置, 则 $G_f \cong S_n$ 故 E_f 不是 F 的根式扩张.

4.2. 回到三次和四次方程情形.

4.2.1. 三次方程. 只需考虑方程 $x^3 + px + q = 0$，其中 p 和 q 是未定元. 设 $K = \mathbb{Q}(p, q, j)$, 这里 j 是 3 次本原单位根. 设 N 是 $x^3 + px + q$ 在 K 上的分裂域, 则由伽罗瓦知 $\mathrm{Gal}(N/K) \cong S_3$. 设方程的三个根是 a, b 和 c. 则 S_3 可以等同为 a, b, c 的置换. 令 $\sigma = (abc)$, 则 $\sigma^2 = (acb)$, 交错群 $A_3 = \{1, \sigma, \sigma^2\}$. 注意到

$$\Delta := (a-b)^2(b-c)^2(c-a)^2 \in K,$$
$$\delta = \sqrt{\Delta} := (a-b)(b-c)(c-a) \notin K,$$

这是因为 Δ 被所有置换固定而 δ 不被 (ab) 固定. 由伽罗瓦理论, 包含在 N/K 中的唯一二次子扩张是 $K(\delta)$. 由于 $[N : L] = 3$ 是素数, 故对任意 $\alpha \notin L$, 一定有 $N = L(\alpha)$.

$$\begin{array}{ccc} 1 & & N = L(\alpha) \\ \Big| 3 & & \Big| 3 \\ A_3 & & L = K(\delta) \\ \Big| 3 & & \Big| 3 \\ S_3 & & K \end{array}$$

拉格朗日定义了所谓的拉格朗日预解式:

$$(j, a) = a + jb + j^2 c.$$

类似地可以定义 (j^2,a). 注意到 $(j,a)\neq 0$. 事实上, 若 $(j,a)=0$, 则 $\sigma(j,a)=\sigma^2(j,a)=0$, 因此

$$\begin{pmatrix} a & b & c \\ b & c & a \\ c & a & b \end{pmatrix}\begin{pmatrix} 1 \\ j \\ j^2 \end{pmatrix}=0,$$

这不可能，因为左边的矩阵的行列式即 $\delta\neq 0$. 由 $\sigma(j,a)=j^2(j,a)$, 我们得到 $(j,a)\notin L$ 且 $N=L((j,a))$.

由韦达定理, 我们知道

$$a+b+c=0,\ ab+bc+ca=p,\ abc=-q.$$

因此 d 和 δ 可记为 p 和 q 的组合:

$$d=-27q^2-4p^3,\quad \delta=\pm\sqrt{-27q^2-4p^3}.$$

经计算知

$$(j,a)^3=(a+jb+j^2c)^3=-\frac{27}{2}q-\frac{3\sqrt{-3}}{2}\delta.$$

因此我们得到 (j,a) 的三个值. 类似地 $(j^2,a)^3=-\frac{27}{2}q+\frac{3i\sqrt{3}}{2}8\delta$. 更进一步地, (j,a) 和 (j^2,a) 由下述关系关联:

$$(j,a)(j^2,a)=-3p.$$

因此我们得到 (j,a) 和 (j^2,a) 的三组值. 最后由关系

$$\begin{cases} 3a=(j,a)+(j^2,a) \\ 3b=j^2(j,a)+j(j^2,a) \\ 3c=j(j,a)+j^2(j^2,a) \end{cases}$$

即给出 a,b,c 的值.

4.2.2. *四次方程*. 令 p,q,r 是未定元, $K=\mathbb{Q}(p,q,r,j)$ 且 $j^3=1$. 我们考虑的四次多项式是

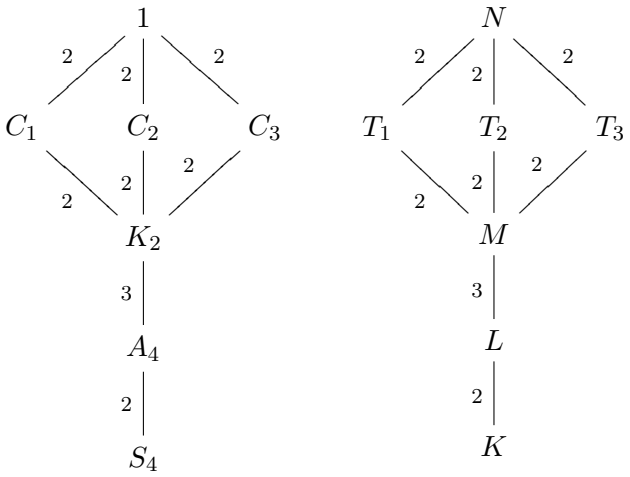
$$f(x)=x^4+px^2+qx+r=(x-a)(x-b)(x-c)(x-d).$$

设 $N=K(a,b,c,d)$ 是 $f(x)$ 的分裂域. 则 N/K 是伽罗瓦扩张，伽罗瓦群 $\mathrm{Gal}(N/K)=S_4$, 可以等同为 a,b,c,d 的置换群. 我们有序列

$$1\subseteq K_2=\{1,(ab)(cd),(ad)(bc),(ac)(bd)\}\subseteq A_4\subseteq S_4$$

而 K_2 有三个 2 阶子群:

$$C_1 = \{1, (ab)(cd)\},\ C_2 = \{1, (ac)(bd)\},\ C_3 = \{1, (ad)(bc)\}.$$



与三次方程同理我们有

$$\Delta = (a-b)^2(a-c)^2(a-d)^2(b-c)^2(b-d)^2(c-d)^2 \in K,$$
$$\delta = (a-b)(a-c)(a-d)(b-c)(b-d)(c-d) \in L\backslash K.$$

于是 $L = K(\delta)$. 令

$$u = (a+b)(c+d),\ v = (a+c)(b+d),\ w = (a+d)(b+c).$$

我们有

(1) 对于 $\sigma = (abc) \in A_4$, $\sigma(u) \neq u$, 故 $u \notin L$. 对所有 $\tau \in K_2$, $\tau(u) = u$, 故 $u \in M$, 因此 $M = L(u)$ (且 $= L(v) = L(w)$).

(2) 我们知道 $a+b \notin M$ 但 $a+b \in T_1$, 故 $T_1 = M(a+b)$. 同理 $T_2 = M(a+c)$ 且 $T_3 = M(a+d)$.

(3) 由计算可知

$$\begin{cases} u+v+w = 2p \\ uv+vw+wu = p^2-4r \\ uvw = -q^2 \end{cases}$$

故 $u, v, w,$ 是方程

$$y^3 - 2py^2 + (p^2-4r)y + q^2 = 0$$

的根, 此方程称为四次方程的预解方程. 故

$$\begin{cases}(a+b)+(c+d)=0\\(a+b)(c+d)=u\end{cases}\Longrightarrow\quad\begin{cases}a+b=\sqrt{-u},\\c+d=-\sqrt{-u}.\end{cases}$$

类似地,

$$a+c=\sqrt{-v},\ b+d=-\sqrt{-v},\ a+d=\sqrt{-w},\ b+c=-\sqrt{-w},$$

于是就得到 a,b,c,d.

4.3. 其他应用.

定理 11. *若 $f(x)\in\mathbb{Q}[x]$ 是素数 $p\geq 5$ 次不可约多项式且只有两个虚根, 则 $G_f\cong S_p$.*

证明. 令 E 是 $f(x)$ 的分裂域. 我们有

(1) 映射 $G_f\to S_p$, $\sigma\mapsto f(x)$ 的所有根的诱导置换是单同态, 因此可以将 G_f 视为 S_p 的子群.

(2) 由 $\deg f=p$, $p\mid[E:\mathbb{Q}]$, 故 G_f 包含 p-轮换.

(3) 令 τ 是复共轭, 则 $\tau|_E\in G_f$ 固定所有实根而互换两个虚根, 因此 $\tau|_E$ 是 2-轮换.

(4) 一个 2-轮换 (ij) 和一个 p-轮换 $(a_1a_2\cdots a_p)$ 生成 S_p. □

定理 12 (伽罗瓦). *若 $f(x)$ 是 $K\subseteq\mathbb{C}$ 上素数次不可约多项式, $x_1,\cdots,x_p$ 是 $f(x)$ 的根而 $N=K(x_1,\cdots,x_p)$, 则 N/K 是根式扩张当且仅当 $N=K(x_i,x_j)$ 对任意对 $i\neq j$ 成立, 即所有其他根都是某两个根的有理函数.*

下面定理是域论中关于尺规作图的主要定理:

定理 13. *对于 $\alpha_1,\cdots,\alpha_k\in\mathbb{R}$, 令 $F=\mathbb{Q}(\alpha_1,\cdots,\alpha_k)$. 则数 $\alpha\in\mathbb{R}$ 可以从给定点 $0,1,\alpha_1,\cdots,\alpha_k$ 出发通过尺规作图构造出来当且仅当存在二次域扩张塔: $F=F_0\subseteq F_1\subseteq\cdots\subseteq F_k$ 使得 $\alpha\in F_k$.*

例 14. (1) 倍方问题: 能否从 $\mathbb{Q}$ 出发, 构造 $\sqrt[3]{2}$? 由于 $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$, 故不存在二次扩张塔使得 $\sqrt[3]{2}$ 在塔中, 因此倍方问题无解.

(2) 三等分角问题. 由于 $\cos 3\theta=4\cos^3\theta-3\cos\theta$, 三等分角问题即问: 给定 $t=\cos 3\theta$, 能否构造 x 使得 $4x^3-3x-t=0$? 由于一般而言 $[\mathbb{Q}(x,t):\mathbb{Q}(t)]=3$, 例如当 $\theta=\frac{\pi}{9},t=\frac{1}{2}$ 时, 因此三等分角也是不可能的.

伽罗瓦理论给出如下的高斯的著名结果:

定理 14 (高斯). *正 p 边形可以用直尺和圆规构造出来当且仅当 $p = 2^{2^n}+1$ 是费马素数.*

证明. 一方面, 正 p 边形的可构造性说明 $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$ 一定是 2 的幂次, 故 p 必然是费马素数. 另一方面, 如果 p 是费马素数, 那么 $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ 是 2 的幂次阶循环群, 它有指数 2 的子群序列, 由伽罗瓦理论这对应于 $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ 的指数为 2 的子扩张序列, 故 ζ_p 和正 p 边形可构造. □

CHAPTER 3

库默尔和代数数论的诞生

1. 库默尔之前的数论

简而言之, 库默尔之前的数论可以如下概括: 两部伟大的著作, 即欧几里得的《几何原本》(The Elements , 大约公元前 300 年) 和卡尔弗里德里希高斯 (1777 年-1855 年) 的《算术研究》(Disquisitiones Arithmeticae,1801 年); 四个伟大的定理: 算术基本定理, 费马小定理 (和它的推广欧拉定理)，中国剩余定理和高斯的二次互反律; 和一个伟大的问题即费马大定理.

我们首先回顾一下同余的定义. 对于整数 $m > 1$ (称为模数), 同余关系 $a \equiv b \bmod m$ 即指 $m \mid (x - y)$, 亦即 x 和 y 被 m 除有相同的余数. 同余条件是等价条件. 模 m 的同余类个数就是 m.

1.1. 两部伟大的著作.

1.1.1. *《几何原本》*. 《几何原本》也称《原本》, 可能是有史以来最重要也最成功的教科书, 是欧几里得在公元前 300 年左右写作的几何和数论的经典巨著. 《几何原本》分为 13 册 (章), 其中第 7-9 章讨论了自然数和整数的理论. 这是数论在历史上的真正开始, 里面包含了许多有关自然数和整数的定理.

在《原本》中有关数论中的伟大定理包括欧几里得第一定理, 这个定理我们将在稍后细讲，和欧几里得第二定理, 它说明素数有无穷多个. 这个漂亮定理由欧几里得在命题 9.20 证明, 这是数学史上第一个有关无限的定理. 我们来看一下欧几里得的优雅证明:

定理 15. *存在无穷多个素数.*

证明. 若不然, 设素数个数有限, 所有的素数为 $p_1, \cdots p_n$. 令 $N = p_1 \cdots p_n + 1$. 则 N 的素因子一定是一个新的素数, 矛盾. □

欧几里得算法, 也就是用来求两个数的最大公约数的算法, 出现在《原本》的第 7 章. 这是最早的整数算法, 但现在还在计算机上广泛使用.

1.1.2. *《算术研究》*. 这部经典是高斯最重要的数学著作, 1801 年出版时他年仅 24 岁. 这本书可以被认为是经典初等数论的终结和代数数论的开始.

在书中高斯首先概括总结了前人的工作, 然后勇敢地迈向更新更深刻的前沿研究.

高斯在书中给出了算术基本定理的第一个现代证明. 为陈述方便, 他引入了同余符号. 通过这个发明, 他可以用一种很优雅的方式来陈述他之前的数论研究.

高斯还给出了二次互反律的第一个严格证明. 他的工作揭示了数论最初考虑的问题和它的各分支间的丰富联系, 这个联系他认为对于这门学科的重要性十分巨大. 他扩充了拉格朗日的二次型理论, 证明两个二次型可以乘起来得到第三个二次型. 后世数学家将这个工作重新组织一下, 就得到有限交换群的一个重要例子. 在书的最后一章，高斯给出了尺规作图的理论 (定理 14)，这是他作为数学家的第一个发现: 正 17 边形可以由直尺和圆规构造. 丹麦数学史学家 Asger Aaboe (1922-2007) 是如此评论《算术研究》的:

> ” 不管以什么样的标准来考量, 高斯的《算术研究》都毫无疑问是数学所有领域任何时期最重要的经典之一.”

1.2. 四个伟大定理.

1.2.1. *算术基本定理.* 这个定理又叫唯一因子分解定理, 它是说

定理 16. *每个大于 1 的正整数都可以唯一分解为有限多个素数的乘积.*

这个定理第一个严格证明出现在高斯的《算术研究》, 但它是《几何原本》中的欧几里得引理 (欧几里得第一定理) 的推论:

定理 17. *若素数 $p \mid ab$, 则 $p \mid a$ 或 $p \mid b$.*

1.2.2. *费马小定理和欧拉定理.* 皮埃尔 • 德 • 费马 (Pierre de Fermat, 1601-1665) 是法国数学家, 通常被称为现代数论之父. 他独立于勒内 • 笛卡尔 (René Descartes, 1596-1650), 创立了解析几何基本原则. 通过与布莱士 • 帕斯卡 (Blaise Pascal, 1623-1662) 的通信, 他们一起创立了概率论. 费马一直以来最喜欢的领域是数论, 但很不幸他找不到同好来分享他对数论的热情.

