Introduction to Algebraic Number Theory

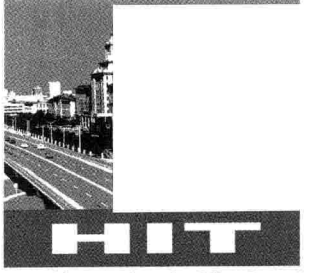
HIT

数学·统计学系列

代数数论入门

冯克勤 编著

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS



数学·统计学系列

代数数论入门

Introduction to Algebraic Number Theory

冯克勤 编著

HITP
哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

内 容 简 介

本书叙述代数数论的最基本内容，共分两大部分. 第一部分是代数理论，介绍代数数论中的代数结果和方法. 第二部分是解析理论，先精练介绍解析数论的思想和方法，然后叙述代数数论中的解析理论.

本书适合大学师生及数学爱好者参阅研读.

图书在版编目(CIP)数据

代数数论入门/冯克勤编著. —哈尔滨：哈尔滨工业大学出版社，2015. 3

ISBN 978-7-5603-4567-3

Ⅰ. ①代… Ⅱ. ①冯… Ⅲ. ①代数数论-高等学校-教材 Ⅳ. ①O156. 2

中国版本图书馆 CIP 数据核字(2014)第 010541 号

策划编辑 刘培杰 张永芹
责任编辑 张永芹 李 欣
封面设计 孙茵艾
出版发行 哈尔滨工业大学出版社
社 址 哈尔滨市南岗区复华四道街 10 号 邮编 150006
传 真 0451-86414749
网 址 http://hitpress. hit. edu. cn
印 刷 哈尔滨市石桥印务有限公司
开 本 787mm×1092mm 1/16 印张 15.25 字数 286 千字
版 次 2015 年 3 月第 1 版 2015 年 3 月第 1 次印刷
书 号 ISBN 978-7-5603-4567-3
定 价 38.00 元

引言

代数数论是研究代数数域(即有理数域的有限次扩域)和代数整数的一门学问. 历史上,它的产生是由于人们研究初等数论(即有理整数)的一些问题而引起的. 最主要的开拓者是两位伟大的德国数学家:高斯(Gauss, 1777—1855)和库默尔(Kummer, 1810—1893). 高斯研究二次互反律、二平方和问题(何种自然数可表示成两个自然数平方和)与二元二次型问题得到二次域整数环中素理想分解规律,类数性质和种(genus)理论;而库默尔对费马猜想的研究,给出分圆域的类数和分圆单位等方面一些深刻的结果和猜想. 我们想着重谈一下库默尔.

法国著名数学家费马(Fermat, 1601—1665)在学习和翻译丢番图(Diophantus)的《算术》一书时,在书的空边上写下了一个著名的"大定理":

方程 $x^n + y^n = z^n$ (n 为大于 2 的自然数)没有 $xyz \neq 0$ 的整数解. 他写道:"我发现了这个定理的证明,但是由于地方太小而写不下."

终于经过三百多年的时间和许多伟大的数学家的努力,这个"大定理"于 1994 年被证明.

容易看出,这个结果的证明可以归结为 $n=4$ 和奇素数的情形. 费马本人对于 $n=4$ 的情形给出了证明(无穷递降法),欧拉(Euler,1707—1783)和勒让德(Legendre,1752—1833)证明了 $n=3$ 的情形,狄利克雷(Dirichlet,1805—1859)证明了 $n=5$ 的情形. 1799 年,22 岁的高斯发表了天才的著作《数论探讨》(Disquisitions Arithmeticae),把初等数论的研究引进一个新的境界,他在二次域和它的整数环上来考虑有理整数的许多问题,得到大量在初等数论上的重要结果. 到了 19 世纪 30 年代至 50 年代,库默尔在研究费马猜想时,继承了高斯的这一创造性思想,他利用 n 次本原单位根 $\zeta_n=e^{2\pi i/n}$,把方程 $x^n+y^n=z^n$ 改写成

$$x^n=(z-y)(z-\zeta_n y)\cdots(z-\zeta_n^{n-1}y)$$

他以为在分圆域 $\mathbf{Q}(\zeta_n)$ 中的"整数"也和普通整数一样,可以唯一地分解成"素数"的乘积. 在这个前提下,库默尔"证明"了费马猜想. 但不久发现,上述前提是不对的! 换句话说,分圆域中的"整数"分解成"素数"的乘积时不具有唯一性. 这个发现使库默尔引入了"理想数"的概念,然后证明了:每个"理想数"可以唯一地分解成素因子的乘积,从而建立了分圆域的许多数论结果. 戴德金(Dedekind,1831—1916)把库默尔的工作系统化并推广到一般代数数域之上,建立了一般的理想论. 为了衡量一个代数整数环与唯一因子分解环相距多远,自然产生了理想类群和理想类数这样一些概念. 库默尔证明了,对于一个奇素数 p,如果分圆域 $\mathbf{Q}(\zeta_n)$ 的理想类数不能被 p 除尽,则费马猜想对于 $n=p$ 的情形是正确的. 于是,除了 37,59 和 67 之外,库默尔证明了费马猜想对于 100 以内的其余奇素数均是正确的. 这些工作不仅把对费马问题的研究推进到一个崭新的阶段,而且也把数论的研究推进到一个崭新的阶段,由此出现了一个新学科:代数数论.