费马小定理, 现在还在素性判定中起重要作用, 即

定理 18. *若 p 是素数, 则对于任意不被 p 整除的整数 a, $a^{p-1} \equiv 1 \bmod p$, 即 $p \mid a^{p-1} - 1$.*

注意到欧拉函数 $\varphi : n \mapsto \varphi(n)$, $\varphi(n)$ 是乘法群

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a \mid 0 < a < n,\ \gcd(a, n) = 1\}$$

的阶. 则 $\varphi(p) = p - 1$. 这样费马小定理由瑞士伟大数学家莱昂哈德 • 欧拉 (Leonhard Euler, 1707-1783) 推广为如下定理:

定理 19. 设 n 是正整数. 则对于任何与 n 互素的整数 a, $a^{\varphi(n)} \equiv 1 \bmod n$, 即 $n \mid a^{\varphi(n)} - 1$.

自然欧拉定理可以看作是拉格朗日定理: 群的元素的阶一定整除群的阶, 的特殊情形.

1.2.3. 中国剩余定理. 这个定理, 来源于三世纪的《孙子算经》中的一个问题, 后来在中国被称为孙子定理, 可能是中国数学家发现的最伟大的定理. 今天中国剩余定理是环论和模论的一个系统性的定理, 大家很容易在初等数论或者抽象代数任何教科书中找到它.

具体说来, 中国剩余定理是有关线性同余方程组的求解的.

定理 20. 设 m 和 n 是互素的整数. 则同余方程组

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases}$$

可解而且它的解集构成模 mn 的一个同余类.

1.2.4. 二次互反律. 设 p 是素数. 对于 $a \in \mathbb{Z}$, 勒让德符号

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{如果 } p \nmid a \text{ 且 } a \mod p \text{ 是平方;} \\ -1, & \text{如果 } a \mod p \text{ 不是平方;} \\ 0, & \text{if } p \mid a. \end{cases}$$

我们可以假设 p 是奇素数. 由定义 $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$, 故由算术基本定理, 勒让德符号 $\left(\frac{a}{p}\right)$ 由 $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ 和 $\left(\frac{q}{p}\right)$ ($q \neq p$ 是奇素数) 的值决定. 首先可以求得

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \tag{4}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \tag{5}$$

二次互反律是高斯证明的下述定理:

定理 21 (Gauss). 设 p 和 q 是不同的奇素数. 则

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \tag{6}$$

这个深刻结果首先由欧拉猜想, 勒让德给了一个错误的证明. 这是现代数论的开始. 从此以后，寻求高阶互反律就成为数论研究的一个主旋律.

1.3. 一个伟大的问题：费马大定理. 这个断言可能是数学史上最伟大的断言了. 在 1637 年阅读丢番图的《算术》时, 费马在书的页边写道: “将一个立方分为两个立方，四次方分为两个四次方, 或者更一般地一个幂方分为两个与它幂次次数相同的幂方都是不可能的.” 他接着说道 “我有一个真正美妙的证明, 但页边太窄我写不下.” 用数学记号来说, 这个后人称为费马大定理的断言是说:

问题 1. 对于 $n \leq 3$, $x^n + y^n = z^n$ 没有非平凡的整数解, 即不存在解 $(x, y, z) \in \mathbb{Z}$ 使得 $xyz \neq 0$.

自费马大定理提出之后 3 个半世纪里, 它击败了所有对它的证明企图, 赢得了数学上最著名的未解决问题的赫赫声名.

1.4. 解析数论的诞生. 欧拉首先开始使用分析工具研究数论. 1737 年, 欧拉引入了欧拉-黎曼 zeta 函数

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \ (s \in \mathbb{R},\ s > 1),$$

并且得到了欧拉乘积, 即对于 $s > 1$,

$$\zeta(s) = \prod_{p\ prime} \frac{1}{1 - p^{-s}}.$$

根据这个乘积再由于调和级数是发散的这一事实, 他给出了欧几里得第二定理 (定理 15), 即素数有无限多个, 的另一个证明.

勒热纳 • 狄利克雷 (Lejeune Dirichlet, 1805-1859) 推广了欧几里得的定理, 在 1837 年证明所有首项和公差互素的算术级数中有无穷多个素数. 这个结果高斯曾经猜想过. 狄利克雷引入了现今所谓的狄利克雷级数的复函数, 并运用分析的方法来证明他的定理. 这个令人惊讶但十分原创性的方法标志着数论一个新分支—解析数论—的诞生.

1.5. 发展高次互反律的尝试. 由于高斯在整数理论上的工作的激励, 特别是他对于二次互反律的证明, 很多年轻的德国数学家, 包括雅可比, 艾森斯坦和库默尔, 被吸引到数论领域来发展高次互反律.

2. 库默尔之前费马大定理的状态

平方和的研究历史悠久, 从古巴比伦人开始就有了这方面的研究. 例如他们发现了 $119^2 + 120^2 = 169^2$. 由初等技巧我们知道

定理 22. *正整数对 (a, b, c) 若满足条件*

(1) $a^2 + b^2 = c^2$,

(2) a, b, c *互素,*

(3) b *是偶数,*

则一定是如下形式

$$a = m^2 - n^2,\ b = 2mn,\ c = m^2 + n^2,\ (\gcd(m, n) = 1 \quad 2 \mid mn).$$

费马声称奇素数是两平方和当且仅当它具有 $4k + 1$ 的形式. 这个结果 (和费马声称的许多其他结果) 最终由欧拉证明. 约瑟夫-路易 • 拉格朗日 (Joseph-Louis Lagrange, 1736-1813) 于 1770 年证明拉格朗日四平方和定理:

定理 23. *任意正整数都是最多四个整数的平方和.*

在算术研究中高斯证明了他的三平方和定理:

定理 24. *正整数 n 是三平方和当且仅当它不是 $4^k(8m + 7)$ 的形式.*

费马大定理是关于高次幂和的. 首先 $n = 4$ 的情形由费马亲自证明. 他发明了无穷递降法来证明 $x^4 + y^4 = z^2$ 在 $\mathbb{Z}$ 上没有非平凡解. 这个方法在怀尔斯于 1995 年最终证明费马大定理时起到重要作用. 欧拉证明了 $n = 3$ 的情形, 尽管他的证明有点小错误. 欧拉的证明与形如 $a + b\sqrt{-3}$ (a 和 b 为整数) 相关. 他的方法引导了我们下面要给出的库默尔的重大发现.

若 $n = 5$, 假设 (x, y, z) 是费马方程的本原解, 则 $10 \mid xyz$. 这时有两种情况需要考虑: (i) x, y, z 中有一个被 10 整除, (ii) x, y, z 中一个是偶数而另外一个被 5 整除. 1825 年, 狄利克雷证明了情形 (i), 接着勒让德证明了情形 (ii). 狄利克雷的证明 (这是他的第一篇文章) 让他声名鹊起. 他后来还证明了 $n = 14$ 的情形并且几乎证明了 $n = 7$ 的情形, 此情形最终被加布里埃 • 拉梅 (Gabriel Lamé, 1795-1870) 证明.

要证明费马大定理, 总可以假设

$n = l$ 是奇素数, x, y, z 两两互素, 且或者 (I) $l \nmid xyz$ 或者

(II) $l \mid z$ (hence $l \nmid x$).

法国女数学家索菲 • 热尔曼 (Sophie Germain, 1776-1831) 证明了如下定理, 这是库默尔在 1840 年代的发现之前在费马大定理方面最重要的结果.

定理 25. *如果存在辅助素数 p, 使得*

(1) 若 $A^l + B^l + C^l \equiv 0 \mod p$, 则 A, B, C 中必有一个被 p 整除,

(2) $X^l \equiv l \mod p$ 无解,

那么费马大定理的情形 I 对于 l 是正确的.

证明. 假设 x, y, z 两两互素, 与 l 互素且 $x^l + y^l + z^l = 0$. 则

$$-x^l = y^l + z^l = (y+z)\sum_{i=0}^{l-1}(-1)^i y^i z^{l-1-i}.$$

注意到

$$\begin{aligned}\gcd(y+z, \sum_{i=0}^{l-1}(-1)^i y^i z^{l-1-i}) &= \gcd(y+z, \sum_{i=0}^{l-1}(-1)^i y^i (y+z-y)^{l-1-i}) \\ &= \gcd(y+z, ly^{l-1}) = 1,\end{aligned}$$

这是因为 $l \nmid y+z$ (否则 $l \mid x$) 且 $\gcd(y,z) = 1$. 因此,

$$y + z = a^l, \quad \sum_{i=0}^{l-1}(-1)^i y^i z^{l-1-i} = \alpha^l, \quad x = -a\alpha.$$

同理,

$$z + x = b^l, \quad \sum_{i=0}^{l-1}(-1)^i z^i x^{l-1-i} = \beta^l, \quad y = -b\beta,$$

$$x + y = c^l, \quad \sum_{i=0}^{l-1}(-1)^i x^i y^{l-1-i} = \gamma^l, \quad z = -c\gamma.$$

这样 $x^l + y^l + z^l \equiv 0 \mod p$，故 x, y, z 必有一个 $\equiv 0 \mod p$.

不妨假设 $x \equiv 0 \mod p$. 则 $2x = b^l + c^l + (-a)^l = 0 \mod p$, 因此 a, b, c 必有一个 $\equiv 0 \mod p$.

若 b 或者 $c \equiv 0 \mod p$, 则 $y \equiv 0 \mod p$, 故 $z \equiv 0 \mod p$, 这不可能. 因此 $a \equiv 0 \mod p$ 而 $y \equiv -z \mod p$. 因此

$$\left.\begin{aligned}\alpha^l &\equiv ly^{l-1} \mod p \\ \gamma^l &\equiv y^{l-1} \mod p\end{aligned}\right\} \Rightarrow \alpha^l \equiv l\gamma^l \mod p.$$

又由于

$$\left.\begin{aligned}y &\neq 0 \mod p \\ \alpha, \gamma &\neq 0 \mod p\end{aligned}\right\} \Rightarrow \frac{\alpha^l}{\gamma^l} \equiv l \mod p.$$

这与 (2): $x^l \equiv l \mod p$ 无解矛盾. □

例 15. 设 l 和 $2l+1$ 都是奇素数. 则 $l=\frac{p-1}{2}$ 且

$$x^{\frac{l-1}{2}} \equiv \begin{cases} \pm 1 & \mod p, \text{ 若 } p \nmid x; \\ 0 & \mod p, \text{ 若 } p \mid x. \end{cases}$$

这说明

(1) 若 $x^l+y^l+z^l=0 \mod p$, 则 x,y,z 中必有一个被 p 整除;
(2) $x^l \neq l \mod p$.
因此由热尔曼的定理有:

推论 1. *若 l 和 $2l+1$ 都是素数, 则 $x^l+y^l=z^l$ 说明 x,y,z 中必有一个被 l 整除.*

3. 库默尔小传

恩斯特 • 爱德华 • 库默尔 (Ernst Edward Kummer) 于 1810 年 1 月 29 日生于普鲁士的勃兰登堡 (今德国), 1893 年 5 月 14 日逝世于柏林. 他的父亲在他三岁的时候去世, 他和哥哥由母亲抚养成人. 1828 年库默尔入哈雷大学学习, 本来想学习新教神学, 但被他的老师 H. F. Scherk 的影响而吸引来学习数学. 1831 年库默尔毕业并获得博士学位.

从 1832 年到 1842 年, 他是利格尼茨 (今波兰莱格尼察) 中学的中学老师. 他是一位出色的老师, 他最好的学生是利奥波德 • 克罗内克 (Leopold Kronecker, 1823-1891). 1836 年他在 Crelle 杂志上发表了一篇关于超几何级数的文章, 他送了一份复印件给雅可比. 这促成了雅可比, 然后是狄利克雷和库默尔之间的数学通信, 他们很快就意识到库默尔拥有在数学最高水平研究的巨大潜力. 1839 年, 尽管他还是高中老师, 库默尔就在狄利克雷的推荐下入选柏林科学院.

1840 年库默尔与狄利克雷妻子的堂妹结婚, 她们俩都来自著名的门德尔松家族. 1842 年在雅可比和狄利克雷的强烈支持下, 库默尔成为布雷斯劳大学 (现波兰弗罗茨瓦夫) 正式教授. 1855 年狄利克雷离开柏林去哥廷根继承高斯的位置, 库默尔成为他在柏林的继任者. 一年以后, 魏尔斯特拉斯 (Weierstrass, 1815-1897) 加入柏林大学. 库默尔从前的学生克罗内克也在 1855 年来到柏林. 从 1855 年起柏林成为世界数学的中心, 领导者是两位高中数学老师库默尔和魏尔斯特拉斯, 以及克罗内克, 他家财万贯只是因为兴趣而来研究数学.

库默尔在柏林成为一位特别受欢迎的老师, 因他授课思路清晰和活泼生动而著名. 库默尔在那里指导了一大批博士生, 包括康托, Gordan (艾米 • 诺

特的导师) 和施瓦兹 (也是库默尔的女婿, 因柯西-施瓦兹不等式闻名). 他还在柏林大学担任了很高的行政职位, 1857-1858 年和 1865-1866 年是学院的院长, 1868-69 年成为大学校长.

4. 库默尔在费马大定理上的工作

4.1. 分圆整数的设置. 设 $l>3$ 是奇素数, $\alpha=\zeta_l$ 是 l-次本原单位根. 设 $x,y.z\in\mathbb{Z}-\{0\}\}$, $\gcd(x,y)=1$, 且

$$x^l+y^l=z^l.$$

则

$$(x+y)(x+\alpha y)\cdots(x+\alpha^{l-1}y)=z^l. \tag{7}$$

库默尔的想法是分解 $x+\alpha^j y$, 就如欧拉证明 $l=3$ 情形时采用的方法一样. 这样就促使他去研究所有分圆整数 $f(\alpha)$ ($f(x)\in\mathbb{Z}[x]$) 的性质. 记

$$\mathbb{Z}[\alpha]=\{f(\alpha)\mid f(X)\in\mathbb{Z}[X]\}.$$

我们知道 α 的最小多项式是 $\Phi_l(X)=X^{l-1}+\cdots+X+1$. 故 $1+\alpha+\cdots+\alpha^{l-1}=0$ 且 $\mathbb{Z}[\alpha]$ 上的任意元素可以唯一写为

$$f(\alpha)=a_0+a_1\alpha+\cdots+a_{l-2}\alpha^{l-2}\text{ 其中 }a_i\in\mathbb{Z}.$$

实际上库默尔将这个数写为

$$f(\alpha)=a_0+a_1\alpha+\cdots+a_{l-1}\alpha^{l-1},$$

它与 $(a_0+c)+(a_1+c)\alpha+\cdots+(a_{l-1}+c)\alpha^{l-1}$ 对任意 $c\in\mathbb{Z}$ 均相等.

正如整数环 $\mathbb{Z}$ 的情形一样,

$$f(\alpha)\mid g(\alpha)\text{ 若 }g(\alpha)=f(\alpha)h(\alpha)\text{ 对某个 }h(\alpha)\in\mathbb{Z}[\alpha]\text{ 成立},$$

$$f(\alpha)\equiv g(\alpha)\mod h(\alpha)\text{ 若 }h(\alpha)\mid(f(\alpha)-g(\alpha)).$$

要研究分圆整数的分解, 库默尔引入了

定义 7. (1) 分圆整数 $f(\alpha)$ 称为单位是指存在另外一个 (唯一的) 分圆整数 $g(\alpha)$ 使得 $f(\alpha)g(\alpha)=1$, 此时 $g(\alpha)$ 称为 $f(\alpha)$ 的逆.

(2) 分圆整数 $h(\alpha)$ 称为素元是指 $h(\alpha)$ 不是单位且如下条件成立: 若 $h(\alpha)\mid f(\alpha)g(\alpha)$, 则或者 $h(\alpha)\mid f(\alpha)$ 或者 $h(\alpha)\mid g(\alpha)$.

(3) $h(\alpha)$ 称为不可约元是指 $h(\alpha)$ 不是单位且如下条件成立: 若 $h(\alpha)=f(\alpha)g(\alpha)$, 则 $f(\alpha)$ 和 $g(\alpha)$ 中必有一个是单位.

定义 8. 两个分圆整数 $f(\alpha)$ 和 $g(\alpha)$ 称为等价是指 $f(\alpha)=g(\alpha)u$, 其中 u 是单位.

引理 1. *若 $f(\alpha)$ 与 $g(\alpha)$ 是两个素元且 $f(\alpha)\mid g(\alpha)$, 则 $f(\alpha)$ 与 $g(\alpha)$ 等价.*

证明. 记 $g(\alpha)=f(\alpha)h(\alpha)$. 则由 $g(\alpha)$ 的素性, $g(\alpha)\mid f(\alpha)$ 或者 $g(\alpha)\mid h(\alpha)$ 成立. 在第一种情形, 记 $f(\alpha)=g(\alpha)h'(\alpha)$, 则

$$g(\alpha)=g(\alpha)h(\alpha)h'(\alpha),$$

因此 $h'(\alpha)h(\alpha)=1$ 故 $h'(\alpha)$ 是单位. 在第二种情形记 $h(\alpha)=g(\alpha)f'(\alpha)$, 同样推理说明 $f(\alpha)f'(\alpha)=1$ 故 $f(\alpha)$ 是单位, 这是不可能的. □

根据伽罗瓦的语言我们知道

$$\mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q})=\{\sigma_a:\alpha\mapsto\alpha^a,\,1\le a\le l-1\}\cong(\mathbb{Z}/l\mathbb{Z})^\times. \tag{8}$$

库默尔将经常使用替换 $\sigma_a:\alpha\mapsto\alpha^a$. α 的共轭元是 α^i $(1\le i\le l-1)$, 因此 $f(\alpha)$ 的共轭元是 $f(\alpha^i)$ $(1\le i\le l-1)$. 库默尔定义

定义 9. 分圆整数 $f(\alpha)$ 的范指

$$Nf(\alpha)=f(\alpha)f(\alpha^2)\cdots f(\alpha^{l-1})\in\mathbb{Z}.$$

命题 4. *下列事实成立:*

(1) $f(\alpha)=0$ *当且仅当* $Nf(\alpha)=0$.

(2) *若* $f(\alpha)\neq 0$, *则*

$$Nf(\alpha)=\prod_{i=1}^{\frac{l-1}{2}}f(\alpha^i)f(\alpha^{l-1-i})=\prod_{i=1}^{\frac{l-1}{2}}|f(\alpha^i)|^2\in\mathbb{Z}_+.$$

(3) *范映射是积性的:* $N(f(\alpha)g(\alpha))=Nf(\alpha)Ng(\alpha)$.

(4) $f(\alpha)$ *是单位当且仅当* $Nf(\alpha)=1$.

4.2. 素元的研究. 库默尔的目的是决定 $x+\alpha^j y$ $(0\le j\le l-1,\,x,y\in\mathbb{Z}$ 且 $\gcd(x,y)=1)$ 的素因子. 设 $h(\alpha)\mid(x+\alpha^j)y$ 是这样一个素元. 则

$$h(\alpha)\mid(x+\alpha^j)y\mid N(x+\alpha^j)=p_1p_2\cdots p_n,$$

那么 $h(\alpha)\mid p$, 其中 $p=p_1,\cdots,p_n$ 是 $N(x+\alpha^j)$ 某个素因子. 若 $h(\alpha)\mid q$ 对另外一个素数 $q\neq p$ 也成立, 则 $h(\alpha)\mid ap+bq$ 对所有 $a,b\in\mathbb{Z}$ 成立, 特别地 $h(\alpha)\mid 1$ 是一个单位, 这不可能. 因此 p 是唯一的素数使得 $h(\alpha)\mid p$. 这表明

$$h(\alpha)\mid n\Leftrightarrow p\mid n\quad(n\in\mathbb{Z}),$$

等价地说,

$$m \equiv n \mod h(\alpha) \Leftrightarrow m \equiv n \mod p \quad (m, n \in \mathbb{Z}).$$

现在由 $x + \alpha^j y \equiv 0 \mod h(\alpha)$, 自然有 $p \nmid y$, 否则 $p \mid y$ 且 $h(\alpha) \mid y$, 因而 $h(\alpha) \mid x$ 且 $p \mid x$, 与 $\gcd(x, y) = 1$ 矛盾. 设 $a \in \mathbb{Z}$ 使得 $ay \equiv 1 \mod p$, 则 $ay \equiv 1 \mod h(\alpha)$, 因此

$$\alpha^j \equiv -ax \mod h(\alpha).$$

设 $i \in \mathbb{Z}$ 且 $ij \equiv 1 \mod l$, 则

$$\alpha = \alpha^{ij} \equiv (-ax)^i \mod h(\alpha).$$

令 $k = (-ax)^i \mod p$, 则我们可以假设存在 $0 < k < p$, 仅仅依赖于 x, y, j, 使得

$$\alpha \equiv k \mod h(\alpha).$$

因此

$$g(\alpha) \equiv g(k) \mod h(\alpha) \text{ 对任意 } g(\alpha) \in \mathbb{Z}[\alpha] \text{ 成立.}$$

这说明

命题 5. *若 $h(\alpha)$ 是整除 $x + \alpha^j y$ 的素元, 其中 $0 \le j \le l - 1$, $x, y \in \mathbb{Z}$ 且 $\gcd(x, y) = 1$, 则存在 $N(x + \alpha^j y)$ 唯一的一个素数因子 p, 和唯一的仅依赖于 x, y, j 的整数 $0 < k < p$ 使得*

$$g(\alpha) \equiv f(\alpha) \mod h(\alpha) \Leftrightarrow g(k) \equiv f(k) \mod p. \tag{9}$$

接下来, 库默尔给出 k 和素元的更多信息.

由于 $\alpha^{l-1} + \cdots + \alpha + 1 = 0$ 以及公式 (9), 则 $k^{l-1} + \cdots + k + 1 \equiv 0 \mod p$. 故 $k^l \equiv 1 \mod p$. 又由于费马小定理, 我们有 $k^{p-1} \equiv 1 \mod p$. 现在要考虑两种情况:

情形 1: $k \equiv 1 \mod p$. 此时 $l \equiv k^{l-1} + \cdots + k + 1 \equiv 0 \mod p$, 因此 $l = p$. 对于 $1 \le i \le l - 1$, $N(\alpha - 1) = l = N(\alpha^i - 1) = l$. 故 $\frac{\alpha^i - 1}{\alpha - 1} = 1 + \cdots + \alpha^{i-1}$ 的范是 1, 因此 $\frac{\alpha^i - 1}{\alpha - 1}$ 是单位且

$$l = (\alpha - 1)^{l-1} u, \text{ 其中 } u \text{ 是单位.}$$

因为 $(\alpha - 1) \mid f(\alpha) - f(1)$, 所以 $(\alpha - 1) \mid f(\alpha)$ 当且仅当 $(\alpha - 1) \mid f(1)$. 此时, $l = N(\alpha - 1) \mid N(f(1)) = f(1)^{l-1}$ 故 $l \mid f(1)$. 因此 $(\alpha - 1) \mid f(\alpha)$ 当且仅当 $l \mid f(1)$. 若 $(\alpha - 1) \mid f(\alpha)g(\alpha)$, 则 $l \mid f(1)g(1)$, 即 $l \mid f(1)$ 或者 $g(1)$, 所以 $(\alpha - 1) \mid f(\alpha)$ 或者 $(\alpha - 1) \mid g(\alpha)$. 这说明 $\alpha - 1$ 是 $\mathbb{Z}[\alpha]$ 的一个素元.

反过来, 由公式 (9), 若 $h(\alpha)$ 是整除 l 的素元, 则 $\alpha \equiv 1 \mod h(\alpha)$ 即 $h(\alpha) \mid (\alpha - 1)$. 由引理 1知它们必须等价. 因此等价意义上说, $\alpha - 1$ 是 $\mathbb{Z}[\alpha]$ 中整除 l 的唯一素元.

情形 2: $k \mod p$ 的阶是 l. 这说明 $l \mid p-1$ 因此 $p \equiv 1 \mod l$.

考虑伽罗瓦作用, 我们有

$$\alpha \equiv k \mod h(\alpha) \iff \alpha^j \equiv k \mod h(\alpha^j) \text{ 对任意 } 1 \le j \le l-1 \text{ 成立,}$$

且

分圆整数 $f(\alpha)$ 是素元当且仅当 $f(\alpha^j)$ 对某个 $1 \le j \le l-1$ 是素元.

若 $h(\alpha^i) \mid h(\alpha^j)$, 则由引理 1, $h(\alpha^j) = h(\alpha^i)u$, 且

$$\alpha^j \equiv k \mod h(\alpha^j), \quad \alpha^i \equiv k \mod h(\alpha^i)$$

这说明 $\alpha^i \equiv \alpha^j \mod h(\alpha^i)$, 即 $(\alpha - 1) \mid h(\alpha^j)$, 这不可能. 因此 $h(\alpha)$, $\cdots$, $h(\alpha^{l-1})$ 是互相不等价的素元, 且 $h(\alpha^j) \mid p$ 对所有 j 成立. 这说明 $N(h(\alpha))) = h(\alpha) \cdots h(\alpha^{l-1}) \mid p$ 进而 $Nh(\alpha) = p$.

定理 26. *下面陈述成立:*

(1) *设 $h(\alpha)$ 是素元且 $h(\alpha) \mid x + \alpha^j y$ 对某互素的 $x, y \in \mathbb{Z}$ 和 $1 \le j \le l-1$ 成立. 那么 $Nh(\alpha) = p$ 是素数, 且或者 $p = l$ 或者 $p \equiv 1 \mod l$.*

(2) *若 $p = l$ 或 $p \equiv 1 \mod l$ 且 $h(\alpha)$ 是分圆整数满足 $Nh(\alpha) = p$, 则 $h(\alpha)$ 是素元且 $h(\alpha) \mid x + \alpha^j y$ 对某互素的 $x, y \in \mathbb{Z}$ 和 $1 \le j \le l-1$ 成立.*

(3) *若 $p = l$, 则等价意义下唯一的素元是 $\alpha - 1$.*

证明. 只需对于 $p \equiv 1 \mod l$ 情形证明 (2).

由于 $\mathbb{F}_p^\times$ 是 $p-1$ 阶循环群而 $l \mid p-1$, 故 $\mathbb{F}_p^\times$ 有唯一的阶为 l 的子群, 令其为 $\{m, \cdots, m^l = 1\}$. 对于 $Nh(\alpha) = p$, 我们有

$$h(X)h(X^2)\cdots h(X^{l-1}) = p + (1 + X + \cdots + X^{l-2})g(X) \text{ for some } g(X) \in \mathbb{Z}[X].$$

因为 $1 + m + \cdots + m^{l-2} = 0 \in \mathbb{F}_p$, 所以 $h(m)h(m^2)\cdots h(m^{l-1}) = 0 \in \mathbb{F}_p$. 在整数上则有

$$h(m)h(m^2)\cdots h(m^{l-1}) \equiv 0 \bmod p.$$

不妨设 $h(m^j) \equiv 0 \bmod p$. 由带余除法知 $h(X) = q(X)(X - m^j) + h(m^j) \in \mathbb{Z}[X]$, 故 $h(\alpha) \equiv q(\alpha)(\alpha - m^j) \bmod p$, 且

$$h(\alpha^\nu) \equiv q(\alpha^\nu)(\alpha^\nu - m^j) \bmod p \text{ 对所有 } 1 \le \nu \le l-1 \text{ 成立.}$$

因此

$$(\alpha - m^j)h(\alpha^2)\cdots h(\alpha^{l-1}) \equiv N(\alpha - m^j)q(\alpha^2)\cdots q(\alpha^{l-1}) \bmod p.$$

然而 $N(\alpha - m^j) = \frac{m^{jl}-1}{m^j-1} \equiv 0 \bmod p$, 所以 $(\alpha - m^j)h(\alpha^2)\cdots h(\alpha^{l-1}) \equiv 0 \bmod p$. 换言之, $p = h(\alpha)h(\alpha^2)\cdots h(\alpha^{l-1}) \mid (\alpha - m^j)h(\alpha^2)\cdots h(\alpha^{l-1})$ 故有 $h(\alpha) \mid \alpha - m^j$. 这说明 $\alpha \equiv m^j \bmod h(\alpha)$.

下要证明 $h(\alpha)$ 是素元. 设 $h(\alpha) \mid f(\alpha)g(\alpha)$ 且 $\alpha \equiv k \bmod h(\alpha)$. 则 $f(k)g(k) \equiv 0 \bmod h(\alpha)$. 这说明在 $\mathbb{Z}$ 上有 $f(k)g(k) \equiv 0 \bmod p$, 故 $f(k)$ 或者 $g(k) \equiv 0 \bmod p$. 所以 $f(k)$ 或者 $g(k) \equiv 0 \bmod h(\alpha)$, 故 $f(\alpha)$ 或者 $g(\alpha) \equiv 0 \bmod h(\alpha)$, 即 $h(\alpha)$ 是素元. □

对于素数 $p \equiv 1 \bmod l$, 库默尔尝试去寻找范为 p 的分圆整数 $h(\alpha)$ (因此 $h(\alpha)$ 是素元). 然而, 他发现对于 $l = 23$ 和 $p = 47$ 的情形,

(1) 不存在分圆整数 $h(\alpha)$, 使得 $Nh(\alpha) = 47$;

(2) $N(-\alpha + \alpha^{21}) = 47 \times 139$.

这说明环 $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta_{23}]$ 中不存在唯一因子分解性质.

4.3. 一般情形 ($p \neq l$).

4.3.1. *素除子*. 对于素数 $p \neq l$, p 的指数指它在 $\mathbb{Z}/l\mathbb{Z} = \mathbb{F}_l$ 中的阶, 即最小的正整数 f 使得 $p^f \equiv 1 \bmod l$. 设 $g = \frac{l-1}{f}$. 令循环群 $(\mathbb{Z}/l\mathbb{Z})^\times = \langle\gamma\rangle \cong \mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q})$, $\gamma\alpha = \alpha_\gamma$.

定义 10. 对于 $i = 1, \cdots, g$, p 的高斯周期即

$$\eta_i := \gamma^i(1 + \gamma^g + \cdots + \gamma^{(f-1)g})\alpha = \alpha^{\gamma^i} + \alpha^{\gamma^{i+g}} + \cdots + \alpha^{\gamma^{i+g(f-1)}}.$$

注记 4. 高斯周期至今还在广泛使用, 比如在编码理论中.

由计算, 库默尔得到下述结果:

命题 6. *对于 $i = 1, \cdots, g$, 存在整数 u_i, $0 \leq u_i < p$, 使得对任意多项式 $F(X_1, \cdots, X_g) \in \mathbb{Z}[X_1, \cdots, X_g]$,*

$$F(\eta_1, \cdots, \eta_g) = 0 \Longleftrightarrow F(u_1, \cdots, u_g) \equiv 0 \bmod p.$$

更进一步地, 若 $(u_1, \cdots, u_g)$ 满足上述性质, 则 $(u_1, \cdots, u_g)$, $(u_2, \cdots, u_g, u_1)$, $\cdots$, $(u_g, u_1, \cdots, u_{g-1})$ 是所有满足这个性质的整数组且它们两两不同.

定理 27. *如上命题给定 $(u_1, \cdots, u_g)$, 可以在分圆整数中定义一个且只有一个等价关系, 满足条件*

(1) $\eta_i \sim u_i$, $p \sim 0$, $1 \not\sim 0$;
(2) 若 $f(\alpha) \sim g(\alpha)$, *则* $h(\alpha)f(\alpha) \sim h(\alpha)g(\alpha)$ *对所有* $h(\alpha) \in \mathbb{Z}[\alpha]$ *成立;*
(3) 若 $f(\alpha) \sim g(\alpha)$ *且* $f'(\alpha) \sim g'(\alpha)$, *则* $f(\alpha) \pm f'(\alpha) \sim g(\alpha) \pm g'(\alpha)$ *且* $f(\alpha)f'(\alpha) \sim g(\alpha)g'(\alpha)$;
(4) 若 $f(\alpha)g(\alpha) \sim 0$ *则或者* $f(\alpha) \sim 0$ *或者* $g(\alpha) \sim 0$.
更一步地, 等价类个数为 p^f.

定义 11. 上述定理得到的等价关系称为 p 上对应于 $(u_1, \cdots, u_g)$ 的素除子. 记 $f \sim g$ 为 $f \equiv g \mod \mathfrak{P}$, 称 $\mathfrak{P}$ 是 p 上对应于 $(u_1, \cdots, u_g)$ 的素除子.

因此共有 $g = \frac{l-1}{f}$ 个素除子位于 p 的上面, 分别对应于 $(u_1, \cdots, u_g)$, $\cdots$, $(u_g, u_1, \cdots, u_{g-1})$.

定义 12. 令 $\mathfrak{P}$ 是 p 上对应于 $(u_1, \cdots, u_g)$ 的素除子.
(1) 我们称 $\mathfrak{P}^\mu \mid g(\alpha)$ 是指 $p^\mu \mid g(\alpha)\psi(\eta)^\mu$, 此处

$$\psi(\eta) = \prod_{i=1}^{g} \prod_{\substack{j=0 \\ j \neq \mu_i}}^{p-1} (j - \eta_i)$$

(2) 我们称 $\mathfrak{P}^\mu \mid\mid g(\alpha)$ 是指 $\mathfrak{P}^\mu \mid g(\alpha)$ 但 $\mathfrak{P}^{\mu+1} \nmid g(\alpha)$. 此时, 定义 $\mathrm{ord}_{\mathfrak{P}}(g(\alpha)) := \mu$.

库默尔证明了若 $g(\alpha) \neq 0$, 则 $\mathrm{ord}_{\mathfrak{P}}(g(\alpha))$ 是唯一决定的. 如果令 $\mathrm{ord}(0) = +\infty$, 我们就得到通常的加性赋值映射:

$$\mathrm{ord}_{\mathfrak{P}} : \mathbb{Z}[\alpha] \to \mathbb{Z}_{\geq 0} \cup \{\pm\infty\}.$$

注意这个事实:

$\mathrm{ord}_{\mathfrak{P}}(g(\alpha)) \neq 0$ 当且仅当 $p \not\sim Ng(\alpha)$.

例 16. 对于 $p = l$, $\mathfrak{P} = (\alpha - 1)$, 且如果 $(\alpha - 1)^\mu \mid g(\alpha)$ 但 $(\alpha - 1)^{\mu+1} \nmid g(\alpha)$, 那么 $\mathrm{ord}_{\mathfrak{P}}(g(\alpha)) = \mu$.

库默尔证明了定理:

定理 28. *若* $g(\alpha), h(\alpha) \neq 0$, *则* $g(\alpha) \mid h(\alpha)$ *当且仅当对所有的素数* p *和* p *上所有的素除子* $\mathfrak{P}$, *均有* $\mathrm{ord}_{\mathfrak{P}}(g(\alpha)) \leq \mathrm{ord}_{\mathfrak{P}}(h(\alpha))$.

作为一个推论, $g(\alpha) = uh(\alpha)$ *其中* u *为单位当且仅当对所有的素数* p *和* p *上所有的素除子* $\mathfrak{P}$, *均有* $\mathrm{ord}_{\mathfrak{P}}(g(\alpha)) = \mathrm{ord}_{\mathfrak{P}}(h(\alpha))$.

4.3.2. 除子.

定义 13. 分圆整数 $g(\alpha)\neq 0$ 对应的主除子是形式积 $\prod_{\mathfrak{P}}\mathfrak{P}^{\mathrm{ord}_{\mathfrak{P}}(g(\alpha))}$.
除子 (或用现代语言而言有效除子) 是形式积

$$A=\prod_{\mathfrak{P}}\mathfrak{P}^{n_{\mathfrak{P}}(A)},\ n_{\mathfrak{P}}(A)\geq 0,\ \text{且 } n_{\mathfrak{P}}(A)=0,\text{对几乎所有的 } \mathfrak{P} \text{ 成立.}$$

最初的时候库默尔称除子为理想复数 (ideal complex number).

定义 14. 设 A 是除子. 称 $f(\alpha)=g(\alpha) \mod A$ 若 $\mathrm{ord}_{\mathfrak{P}}(f(\alpha)-g(\alpha))\geq n_{\mathfrak{P}}(A)$ 对所有素除子 $\mathfrak{P}$ 成立.

库默尔证明了更多结果:

定理 29. 设 $\{\mathfrak{P}_1,\cdots,\mathfrak{P}_g\}$ 是素数 p 上的素除子. 若 $Ng(\alpha)=p^f$, 则 $g(\alpha)$ 是素元且存在 $1\leq i\leq g$ 使得

$$\mathrm{ord}_{\mathfrak{P}_i}(g(\alpha))=1 \ \text{ 且 } \ \mathrm{ord}_{\mathfrak{P}_j}(g(\alpha))=0 \text{ 若 } j\neq i.$$

定理 30. 对于每个 i, 存在 $\psi_i(\eta)=a_1\eta_1+\cdots+a_g\eta_g$ $(a_i\in\mathbb{Z})$, 使得

$$\mathrm{ord}_{\mathfrak{P}_i}(\psi_i(\eta))=1 \ \text{ 且 } \ \mathrm{ord}_{\mathfrak{P}_j}(\psi_i(\eta))=0 \text{ 若 } j\neq i.$$

注记 5. 此后我们记素除子 $\mathfrak{P}=(p,\psi_{\mathfrak{P}}(\eta))$. 则
(1) 除子 $A=(p_1,\psi_1(\eta))^{\mu_1}\cdots(p_m,\psi_m(\eta))^{\mu_m}$.
(2) p 对应的主除子即

$$\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_g=(p_1,\psi_1(\eta))\cdots(p_g,\psi_g(\eta)).$$

4.3.3. 除子的范. 伽罗瓦群通过

$$\sigma(p,\psi(\eta)):=(p,\sigma\psi(\eta))$$

作用于素除子上, 并通过乘积延申作用在除子上.

定义 15. 对于除子 A, 令 $N(A)=A\sigma(A)\cdots\sigma^{l-2}(A)$, 此处 σ 是伽罗瓦群的一个生成元.

定理 31. $N(A)$ 作为除子由一个正整数生成, 我们混淆记号称此正整数为 A 的范, 它由如下两个条件决定:
(1) $N(AB)=N(A)N(B)$,
(2) $N(p,\psi(\eta))=p^f=(p,\psi(\eta))$ 中等价类的个数.

定理 32 (中国剩余定理). 设 A 和 B 是互素的除子. 则对于任意分圆整数 a 和 b, 存在 $x \in \mathbb{Z}[\alpha]$ 满足

$$\begin{cases} x \equiv a \mod A, \\ x \equiv b \mod B. \end{cases} \tag{10}$$

更进一步地, 所有满足方程 (10)的分圆整数组成模 AB 的一个等价类.

4.3.4. 类数.

定义 16. 设 A 与 A' 是两个除子. 若对所有除子 B', AB 是主除子当且仅当 $A'B$ 是主除子, 则称 $A \sim A'$.

引理 2. 上述关系是等价关系, 即它满足自反性, 对称性和传递性.

记 $[A]$ 是 A 所在的等价类.

定理 33. 除子的等价类个数有限, 即存在除子 $A_1, \cdots, A_k$ 使得任何除子都等价于某个 A_i. 更进一步地, 定义乘法 $[A][B] = [AB]$, 则 $\mathbb{Z}[\alpha]$ 的除子等价类构成一个有限阿贝尔群, 其单位元是主除子所在的类.

定义 17. $\mathbb{Z}[\alpha]$ 的除子类构成的有限群称为 $\mathbb{Z}[\alpha]$ 或者 $\mathbb{Q}[\alpha]$ 的类群, 它的阶称为类数.

推论 2. 设 h 是 $\mathbb{Z}[\alpha]$ 的类数. 则对于任意除子 C, C^h 是主除子.

4.4. 库默尔关于费马大定理的工作.

定义 18. 素数 l 若不整除 $\mathbb{Z}[\alpha]$ 的类数 h, 则称它为正则素数.

引理 3. 若 ε 是单位, 则 $\varepsilon/\bar{\varepsilon} = \alpha^r$ 对某个 r 成立.

证明. 设 $E(X) = a_0 + a_1 X + \cdots + a_{l-1}X^{l-1}$ 使得 $E(\alpha) = \varepsilon/\bar{\varepsilon}$. 设 $E(X^{l-1})E(X) = Q(X)(X^l - 1) + R(X)$ 其中 $R(X) = A_0 + \cdots + A_{l-1}X^{l-1}$. 取 $X = \alpha$, 则 $R(\alpha) = 1$ 且 $A_0 - 1 = A_1 = \cdots = A_{l-1}$. 假设这个数是 k. 取 $X = 1$, 则

$$(a_0 + a_1 + \cdots + a_{l-1})^2 = A_0 + \cdots + A_{l-1} = 1 + kl.$$

所以 $a_0 + a_1 + \cdots + a_{l-1} \equiv \pm 1 \bmod l$. 将 a_i 用 $a_i + c$ 代替, 我们不妨假设 $a_0 + a_1 + \cdots + a_{l-1} = \pm 1$, 故对于这个新的 $E(X)$, $A_0 = 1$ 且 $A_i = 0$ 对所有 $0 < i < l - 1$ 成立. 注意到

$$a_i X^{(l-1)i} a_j X_j \equiv a_i a_j X^r \mod X^l - 1$$

此处 $0 \le r < l$ 而 $j - i \equiv r \mod l$, 故

$$A_r = \sum_{j-i\equiv r} a_i a_j.$$

特别地 $A_0 = a_0^2 + \cdots + a_{l-1}^2$. 对于 $A_0 = 1$, 只有一个 $a_r = \pm 1$ 而所有其他的均为 0, 所以 $E(\alpha) = \pm\alpha^r$.

若 $\varepsilon/\bar{\varepsilon} = -\alpha^r$, 由于 r 或者 $r + l$ 是偶数, 可以假设 $\varepsilon/\bar{\varepsilon} = -\alpha^{2s}$, 故 $\varepsilon\alpha^{-s} = -\bar{\varepsilon}\alpha^s$. 设 $F(\alpha) = \varepsilon\alpha^{-s}$ 其中 $F(0) = 0$, 那么 $F(\alpha) = -F(\alpha^{-1})$. 这样就得到一个非单位 $(\alpha - \alpha^{-1})$ 整除单位 $F(\alpha)$, 自然这是不可能的. □

我们还需要下面的引理 (称为库默尔引理):

引理 4. *若 l 正则, 则对于单位 $\epsilon \in \mathbb{Z}[\alpha]$, 若 $\epsilon \equiv$ 某整数 $\mod l$, 则 $\epsilon = (\epsilon')^l$ 对于某单位 ϵ' 成立.*

注记 6. 这个引理被库默尔称为条件 (B), 正则性条件即条件 (A). 库默尔最终证明 (A) 推出 (B). 他的证明过程简述如下. 通过狄利克雷引入的解析方法, 库默尔证明 $\mathbb{Q}(\alpha)$ 的类数公式, 并且证明正则性条件等价于 l 不整除伯努利数 $B_2, B_4, \cdots, B_{l-3}$ 的分子, 这里伯努利数如下定义

$$\frac{x}{e^x - 1} = \sum_n B_n \frac{x^n}{n!}.$$

然后他需要分析 $\mathbb{Q}(\alpha)$ 的单位的结构, 这又是狄利克雷的思想 (狄利克雷单位定理).

定理 34. *若 l 是正则素数, 则 $x^l + y^l = z^l$ 没有非平凡的整数解.*

证明. 不妨假设 x, y, z 两两互素, 且下面两个条件中一个条件成立:

I : x, y, z 均与 l 互素;
II : $l \nmid xy$ 但 $l \mid z$.

记

$$x^l + y^l = (x + y)(x + \alpha y)\cdots(x + \alpha^{l-1}y) = z^l.$$

若 $x + \alpha^j y$ 与 $x + \alpha^{j+k} y$ 有公因子, 这个因子一定是下面分圆整数的公因子:

(1) $(x + \alpha^{j+k}y) - (x + \alpha^j y) = \alpha^j(\alpha^k - 1)y = unit \cdot (\alpha - 1)y$;
(2) $(x + \alpha^{j+k}y) - \alpha^k(x + \alpha^j y) = unit \cdot (\alpha - 1)x$.

由于 $\gcd(x, y) = 1$, 故这个公因子一定是 $\alpha - 1$ 的因子. 于是,

- 或者 $(x + \alpha^{j+k}y)$ 互素且 $(\alpha - 1) \nmid z^l$; (情形 I)

- 或者所有的 $(x+\alpha^{j+k}y)$ 均有因子 $\alpha-1$ 而它们的商两两互素, 且 $l \mid z$. (情形 II)

情形 I. 此时 $x+y, x+\alpha y, \cdots x+\alpha^{l-1}y$ 两两互素而它们的乘积是 l-次幂, 因此每一个 $x+\alpha^j y$ 的主除子是某个除子 C_j 的 l 次幂. 然而由于 $[C_j]^h = 1 = [C_j]^l$ 而 $l \nmid h$, 故 C_j 是主除子. 因此 $x+\alpha^j y = \epsilon_j t_j^l$, 此处 ϵ_j 是单位而 t_j 是分圆整数.

取 $j=1$. 令 $^-$ 是复共轭. 则

$$x+\alpha y = \epsilon t^l, \quad x+\alpha^{-1}y = \overline{x+\alpha y} = \bar{\epsilon}\bar{t}^l.$$

由引理 3, $\frac{\epsilon}{\bar{\epsilon}} = \alpha^r$ 对某个 $0 \le r \le l$ 成立. 我们还有 $t^l \equiv \bar{t}^l \mod l$. 因此

$$x+\alpha^{-1}y = \alpha^{-r}\epsilon\bar{t}^l \equiv \alpha^{-r}\epsilon t^l \equiv \alpha^{-r}(x+\alpha y) \mod l.$$

若 $r=0$, 则 $(\alpha-\alpha^{-1})y \equiv 0 \mod l$, 所以 $\alpha-1 \mid y$ 故 $l \mid y$, 这不可能. 故 $0<r<l$. 我们有

$$\alpha^{r-1}(\alpha x+y) \equiv x+\alpha y \mod l,$$

$$[(\alpha-1)+1]^{r-1}[(\alpha-1)x+x+y] \equiv (x+y)+(\alpha-1)y \mod (\alpha-1)^{l-1}$$

比较两端的 $(\alpha-1)^2$-项, 即得 $x \equiv y \mod l$. 同理 $x \equiv -z \mod l$. 由于 $x^l+y^l \equiv x+y \equiv z^l \equiv z \mod l$, 故 $3x \equiv 0 \mod l$, 所以 $l=3$. 这个情形已经由欧拉证明了.

情形 II. 此时对所有 j 均有 $(\alpha-1) \mid x+\alpha^j y$,

$$\prod_{i=0}^{l-1}\left(\frac{x+\alpha^j y}{\alpha-1}\right) = z^l(\alpha-1)^{-l}$$

是 l-次而且 $\frac{x+\alpha^j y}{\alpha-1}$ 两两互素. 则

> 对所有的 j, $x+\alpha^j y = (\alpha-1)\epsilon_j t_j^l$, 其中 ϵ_j 是单位, t_j 两两互素.

因为 $l \mid z$, 故 $l \mid x+y$, 所以 $(\alpha-1) \mid t_0$, 且 $(\alpha-1) \nmid t_j$ 对所有 $j \neq 0$.

令 $t_0 = (\alpha-1)^k\omega$, $(\alpha-1) \nmid \omega$, 则 $k \ge 1$. 记

$$\begin{cases} x+\alpha^{-1}y = (\alpha-1)\epsilon_{-1}t_{-1}^l; \\ x+y = (\alpha-1)\epsilon_0(\alpha-1)^{kl}\omega^l; \\ x+\alpha y = (\alpha-1)\epsilon_1 t_1^l. \end{cases}$$

由于 $\alpha\times[(x+y)-(x+\alpha^{-1}y)]=(x+\alpha y)-(x+y)$, 我们得到

$$0=\epsilon_1 t_1^l+\alpha\epsilon_{-1}t_{-1}^l-(1+\alpha)\epsilon_0(\alpha-1)^{kl}\omega^l.$$

它有如下形式

$$E_0(\alpha-1)^{kl}\omega^l=t_1^l+E_{-1}t_{-1}^l,\ \text{其中 } E_1,\ E_{-1}\ \text{是单位.}$$

在两边同时模 l, 注意到 $t_1^l\equiv$ 某个整数 $\mod l$ 且 $t_{-1}^l\equiv$ 某个整数 $\mod l$, 并且它们俩均非零, 这是因为 $(\alpha-1)\nmid t_1$ 且 $(\alpha-1)\nmid t_{-1}$, 因此单位 $E_{-1}\equiv$ 整数 $\mod l$. 由库默尔引理 (引理 4), $E_{-1}=\epsilon^l$ 对于某单位 ϵ 成立. 我们得到

$$E_0(\alpha-1)^{kl}\omega^l=t_1^l+(\epsilon t_{-1})^l.$$

考虑如下形式的方程

$$x^l+y^l=\epsilon(\alpha-1)^{kl}\omega^l \tag{11}$$

其中 ϵ 是单位, $k>0$ 而 $x,y,\alpha-1,\omega$ 两两互素. 注意到至少一个 $x+\alpha^j y$ 被 $\alpha-1$ 整除, 故它们所有均被 $\alpha-1$ 整除且商两两互素. 记

$$x\equiv a_0+a_1(\alpha-1)\mod(\alpha-1)^2,\quad y\equiv b_0+b_1(\alpha-1)\mod(\alpha-1)^2,$$

其中 $a_0,a_1,b_0,b_1\in\mathbb{Z}$, 则

$$x+\alpha^j y\equiv(a_0+b_0)+[a_1+b_1+jb_0](\alpha-1)\mod(\alpha-1)^2.$$

由于 $\alpha-1\nmid y$, 故 $b_0\not\equiv 0 \mod l$. 因此存在恰好一个 j 使得 $l\mid a_1+b_1+jb_0$, 即存在恰好一个 j 使得 $(\alpha-1)^2\mid x+\alpha^j y$. 因此 $(\alpha-1)^{l+1}\mid\prod_{j=0}^{l-1}(x+\alpha_j y)$, 这说明 $k>1$. 换言之, 若 $k=1$, 则方程 (11) 无解.

记 $k=K+1$. 将 y 由 $\alpha_j y$ 替代, 此 j 满足条件 $(\alpha-1)^2\mid x+\alpha^j y$. 则

$$\begin{cases}x+\alpha^{-1}y=(\alpha-1)\epsilon_{-1}t_{-1}^l\\ x+y=(\alpha-1)\epsilon_0(\alpha-1)^{Kl}\omega^l\\ x+\alpha y=(\alpha-1)\epsilon_1 t_1^l\end{cases}$$

重复之前的论述则有

$$X^l+Y^l=E(\alpha-1)^{Kl}\omega^l$$

其中 $X,Y,\omega,\alpha-1$ 两两互素, E 是单位而 $K=k-1$. 这样由递降法将导致 $K=1$ 的情形的解, 这不可能. □

5. 库默尔在数论上的进一步工作

5.1. 库默尔扩张和库默尔配对. 设 $n>1$ 是整数. 设 F 是域, $\mathrm{char}\ F$ 或者是 0 或者与 n 互素, 并包含本原 n-次单位根 ζ_n, 则扩张 $E=F(\sqrt[n]{a})$ 称为库默尔扩张. 由于 E 是可分多项式 x^n-a 的分裂域, 故 E 是 F 上的伽罗瓦扩张. 更进一步地, $\sigma\in\mathrm{Gal}(E/F)$ 由 $\sqrt[n]{a}$ 的像 $\zeta_n^t\sqrt[n]{a}$ 完全决定. 因此

$$\mathrm{Gal}(E/F)\to\mathbb{Z}/n\mathbb{Z},\ \sigma\mapsto t \mod n$$

是单同态. 我们有

引理 5. *若 E/F 是库默尔扩张, 则 $\mathrm{Gal}(E/F)$ 是阶整除 n 的循环群.*

定义 19. 域扩张 L/K 称为阿贝尔扩张是指 L/K 是伽罗瓦扩张且 $\mathrm{Gal}(L/K)$ 是阿贝尔群. 如果更进一步地, $\mathrm{Gal}(L/K)$ 的元素的阶都整除 n, 那么称 L/K 是指数 n 的阿贝尔扩张.

库默尔有如下定理:

定理 35. *设 $\mu_n\subseteq F$, $\mathrm{char}\ F$ 等于 0 或者与 n 互素, 并包含本原 n-次单位根 ζ_n. 则 L/F 是指数 n 的阿贝尔扩张当且仅当 $L=F(\sqrt[n]{\Delta})$, 此处 Δ 是群 $F^\times/(F^\times)^n$ 的有限子群.*

5.2. 库默尔同余.

定理 36. *若 $p\nmid a$, 则*

$$n_1\equiv n_2 \mod p^{k-1}(p-1)\Longrightarrow(1-a^{1+n_1})\zeta(-n_1)\equiv(1-a^{1+n_2})\zeta(-n_2) \mod p^k.$$

库默尔同余是构造 p 进 L 函数的起点.

CHAPTER 4

数论上的进一步工作 (1950 年前)

1. 代数数论的发展和交换环论的诞生

1.1. 戴德金的理想概念. 理查德戴德金 (Richard Dedekind, 1831-1916) 是高斯的关门弟子, 于 1852 年在哥廷根拿到博士学位. 然而那时他在高等数学上的训练还不太够. 在狄利克雷 1855 年接替高斯在哥廷根的位置后, 戴德金和黎曼都听了狄利克雷的很多课程, 这对于他作为数学家的提升有相当大的好处. 戴德金在分析上的主要贡献是使用戴德金切割重新定义了无理数, 而他对于理想概念的引入则给他在代数和数论领域带来持久荣光.

1859 年狄利克雷逝世后, 戴德金开始整理狄利克雷的数论课程讲义. 1863 年它以《数论讲义》(Vorlesungen über Zahlentheorie) 的名字出版. 必须注意到

> 尽管这本书毫无疑问基于狄利克雷的讲义, 尽管在戴德金一生中都将这本书引用为狄利克雷的著作, 但是这本书实际上完完全全是戴德金写作的, 其中大部分是在狄利克雷逝世以后.

在 1879 年和 1894 年《数论讲义》的第三版和第四版, 戴德金写作了几个附录, 其中他引进了理想的概念. 戴德金是在代数数域整数环上构造他的理论的, 这是因为一般意义上的环的概念当时还不存在.

对于库默尔定义的理想复数 (除子) A, 令

$$I(A) = \{f(\alpha) \in \mathbb{Z}[\alpha] \mid f(\alpha) \equiv 0 \mod A\}.$$

戴德金注意到 A 完全由 $I(A)$ 决定而且对于 $f(\alpha)$ 和 $g(\alpha) \in I(A)$, $h(\alpha) \in \mathbb{Z}[\alpha]$, 总有

$$f(\alpha) \pm g(\alpha) \in I(A), \quad h(\alpha)f(\alpha) \in I(A) \tag{12}$$

他称满足方程 (12) 的 $Z[\alpha]$ 的子集合为理想, 并且证明如果 I 是 $Z[\alpha]$ 的理想, 那么存在除子 A 使得 $I = I(A)$.

代数数域的整数环, 也就是戴德金发展理想概念的地方, 现在是戴德金环的一个例子. 戴德金还引入了数域的 zeta 函数的概念, 现在这个 zeta 函数称为戴德金 zeta 函数. 他甚至还引入了域的概念 (德文称为 Körper).

由于库默尔, 狄利克雷和戴德金的工作, 我们就有了代数数论基础. 具体说来, 设 K 是数域而 O_K 是 K 的整数环. 则

定理 37 (戴德金). *整数环 O_K 的每个非零素理想都是极大理想且它的每个理想都可以唯一表示为素理想的乘积.*

定理 38 (狄利克雷). *单位群 $O_K^\times$ 是有限生成阿贝尔群, 秩为 r_1+r_2-1, 其中 r_1 是 K 的实嵌入个数, r_2 是 K 的复嵌入对的个数.*

定理 39 (库默尔). *K 的理想类群 Cl_K 是有限阿贝尔群.*

对于数域 K, 戴德金 Zata 函数即

$$\zeta_K(s)=\sum_{\mathfrak{a}}(N\mathfrak{a})^{-s}\ (\mathrm{Re}(s)>1)$$

其中 $\mathfrak{A}$ 过 O_K 的所有整理想. Hecke 证明 $\zeta_K(s)$ 有一个函数方程可以开拓到整个复平面, 并且它在 $s=0$ 处的首项系数与 K 的类数有关 (称为解析类数公式).

1.2. 交换环论的诞生. 一般环的定义是大卫 • 希尔伯特 (David Hilbert, 1862-1943) 引入的. 希尔伯特第一个工作是关于不变量理论的, 他在 1888 年证明了著名的希尔伯特基定理, 论文于 1890 年出版. 20 年前保罗 • 戈登 (Paul Gordan, 库默尔的学生) 通过高度计算化的技巧证明了二次型的有限基定理. 希尔伯特则采用了全新的技巧用完全抽象的办法证明对任意多个变量的有限基定理. 接下来在 1893 年他发表零点定理 (Nullstellensatz) 的证明. 在这期间他引入了环的概念. 希尔伯特这两个定理现在被广泛应用于交换环论和代数几何.

1.3. 诺特和抽象代数. 作为戈登的学生, 艾米 • 诺特 (Emmy Noether, 1882-1935) 最初也研究不变量理论. 诺特的博士论文采用戈登的构造性方法, 列举了 331 个共变型. 但她逐渐转向希尔伯特的抽象方法. 1915 年希尔伯特和克莱因邀请诺特到哥廷根工作. 来到哥廷根后她首先在理论物理领域证明了一个很基本的定理. 1919 年开始诺特从不变量理论研究转向研究理想的理论, 与埃米尔 • 阿廷以及她的学生们一起, 发展了抽象代数的理论. Idealtheorie in Ringbereichen (1921) 对于近世代数的发展有根本的重要性. 在这篇文章中, 她证明了满足升链条件的交换环 (即后来的诺特环) 中的理想

是准素理想的交, 这推广了伊曼纽尔 • 拉斯克 (Emanuel Lasker, 1868-1941, 1894 年-1921 年的国际象棋世界冠军, 艾米的父亲马克斯 • 诺特的学生) 在域的多项式环上的工作. 诺特学派的很多结果被收入范德瓦尔登 (van der Waerden, 1903-1996) 两卷本《近世代数》(Modern Algebra, Vol. I 1930, Vol. II 1931). 这本书促成了抽象代数在公众中的流行.

2. 克罗内克青春之梦和类域论

2.1. 克罗内克和他的青春之梦 (Jugendtraum). 利奥波德 • 克罗内克 (Leopold Kronecker, 1823-1891), 如我们前面所说, 是库默尔的高中学生. 他也是狄利克雷的博士生. 他的著名口号是

"上帝创造了整数, 所有其他的都是人做的工作".

1853 年, 他声称证明了下面的定理:

定理 40. *若 $K/\mathbb{Q}$ 是有限阿贝尔扩张, 则 $K \subseteq \mathbb{Q}(\zeta_n)$ 对某个 n 成立.*

这个定理叫克罗内克-韦伯定理, 韦伯在 1886 年给了一个证明, 但 90 年后人们发现证明中的一个小错误. 这个定理第一个正确的证明是希尔伯特在 1896 年给出的.

克罗内克青春之梦 (Jugendtraum, dream of youth) 是他对于构造虚二次域有限阿贝尔扩张的尝试, 由他在 1880 年给戴德金的信中提出:

猜想 1 (克罗内克青春之梦). *虚二次域 k 的任何有限阿贝尔扩张都包含在 k 的某个由带复乘的椭圆函数特殊值生成的扩张中.*

这里我们要注意下述几点:

(1) 阿贝尔 (1829) 通过椭圆函数特殊值构造了 $\mathbb{Q}(i)$ 的一些有限阿贝尔扩张.
(2) 克罗内克本人推广了阿贝尔的工作.
(3) 椭圆函数理论是 19 世纪数学研究的主流, 很多杰出的数学家都在这个领域工作, 比如阿贝尔，雅可比, 伽罗瓦, 魏尔斯特拉斯, 克罗内克, 等等.

从 1860 年代开始直到逝世, 克罗内克是数学界的领袖, 所以他的问题自然得到很多关注. 韦伯在证明克罗内克-韦伯定理的尝试中引入了同余理想类群和同余类域的概念. 接着希尔伯特引入了现在所谓的希尔伯特类域, 即数域 K 的极大不分歧阿贝尔扩张 H, 它的伽罗瓦群 $\mathrm{Gal}(H/K) = \mathrm{Cl}_K$. 1914 年，Fueter 证明

定理 41. 克罗内克青春之梦对于虚二次域的奇数次阿贝尔扩张是正确的.

2.2. 高木贞治. 高木贞治 (Teij Takagi, 1875-1960) 是第一位伟大的现代日本数学家. 高木的博士论文是基于他在哥廷根大学学习时的工作, 他在文中证明了 $\mathbb{Q}(i)$ 的克罗内克青春之梦, 推广了阿贝尔和克罗内克的工作. 他的论文于 1903 年发表. 此后直到 1914 年, 他集中精力为日本写教科书, 没有做任何的研究工作. 一战爆发造成日本与欧洲的学术世界的隔绝. 高木在战前收到的最后一篇论文是 Fueter 的文章. 为了维持在数学研究前沿, 从 1914 年开始, 高木致力于研究类域论, 最终他得到了类域论的主要定理.

我们来介绍一下高木的工作.

定义 20. 记模 $\mathfrak{m} = \mathfrak{m}_f \cdot \mathfrak{m}_\infty$, 其中 $\mathfrak{m}_f$ 是 O_K 的非零理想而 $\mathfrak{m}_\infty$ 是 K 的实嵌入的形式积.

(1) 记 $I_\mathfrak{m}$ 为所有与 $\mathfrak{m}$ (即与 $\mathfrak{m}_f$) 互素的分式理想群, 记 $P_\mathfrak{m}$ 为 $I_\mathfrak{m}$ 中由主分式理想 (α/β) 生成的子群, 其中

(i) (α) 和 (β) 与 $\mathfrak{m}_f$ 互素.

(ii) $\alpha \equiv \beta \mod \mathfrak{m}_f$.

(iii) $v(\alpha/\beta) > 0$ 对所有 $v \mid \mathfrak{m}_\infty$, $v : K \longrightarrow \mathbb{R}$ 成立.

(2) 群 $I_\mathfrak{m}/P_\mathfrak{m}$ 称为 K 模 $\mathfrak{m}$ 的广义理想类群.

(3) I_K 的子群 H 称为理想群是指存在模 $\mathfrak{m}$ 使得 $P_\mathfrak{m} \subseteq H \subseteq I_\mathfrak{m}$.

例 17. 令 $N_\mathfrak{m}(L/K) = \{\mathfrak{A} \subseteq K \mid \mathfrak{a} = N_{L/K}(\mathfrak{A}) \text{ 与 } \mathfrak{m} \text{ 互素}\}$, 则 $H_\mathfrak{m}(L/K) = P_\mathfrak{m} N_\mathfrak{m}(L/K)$ 是理想群.

定义 21. L/K 称为类域是指 $[I_\mathfrak{m} : H_\mathfrak{m}(L/K)] = [L : K]$ 对某个 K-模 $\mathfrak{m}$, 这个模 $\mathfrak{m}$ 称为可容许的. 最小的可容许模称为 L/K 的导子, 并记为 $\mathfrak{f}_{L/K}$.

定理 42 (高木贞治 1920). 设 K 是数域.

(1) *存在性:* 对于任何理想群 H, 存在 K 的一个类域.

(2) *同构定理:* 若 H 是模 $\mathfrak{m}$ 的理想群且有类域 L/K, 则 $\mathrm{Gal}(L/K) \cong I_\mathfrak{m}/H$.

(3) *完备性:* K 的任何有限阿贝尔扩张都是类域.

(4) *比较定理:* 若 H_1 和 H_2 有共同的模 $\mathfrak{m}$ 而他们的类域分别是 L_1 和 H_2, 则 $L_1 \subseteq L_2$ 当且仅当 $H_2 \subseteq H_1$.

(5) *导子:* 对于有限阿贝尔扩张 L/K, K 的在导子 $\mathfrak{f}_{L/K}$ 中出现的素位是 L/K 上分歧的素位.

(6) 分解定理: 若 H 是模 $\mathfrak{m}$ 的理想群, 它的类域是 L/K, 则每个不整除 $\mathfrak{m}$ 的素理想 $\mathfrak{p}$ 都不在 L 上分歧且它的剩余类域次数 $f_{\mathfrak{p}}(L/K)$ 等于 $\mathfrak{p}$ 在 $I_{\mathfrak{m}}/H$ 的阶.

定理 43 (高木). 克罗内克青春之梦是正确的.

定理 44. 设 K 是虚二次域, $E: y^2 = 4x^3 - g_2x - g_3$ 是 $\mathbb{C}$ 上的椭圆曲线且 $\mathrm{End}(E) \cong O_K$, 则

(1) K 的最大非分歧阿贝尔扩张 (即 K 从希尔伯特类域) 是 $K(j(E))$, 这里 $j(E) = \frac{1728g_2^3}{g_2^3 - 27g_3^2}$ 是 E 的 j-不变量.

(2) K 的所有有限阿贝尔扩张的复合是 $K^{ab} = K(j(E), \phi_E(T) : T \in E_{\mathrm{tors}})$, 这里 $\phi_E : E \longrightarrow \mathbb{P}'$ 是韦伯函数:

$$P \longmapsto \begin{cases} \dfrac{g_2g_3}{g_2^3 - 27g_3^2} \cdot x(P), & 若 j(E) \neq 0, 1728, \\ \dfrac{g_2^2}{g_2^3 - 27g_3^2} \cdot x(P)^2, & 若 j(E) = 1728, \\ \dfrac{g_3}{g_2^3 - 27g_3^2} \cdot x(P)^3, & 若 j(E) = 0. \end{cases}$$

2.3. 阿廷互反律. 在他于抽象代数领域做出主要贡献之前, 奥地利数学家埃米尔 • 阿廷 (Emil Artin, 1898-1962) 完成了类域论. 高木同构定理说明有一个同构 $I_{\mathfrak{m}}/H_{\mathfrak{m}} \cong \mathrm{Gal}(L/K)$. 阿廷则则将这个同构用互反映射清楚说明:

定理 45 (阿廷, 1927). 若 $\mathfrak{m}$ 是一个 K-模, 被 K 在 L 上分歧的素位整除, 则阿廷映射

$$\Phi_{L/K,\mathfrak{m}} : I_{\mathfrak{m}} \longrightarrow \mathrm{Gal}(L/K) \quad \mathfrak{p} \longmapsto \mathrm{Frob}_{\mathfrak{p}}(L/K) \text{ 对任意} \mathfrak{p} \nmid \mathfrak{m}$$

是满射. 若 $\mathfrak{m}$ 是可容许的, 则 $\Phi_{L/K,\mathfrak{m}}$ 诱导同构

$$I_{\mathfrak{m}}/H_{\mathfrak{m}}(L/K) = I_{\mathfrak{m}}/P_{\mathfrak{m}}N_{\mathfrak{m}}(L/K) \cong \mathrm{Gal}(L/K).$$

阿廷证明阿廷互反律的灵感来自于苏联数学家尼古拉 • 格里戈里耶維奇 • 切博塔廖夫 (Nikolai Grigorévich Chebotarev, 1894-1947) 1922 年证明一般密度定理的思路. 切博塔廖夫密度定理本身也是类域论的一部分, 是狄利克雷密度定理的推广:

定理 46 (切博塔廖夫). 对于有限伽罗瓦扩张 L/K, $\mathrm{Frob}_{\mathfrak{p}}$ 落在伽罗瓦群 $G = \mathrm{Gal}(L/K)$ 某个共轭类 C 中的 L 的素理想 $\mathfrak{p}$ 的密度等于 $|C|/|G|$.

3. 从局部到整体

3.1. 亨泽尔. 科特 • 亨泽尔 (Kurt Hensel, 1861-1941) 是克罗内克的学生, 他的祖母是著名的作曲家范妮门 • 德尔松. 1897 年他发明了 p 进数. 在整数环 $\mathbb{Z}$ 上, 如果 $p^a||n$, 令 $|n|_p = p^{-a}$, 通过这个方法就可以在 $\mathbb{Z}$ 上对每个素数 p 定义 p 进度量, 并通过 $|\frac{a}{b}|_p = |a|_p \cdot |b|_p^{-1}$ 延拓到 $\mathbb{Q}$ 上. 由此 $\mathbb{Q}$ 在 p 进度量意义下成为度量空间.

定理 47 (Ostrowski). *一般绝对值 $|\cdot|$ 和 p 进度量 $|\cdot|_p$ 是等价意义下 $\mathbb{Q}$ 上的所有不同度量.*

亨泽尔通过 p 进度量完备化 $\mathbb{Q}$, 从而得到 p 进数域 $\mathbb{Q}_p$. p-进整数环, 通常记为 $\mathbb{Z}_p$, 就是整数环 $\mathbb{Z}$ 的 p-进完备化.

现今, 有理数域 $\mathbb{Q}$ 和有理函数域 $\mathbb{F}_p(t)$ 的有限扩张被称作整体域, 而它们在各种赋值下的完备化称为局部域. $\mathbb{Q}$ 的有限扩张也称为数域而 $\mathbb{F}_p(t)$ 的有限扩张则被称作整体函数域. Ostrowski 定理的推广形式告诉我们数域 K 等价度量由它的整数环 O_K 的理想以及 K 的实和复嵌入 (其中两复嵌入通过复共轭等价) 给出. 这些度量称为 K 的素位. 对于整体函数域也有类似结果. 这样就有了如下对应:

$$\text{赋值理论} \Longleftrightarrow \begin{cases} O_K\text{的理想} \\ \text{实嵌入} \\ \text{复嵌入对} \end{cases}$$

3.2. 哈塞原理. 赫尔穆特 • 哈塞 (Hermut Hasse, 1898—-1979) 是德国数学家，因对亨泽尔创造的 p 进数极为感兴趣而转到亨泽尔所在的马尔堡大学学习, 在亨泽尔的指导下于 1921 年获得博士学位. 1920 年他证明了如下定理:

定理 48 (哈塞 -闵可夫斯基). *设 $f(x_1, \cdots, x_n)$ 是有理数域 $\mathbb{Q}$ 上的二次函数. 则方程 $f(x_1, \cdots, x_n) = 0$ 在 $\mathbb{Q}$ 上有解当且仅当方程在 $\mathbb{Q}_p$ (p 过所有素数) 上和在 $R = \mathbb{Q}_\infty$ 有解.*

这个定理引出了现代数论广泛使用的研究方法, *哈塞原理*或谓 *局部整体原理*: 研究一个整体域, 应该首先研究它的所有局部域, 然后再寻找局部与整体的差异, 这个差异通常会由某个上同调群刻画.

3.3. Adèles 和 Idèles. 法国数学家、布尔巴基学派的创始人之一克劳德 • 谢瓦莱 (Claud Chevalley, 1909-1984) 于 1936 年和 1941 年分别引入了 adèles 和 idèles 的概念.

设 K 是数域. K 的 adèle 环是所有 K 的局部域 K_v 相对于整数环 O_{K_v} 的限制乘积:

$$\mathbb{A}_K = \prod_{}^{\prime} K_v = \{(a_v) \in \prod_v K_v \mid a_v \in O_{K_v} \text{ 对几乎所有是素位} v \text{ 成立}\}.$$

K 的 idèle 群是所有 $K_v^\times$ 相对于 $O_{K_v}^\times$ 的限制乘积:

$$J_K = \mathbb{A}_K^\times = \prod_{}^{\prime} K_v^\times v = \{(a_v) \in \prod_v K_v^\times \mid a_v \in O_{K_v}^\times \text{ 对几乎所有是素位} v \text{ 成立}\}.$$

由此, 类域论就可以用 idèle 的语言来描述. 注意到

$$K^\times \hookrightarrow J_K, \quad a \longmapsto (a, a, \cdots).$$

令 $U = \prod O_{K_v}^\times$, 令 idèle 类群 $C_K = J_k/K^\times$.

定理 49. *设 K 是数域.*

(1) *若 L/K 是阿贝尔扩张, 则 $J_K/K^\times N_{L/K} J_L \cong \mathrm{Gal}(L/K)$.*

(2) *若 H 是群 J_K 有限指数开子群而且 $K^\times \subseteq H$, 则存在唯一的有限阿贝尔扩张 L/K 使得 $K^\times N_{L/K} J_L = H$.*

(3) *$L_1 \subseteq L_2$ 当且仅当 $K^\times N_{L_1/K} J_{L_1} \supseteq K^\times N_{L_2/K} J_{L_2}$.*

4. 门德尔松家族和 19 世纪的数学大家

摩西 • 门德尔松 (Moses Mendelssohn, 1729 年 9 月 6 日–1786 年 1 月 4 日) 是 18 世纪启蒙时代德国犹太哲学家, 是近代犹太史上的重要人物. 他对宗教包容的提倡引起具前瞻性的天主教徒和犹太教徒的共鸣. 他支持宗教信仰自由、政治宽容，倡导公民平等而不必遵循教条. 1763 年, 门德尔松因一篇将数学证明应用到形而上学的文章赢得柏林科学院大奖, 而康德只赢得提名奖.

摩西 • 门德尔松有六个孩子. 他的儿子亚伯拉罕 • 门德尔松 (Abraham Mendelssohn, 1776-1835) 是德国首屈一指的银行家, 他有两个儿子费力克斯和保罗, 和两个女儿范妮和瑞贝卡. 费利克斯 • 门德尔松 (Felix Mendelssohn, 1809-1847) 是德国作曲家, 钢琴家, 指挥家, 教师, 神童和早期浪漫时代最具代表性的人物之一，他的著名作品包括《仲夏夜之梦》序曲 (1826), 《意大利交响曲》(1833), 小提琴协奏曲 (1844), 两部钢琴协奏曲 (1831, 1837) 和清唱剧《以利亚》(1846) 等.

范妮 • 门德尔松 (Fanny Mendelssohn, 1805-1847), 婚后的名字即范妮 • 亨泽尔, 是钢琴家和作曲家, 费利克斯的大姐和最信赖的人. 范妮据说是和弟弟相当的音乐天才. 两个人的关系十分亲密, 1847 年范妮的过早去世让费利克斯悲痛欲绝, 最终他在六个月后也离开人世. 1829 年范妮与普鲁士宫廷画家威尔海姆 • 亨泽尔结婚. 他们的儿子塞巴斯蒂安 • 亨泽尔根据范妮的日记和书信写作了门德尔松家族的传记, 里面提及了费利克斯很多生活细节. 塞巴斯蒂安有两个儿子, 哲学家保罗 • 亨泽尔和数学家科特 • 亨泽尔.

瑞贝卡 • 门德尔松 (Rebecka Mendelssohn, 1811-1858), 是范妮和费利克斯的妹妹, 她嫁给了狄利克雷. 她于丈夫去世之前一年离开人世.

内森 • 门德尔松 (Nathan Mendelssohn, 1781-1852) 是摩西的小儿子, 亚伯拉罕的弟弟, 他是数学教具制造商. 内森的女儿, 奥蒂莉嫁给了库默尔, 而他们的一个女儿, 玛丽 • 伊丽莎白 • 库默尔, 则嫁给了库默尔的学生赫尔曼 • 施瓦兹, 也就是我们熟知的柯西-施瓦兹不等式的施瓦兹. 施瓦兹在微分几何特别是极小曲面领域有重大贡献. 1892 年他从哥廷根大学教授位置离开, 来柏林继承魏尔斯特拉斯在柏林大学的位置, 之后希尔伯特于 1895 年去了哥廷根. 这一系列人员移动, 促成了哥廷根大学的崛起和柏林大学的衰落. 此后哥廷根成为世界数学的中心, 直到 1930 年代被纳粹政府驱散.

我们知道, 克罗内克是库默尔和狄利克雷的学生, 也是科特 • 亨泽尔的导师, 而亨泽尔是哈塞的导师. 所以我们可以看出门德尔松家族和 19 世纪数论学界甚至整个数学界的紧密联系.

CHAPTER 5

伽罗瓦上同调和伽罗瓦表示

1. 重访伽罗瓦理论

我们现在回到伽罗瓦理论. 这个领域的一个主要问题是

1.1. 伽罗瓦理论的反问题/反伽罗瓦问题.

问题 2. 给定有限群 G, 是否存在伽罗瓦扩张 $K/\mathbb{Q}$, 使得 $\mathrm{Gal}(K/\mathbb{Q}) = G$?

注记 7. (1) 若将 $\mathbb{Q}$ 换为某些别的域 F 时, 则上面问题的答案是肯定的:

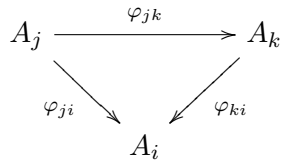
- $F = \mathbb{C}(t)$.
- $F = K(t)$ 其中 K 是 p 进域.

(2) Kronecker-Weber 定理是说当 G 是阿贝尔群时, 答案是肯定的.
(3) 对于 G 非交换, 问题还是开放的:

- 1892 年希尔伯特证明了 $G = S_n$ 和 A_n 的情形.
- 诺特一个著名定理声称: 令 $M = \mathbb{Q}(t_1, ..., t_n)$, G 是 S_n 的可迁子群而 $K = M^G$, 若 K 同构于有理数域 $\mathbb{Q}$ 的有理函数域, 则反伽罗瓦问题对于群 G 是肯定的.
- Scholz-Reichardt (1937) 证明 G 是 p-群的情形, 其中素数 $p > 2$.
- Shafarevich 于 1954 年证明 G 是可解群的情形.
- 对于单群, $\mathrm{PSL}(2, p)$ $(p \leq 7)$ 和除 M_{23} (Mathieu 群) 外的所有散在单群答案都是肯定的.

1.2. 无限伽罗瓦扩张. 设 I 是有向集, 这是说 I 上存在偏序满足条件: 对任意 i 和 $j \in I$, 均存在 k 使得 $i < k$ 且 $j < k$ 成立. 射影系 $(A_i)_{i \in I}$ 则是可以如下描述: A_i $(i \in I)$ 是某个具有无穷乘积的阿贝尔范畴的对象, 比如集

合, 群，环或者域, 且对于任意 $i<k<j$, 存在此范畴的交换图表:



射影系的射影极限即

$$\varprojlim_{i\in I} A_i := \{(a_i)_{i\in I} \mid \varphi_{ji}(a_j)=a_i \quad \text{对所有 } j>i\text{成立}\} \subseteq \prod_{i\in I} A_i.$$

如果对象 A_i 都是拓扑空间, 那么 $\prod_i A_i$ 被赋予乘积拓扑而 $\varprojlim_i A_i$ 可以看作 $\prod_i A_i$ 的闭子集. 例如, 若 A_i 是有限集合, 通常可以赋予它们离散拓扑, 则由吉洪诺夫定理, $\prod_i A_i$ 是紧致豪斯多夫拓扑空间, 同样射影极限 $\varprojlim_i A_i$ 也是如此, 此时称为是射影有限极限.

例 18. 对于素数 p, 射影系 $(\mathbb{Z}/p^n\mathbb{Z}))_n$ 的连接映射为限制映射 $\mathbb{Z}/p^n\mathbb{Z}\to\mathbb{Z}/p^m\mathbb{Z}(n\geq m)$, 它的射影极限

$$\varprojlim_{n} \mathbb{Z}/p^n\mathbb{Z}$$

与 p 进整数环 $\mathbb{Z}_p$ 典范同构, 由极限得到的射影有限拓扑与 $\mathbb{Z}_p$ 本身的 p 进拓扑是同一个拓扑.

我们回顾定义

定义 22. 伽罗瓦扩张是代数可分正规扩张.

设 L/K 是无限伽罗瓦扩张. 注意到如果 M/K 是 L 的有限子扩张, 那么 M 的伽罗瓦闭包 N/K 是 L 的有限伽罗瓦子扩张. 现在令 $I=\{E/K \mid K\subset E\subset L,\ E/K \text{ 是有限伽罗瓦扩张}\}$, 并赋予它由包含关系确定的偏序. 对于 $E\subset F\in I$, 则存在自然映射 $\mathrm{Gal}(F/K)\to\mathrm{Gal}(E/K)$. 这样就得到有限群的射影系 $(\mathrm{Gal}(E/K))_{E\in I}$.

定义 23. 伽罗瓦群 $\mathrm{Gal}(L/K)$ 即有限射影系 $(\mathrm{Gal}(E/K))_{E\in I}$ 的射影极限, 即

$$\mathrm{Gal}(L/K) = \varprojlim_{\substack{K\subset E\subset L \\ E/K \text{ 有限伽罗瓦}}} \mathrm{Gal}(E/K).$$

由定义，伽罗瓦群是射影有限群, 因此是豪斯多夫和紧致的拓扑空间. 注意到 L/K 如是有限扩张, 上述定义与原来的定义是一致的. 对于 $x\in L$

和 $\sigma = (\sigma_E)_{E\in I} \in \mathrm{Gal}(L/K)$, 令 M 是包括 x 的一个有限伽罗瓦子扩张 (例如, $K(x)$ 的伽罗瓦闭包), 令 $\sigma(x) = \sigma_M(x)$. 则 $\sigma(x)$ 独立于 M 的选取. 这样就定义了 L 上的 $\mathrm{Gal}(L/K)$-作用.

定理 50 (伽罗瓦理论基本定理). *设 L/K 是伽罗瓦扩张, 其伽罗瓦群 $G = Gal(L/K)$. 那么存在一一对应:*

$$\begin{array}{ccc} \{G\text{的闭子群}\} & \longleftrightarrow & \{L/K \text{ 的代数子扩张}\} \\ H & \longmapsto & L^H \\ \mathrm{Gal}(L/M) & \longleftarrow & M \end{array}$$

更进一步地, 此对应给出

(1) 正规子群对应伽罗瓦子扩张.

(2) 开子群对应有限子扩张. 此时 $[G:H] = [M:K]$.

(3) 开正规子群对应有限伽罗瓦子扩张. 此时 $G/H \cong \mathrm{Gal}(M/K)$.

例 19. (1) 令 K^s 是域 K 的可分闭包, $G_K = \mathrm{Gal}(K^s/K)$ 称为 K 的绝对伽罗瓦群. 注意到若 $\mathrm{char}(K) = 0$, 则 $K^s = \overline{K}$ 是 K 的代数闭包.

(2) 设 p 是素数. 设存在域扩张塔

$$K = K_0 \subseteq K_1 \subseteq ... \subseteq K_n \subseteq ... \subseteq \bigcup_{n\in N} K_n = K_\infty$$

使得

$$\begin{array}{ccc} \mathrm{Gal}(K_n/K_0) & \xrightarrow{\cong} & Z/p^nZ \\ {\scriptstyle res}\downarrow & & \downarrow{\scriptstyle res} \\ \mathrm{Gal}(K_{n-1}/K_0) & \xrightarrow[\cong]{} & Z/p^{n-1}Z \end{array}$$

则

$$\mathrm{Gal}(K_\infty/K) = \varprojlim_n \mathrm{Gal}(K_n/K) \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p.$$

K_∞/K 称为一个 $\mathbb{Z}_p$-扩张. 由于 $\mathbb{Z}_p$ 的闭子群为 0 (它不是开子群) 和 p^nZ_p ($n \geq 0$, 它们也是开子群), 因此 K_∞/K 包含的子扩张为 K_∞ 和 K_n.

研究数域的 $\mathbb{Z}_p$-扩张现在称为岩泽理论 (Iasawa Theory), 此方面的研究由岩泽键吉于 1950 年代末开始.

设 K 是数域而 G_K 是它的绝对伽罗瓦群. 对于 K 的每个素位 v (即 O_K 的素理想或实嵌入 $K \to R$ 或复嵌入对 $K \to \mathbb{C}$), 令 $G_{K_v} = \mathrm{Gal}(\overline{K_v}/K_v)$.

则图表

$$\begin{array}{ccc} K & \xrightarrow{\subset} & K_v \\ \cap\downarrow & & \downarrow\cap \\ \bar{K} & \xrightarrow[\subset]{} & \bar{K}_v \end{array}$$

说明 G_{K_v} 可以看作是 G_K 的子群.

数论的主要问题是对于数域 K 研究 G_K 的结构, 特别是 $K=\mathbb{Q}$ 的情形.

(1) 令 $G_K^{ab}=G_k/\overline{[G_K,G_K]}$ 是 G_K 的极大阿贝尔商. 则

$$\text{研究}G_K^{ab}\longleftrightarrow\text{描述 }K\text{ 的阿贝尔扩张}\longleftrightarrow\text{类域论}.$$

现在已经知道:

- 局部类域论: 对于局部域 K, 研究 G_K^{ab} 等同于研究 $K_v^\times$ 的完备化.
- 整体类域论: 对于整体域 K, 研究 G_K^{ab} 等同于研究 idèle 类群 $C_K=J_K/K^\times$.

(2) 局部-整体原理 (即哈塞原理): 先研究局部片 G_{K_v}, 再找一个方式将它们拼起来.

(3) 研究群需要研究它的表示. 对于数域/局部域, 需要研究

复 (即 $\mathbb{C}$-) 表示，ℓ-进和 p-进表示, $\mathbb{Z}_p$-表示和 $\mathbb{F}_p$-表示等.

2. 伽罗瓦上同调和伽罗瓦表示

2.1. 约翰·泰特. 1940 年代, 代数拓扑和同调代数在 Levy, Henri Cartan-Eilenberg, Serre 和其他数学家手中经历了迅猛发展. 约翰•泰特 (John Tate, 1925-2019) 则是将上同调工具融入到数论研究的关键人物.

泰特是阿廷的学生和女婿. 由于在数论和算术几何上的巨大贡献, 他于 2010 年荣获阿贝尔奖, 于 2002/03 年荣获沃尔夫奖. 作为我们这个时代最伟大的数学家之一, 他的成就包括

(1) 泰特 1950 年在普林斯顿大学的博士论文发展了数域上的傅里叶分析, 为研究自守表示和朗兰兹纲领铺平了道路. 可以说从来没有同时同地的两篇数学博士论文比两个约翰 (泰特和纳什) 1950 年完成的普林斯顿大学博士论文更为重要.

(2) 1950 年代阿廷和泰特开始使用上同调语言改写类域论. 他们的工作包括在经典著作《类域论》(Harvard 1961, W.A.Benjamin 1967) 中. 在书中伽罗瓦上同调现代语言被使用来证明局部和整体类域论.

(3) 泰特 (p-divisible group, Proc. of a Conference on Local fields, 158-183,1967) 创立了 p-可除群理论, 现在 p-可除群也叫 Barsotti-Tate 群. 这是 p-进霍奇理论的开始, 后来由让-马克 • 方丹 (Jean-Marc Fontaine, 1944-2019) 和其他人发扬光大.

(4) 泰特 (Rigid analytic space. Invent.Math.12, 257-289 1971) 引入了刚性解析空间的概念, 作为复解析空间的类比, 这是当今数论研究最热门的概念之一.

(5) 很多数学术语以泰特命名, 或许比任何其他的现代数学家都要多: Tate 模, Tate 曲线, Tate 链, Tate 代数, Hodge-Tate 分解, Tate 上同调, Lubin-Tate 群, Shafarevich-Tate 群, Néron-Tate 高度, $\cdots$

2.2. 伽罗瓦上同调. 设 K 是域而 L/K 是伽罗瓦扩张. 则伽罗瓦群 $\mathrm{Gal}(L/K)$ 作用于很多算术对象上:

$$L,\ L^\times,\ \mu(L),\ \text{等等.}$$

若 $L = K^s$ 是 K 的可分闭包, 则有 G_K-模 (伽罗瓦模)

$$K^{s\times},\ \mu_{p^\infty},\ \mu_n,\ A(K^s\ \ (A/K \text{ 是阿贝尔簇}),\ E(K^s)\ (E/K \text{ 是椭圆曲线}) \text{ 等.}$$

因此很自然可以使用群的上同调和同调来研究这些对象.

设 G 是有限群而 A 是 G-模.

(1) 设 $H^0(G,A) = A^G$, 函子 $A \mapsto A^G$ 的导出函子给出高阶上同调群 $H^i(G,A)$;

(2) 设 $H_0(G,A) = A_G == A/\langle ga - a :\ a \in A,\ g \in G\rangle$, 函子 $A \mapsto A_G$ 给出高阶同调群 $H_i(G,A)$.

(3) 泰特引入泰特上同调 $\hat{H}^0(G,A)$ 和 $\hat{H}^{-1}(G,A)$, 将 A 的上同调群和同调群统一起来.

对于 G 是射影有限群而 A 是离散 G-模, 同样上同调群 $H^i(G,A)$ 由函子 $A \mapsto H^0(G,A) = A^G$ 导出.

对于 H^1, 希尔伯特的定理 90 说明

定理 51 (Hilbert Theorem 90). $H^1(\mathrm{Gal}(L/K), L^\times) = 0$.

由这个定理即得库默尔理论 (库默尔配对和库默尔扩张).

对于 H^2, Brauer 群 $\mathrm{Br}(L/K) = H^2(\mathrm{Gal}(L/K), L^\times)$ 和 $\mathrm{Br}(K) = H^2(G_K, K^{s\times})$. 类似定义局部域的 Brauer 群 $\mathrm{Br}(K_v)$. Brauer 群给出域上可除代数的分类. 通过研究 Brauer 群, 阿廷-泰特构造了阿廷互反映射并证明了局部和整体类域论.

更进一步地, 伽罗瓦上同调给出

- 泰特局部对偶,
- Poitou-Tate 正合列,

这些在数域研究中起关键作用.

注记 8. 关于伽罗瓦表示, 读者可参考下面两部经典著作:

(1) Serre: Galois cohomology

(2) Neukirch, Schmidt and Wingberg: Cohomology of number fields.

2.3. ℓ-进表示.

定义 24. 设 K 是域, $G_K = \mathrm{Gal}(K^s/K)$ 是它的绝对伽罗瓦群.

(1) 设 E 是 (拓扑) 域并配备 G_K 的 (连续) 作用. G_K 的 E-表示是指一个有限维 E-线性空间 V, 其上配备有 (连续) 半线性的 G_K 作用.

(2) 更进一步地, 设 R 是 (拓扑) 环并配备 G_K 的 (连续) 作用. G_K 的 R-表示是指一个有限生成 R-模 M, 其上配备有 (连续) 半线性的 G_K 作用.

注意到若 G_K 在 E 上作用平凡, 则上述定义中的半线性 $=$ 线性.

例 20. 设 ℓ 是素数, 则 $\mathbb{Q}_\ell$-表示称为 ℓ-进表示.

例 21. (1) 熟知分圆特征 $\chi : G_K \to \mathbb{Z}_\ell^\times$, 其中 $\chi(g)$ 由关系式 $g(\zeta) = \zeta^{\chi(g)}$ (对所有 $\zeta \in \mu_{\ell^\infty}(K^s)$ 和 $g \in G_K$ 成立) 给出. 乘法群的泰特扭 (Tate twist) 即

$$T_\ell(\mathbb{G}_m) = \varprojlim_n \mu_{\ell^n}(K^s) \cong \mathbb{Z}_\ell t = \mathbb{Z}_l(1),$$

$$V_\ell(\mathbb{G}_m) = \mathbb{Q}_\ell t = \mathbb{Q}_\ell(1) = \mathbb{Z}_\ell(1) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell,$$

这里 $g(t) = \chi(g)t$ 对所有 $g \in G_K$ 成立. 则 $T_\ell(\mathbb{G}_m)$ 是 G_K 的秩为 1 的自由 $\mathbb{Z}_\ell$-表示而 $V_\ell(\mathbb{G}_m)$ 是 G_K 的 1 维 ℓ-进表示.

(2) 对于 E 是 K 上的椭圆曲线, 或更一般地 A 是 K 上的阿贝尔簇, 可以定义泰特模 $T_\ell(E)$ (及 $V_\ell(E)$) 和 $T_\ell(A)$ (及 $V_\ell(A)$). 它们是 G_K 的 $\mathbb{Z}_\ell$ 和 $\mathbb{Q}_\ell$-表示.

(3) 设 X 是 K 上真光滑簇. ℓ-进上同调群 $H^m_{\mathrm{et}}(X_{K^s}, \mathbb{Z}_\ell)$ 和 $H^m_{\mathrm{et}}(X_{K^s}, \mathbb{Q}_\ell)$ 给出更一般的 G_K 的 $\mathbb{Z}_\ell$ 和 ℓ-进表示的例子, 泰特模是其特殊情况.

2.4. p-进伽罗瓦表示. 若 K 是局部域, 设它的剩余类域 k 是特征 p 域, 研究 ℓ-进表示有两种情况需要考虑:

- $p \neq \ell$, 这要容易一些;

- $p=\ell$, 这要困难许多. p-进霍奇理论就是研究剩余类域特征 p 的局部域的 p-进伽罗瓦表示.

设 V 是 p-进表示.

(1) 维数 $\dim_{\mathbb{Q}_p} V=1$ 的情形是泰特的工作.
(2) 令 $\mathbb{C}_p=\widehat{\overline{\mathbb{Q}_p}}$ 是 $\mathbb{Q}_p$ 的代数闭包的 p-进完备化. 令 $W=V\bigotimes_{\mathbb{Q}_p}\mathbb{C}_p\mathbb{C}_p$. 则 W 是 G_K 的一个 $\mathbb{C}_p$-表示. 泰特的学生 Sen 分类了所有 $\mathbb{C}_p$-表示. 这引出了 Hodge-Tate weight 和 Hodge-Tate 分解这些概念.

让-马克 • 方丹 (Jean-Marc Fontaine, 1944-2019) 创立了 p-进霍奇理论来研究 p-进伽罗瓦表示. 他构造了几个具有连续 G_K 作用的大拓扑环 (p-进周期环):

(1) B_{dR}^{+}, 这是一个离散赋值环, t 是素元而 $\mathbb{C}_p$ 是剩余类域 (因此它十分巨大). 它的分式域是 p 进周期域 B_{dR};
(2) B_{cris}, 这是从 divided power envelope 构造而来;
(3) B_{st}, 它是 B_{cris} 的多项式环.

Fontaine 构造的关键点如下. 设 k 是 K 的剩余类域. Fontaine 注意到

$$R=\varprojlim_{x\mapsto x^p} O_{\overline{K}}/pO_{\overline{K}}=\varprojlim_{x\mapsto x^p} O_{\overline{K}}$$

是一个完全赋值环, 具有混合特征, 剩余类域是 k 的代数闭包, 且

$$\mathrm{Fr}R=\varprojlim_{x\mapsto x^p}\overline{K}$$

是代数闭的. 则 $\pi=(1,\zeta_p,\cdots,)\in R$ 且

- $k[[\pi]]\subseteq R$.
- $\mathrm{Fr}R$ 是代数闭的, $=\widehat{k((\pi))^{sep}}$.
- Fontaine-Wittenberger 证明存在典范同构

$$\mathrm{Gal}(k((\pi))^{sep}/k((\pi)))\cong\mathrm{Gal}(\overline{K}/K(\zeta_{p^\infty})).$$

这样从 Witt 环 $W(R)$ 开始, Fontaine 构造了 B_{dR}, B_{cris} 和 B_{st}.

定义 25. 对于 $B=B_{\mathrm{dR}}, B_{\mathrm{st}}$ 或 B_{cris}, 若 $(B\otimes_{Q_p}V)^{G_K}$ 生成 $(B\otimes_{Q_p}V)$, 则称 V 是 B-表示.

一般说来,

- 晶体表示 (crystalline 表示) 通常是好的表示;
- p-进单值定理说明 de Rham 表示是 potentially 半稳定的 (即经过有限扩张后半稳定), 因此 de Rham 和半稳定表示几乎是一样的.

猜想 2 (Fontaine-Mazur). *设 V 是 $G_{\mathbb{Q}}$ 的连续不可约 ℓ-进表示. 则 V "来自于几何", 即*

$$V = \text{某代数簇 } X/\mathbb{Q} \text{ 的上同调群 } H^i_{\text{et}}(X_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}_\ell(j)}) \text{ 的子商}$$

当且仅当下面两个条件成立:

(1) V 是几乎处处非分歧的,

(2) 它在 $G_{\mathbb{Q}_\ell}$ 上的限制是 de Rham 表示.

注记 9. 维数 2 时的 Fontaine-Mazur 猜想由 Misin 和 Emerton 的工作证明, 它说明费马大定理成立.

2.5. 类完全域和类完全空间. 最后我们稍微提及一下 Peter Scholze 的伟大工作.

定义 26. Perfectoid 域 K 是完备拓扑域, 它的拓扑由一个秩 1 的非离散赋值诱导, 且 $\Phi : K^o/p \to K^o/p, x \mapsto x^p$ 是漫射, 此处 K^o 是 K 中幂有界的元素构成的集合.

例 22. $\mathbb{Q}_p(\zeta_{p^\infty})$, $\mathbb{Q}_p(\frac{1}{p^{p^\infty}})$, $\mathbb{C}_p$, 和 $\overline{\mathbb{Q}_p}$ 都是 perfectoid 域.

设 K 是 perfectoid 域. 令

$$K^\flat = \varprojlim_{x \mapsto x^p} K.$$

Scholze 发现 $K^\flat$ 是特征 p 的 perfectoid 域. 对于 $x \in K^\flat$, 则 $x = (x^{(0)}, x^{(1)}, ...)$, $(x^{(n+1)})^p = x^{(n)}$. 令

$$x^\sharp = x^{(0)} \in K.$$

Scholze 推广了 Fontaine-Wittenberger 的定理得到

定理 52. *$G_K \cong G_{K^\flat}$ 是典范同构.*

定义 27. Perfectoid K-代数 R 即一个巴拿赫 K-代数, 它的幂有界元素集合 R^o 是有界集且 $\Phi : R^o/p \twoheadrightarrow R^o/p,\ x \mapsto x^p$ 是满射.

类似定义 $R^\flat = \varprojlim_{x \mapsto x^p} R$ 和 $\sharp$.

定理 53. *存在自然的范畴等价:*

$$\{\textit{perfectoid } K\text{-代数}\} \longleftrightarrow \left\{\textit{perfectoid } K^\flat\text{-代数}\right\}$$

$$R \longmapsto R^\flat$$

$$(R^\flat)^\sharp \longleftarrow R^\flat$$

接下来 Scholze 开始研究刚性解析空间. 通过映射

$$(R, R^+) \longmapsto (R^\flat, R^{\flat +})$$

其中 R^+ 过 R^o 的开整闭子集，他证明 K 上和 $K^\flat$ 上的 affinoid perfectoid 代数范畴等价. 令 $X = \mathrm{Spa}(R, R^+)$ 是 Huber 的 Adic 空间, 其中的点是在 R^+ 上 ≤ 1 的连续赋值 $x: \quad R \mapsto\to \Gamma \cup 0, f \mapsto |f(x)|$ 的等价类.

定理 54. 令 $X = \mathrm{Spa}(R, R^+)$, $X^\flat = \mathrm{Spa}(R^\flat, R^{\flat +})$.

(1) 下面的映射是同胚映射:

$$\begin{aligned} X \quad &\longrightarrow \quad X^\flat \\ x \quad &\longmapsto \quad x^\flat \\ |f(x^\flat)| \ &= \ |f^\sharp(x)| \end{aligned}$$

(2) 映射诱导层之间的同构 $O_X \cong O_{X^\flat}$.

将这些 affinoid 片粘起来, 就得到 perfectoid 空间.

定理 55. K 上的 *perfectoid* 空间组成的范畴与 $K^\flat$ 上的 *perfectoid* 空间组成的范畴等价.

这给出如下用法尔廷斯的 almost mathematics 语言描述的一个定理:

定理 56. 设 R 是 *perfectoid* K-代数, 而 S/R 是有限平展的. 则 S 是 *perfectoid* K-代数, 而 S^o 在 R_o 上是几乎有限平展的.

最后令 X 是 perfectoid 空间, X_{et} 是它的平展 site. 则

定理 57. $X_{\mathrm{et}} \cong X^\flat_{\mathrm{et}}$ 作为 *site* 典范等价.