继库默尔之后,对代数数论做出重大贡献的是另一位德国大数学家希尔伯特(Hilbert,1862—1943). 1897 年,希尔伯特应德国数学会的要求写了一本关于代数数论的大部头著作《数论报告》(Zahlbericht). 他在这本名著中系统地总结了直到库默尔和戴德金的研究成果,对于二次域、分圆域、库默尔域以及相对伽罗瓦扩域(特别是阿贝尔域)做了极为详尽的研究和论述. 在这个基础上,他对于数域的阿贝尔扩张提出了许多大胆的猜想. 1900 年在巴黎召开了第二次国际数学家大会. 希尔伯特在会上做了"数学问题"的演讲,提出了著名的二十三个问题. 这些问题涉及数学的许多领域,对于 20 世纪的数学发展起了极大的影响. 在这些问题当中,就有四个是属于代数数论(9~12). 例如,第 9 个问题是问:在代数数域中是否有像高斯二次互反律那样的一般互反律? 第 12 问题是:如何构作一个代数数域的极大阿贝尔扩域? 他预言这两个问题之间应当有深刻的联系. 希尔伯特的学生 Furtwängler 对于解决希尔伯特关于代数数域的上述猜想和问题做出了很大贡献. 经过许多数学家的努力,日本数学家高木贞

治(Takagi)于1920年最终完成了关于数域阿贝尔扩张的完整而优美的理论——类域论.

高木在建立类域论的过程中,除了吸取上面所述的代数成果之外,还使用了解析手段.代数数论中的解析工具主要包括Hensel(1861—1941)创建的局部化方法(p-adic赋值理论)和古典解析数论到代数数域上的推广与应用.我们现在简要地谈谈后者的历史.

最早用解析方法研究古典数论问题的是欧拉,中心课题是研究素数的分布.欧拉于1737年发现,"每个自然数均可唯一地表示成素数的乘积"这件事可以用下面的公式体现出来

$$\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_{p}\left(1-\frac{1}{p^s}\right)^{-1}\quad(s>1)$$

其中右边乘积是过全部素数p.利用这种新的看法,欧拉得到了素数的许多性质.这无疑是一个天才的发现,但是欧拉只是将$\zeta(s)=\sum_{n=1}^{\infty}n^{-s}$看作是实变量$s$的函数.进一步运用分析工具的是高斯的学生狄利克雷.他在19世纪数学家和理论物理学家的摇篮——哥丁根(Göttingen)接替了高斯之后,致力于研究算术级数中的素数问题.他证明了:如果a和b是互素的自然数,则在算术级数a,$a+b,a+2b,\cdots,a+nb,\cdots$中必然存在无穷多个素数(而自然数中有无穷多个素数是由欧几里得在公元前3世纪就证明了的).为了证明这个定理,狄利克雷精心设计了一种函数$L(s,\chi)$(L-函数).狄利克雷的重大贡献是把$\zeta(s)$和$L(s,\chi)$均看成是复变函数,并且认识到这些复变函数的解析特性与素数的分布有极为密切的关系.在这种认识的指导下,伟大的德国数学家黎曼(Riemann,1826—1866)深入地研究了$\zeta(s)$的解析性质,他证明了$\zeta(s)$满足一个函数方程,并由此将$\zeta(s)$解析延拓到整个复平面上,发现$\zeta(s)$只有一个奇点$s=1$,并且是留数为1的单极点.至于$\zeta(s)$的零点,他证明了:除了$s=-2,-4,-6,\cdots$是$\zeta(s)$的(平凡的单重)零点之外,其余零点均在带状区域$\{s=\sigma+it\mid 0<\sigma<1\}$之中.从函数方程的对称性,他猜想$\zeta(s)$的非平凡零点均在直线$s=\frac{1}{2}+it$$(-\infty<t<+\infty)$之上.这就是至今未能解决的黎曼猜想,而$\zeta(s)$也从此被人们称之为Riemann zeta函数.1896年,法国分析学家阿达玛(Hadamard)和dela Vallée Poussin利用在法国成长起来的很深刻的复变函数理论,证明了素数定理,即

$$\lim_{x\to\infty}\frac{\pi(x)}{x/\log x}=1$$

其中$\pi(x)$表示不超过x的素数个数,$\log x$表示自然对数.将同样的解析工具用于L函数,对于算术级数中的素数分布也得到类似的结果,而解析数论也从

此蓬勃地发展起来.

最早将这套解析机制运用到代数数域上的是戴德金. 对于每个代数数域 K,他构作了一个复变函数 $\zeta_K(s)$. 沿袭上述关于 $\zeta(s)$ 和 $L(s,\chi)$ 的解析成果,Hecke 和 Landau 对于 $\zeta_K(s)$ 的解析性质做了平行性的研究(函数方程,解析延拓,奇点和零点,广义黎曼猜想和素理想定理). 沿着这条路线发展的还有俄国数学家 Чебомалёв 的工作(密度定理). 但更重要的是,他们发现了 $\zeta_K(s)$ 在单极点 $s=1$ 处的留数值反映了代数数域 K 本身相当深刻的数论特性:这个留数值几乎与数域 K 的全部数论特性发生了本质性的联系! 20 世纪 20 年代至50 年代,德国数学家哈塞(Hasse,1898—1981)利用这些解析工具研究阿贝尔数域. 他在 1952 年所写的《关于阿贝尔域的类数》(Uber die Klassenzabl Abelscher Zahlkörper)一书中总结了他本人在这方面的成果,给出阿贝尔域的类数解析公式,并且对类数问题做了极为详尽的剖析. 哈塞的学生 Leopoldt 继承和发展了这方面的工作.

20 世纪下半叶,代数数论不断有重大的发展和突破. 我们可以例举:岩泽健吉(Iwasawa)从 50 年代末期创建的分圆域的全新理论;威尔(A. Weil)关于代数数论和代数几何算术性质的统一理论(集中体现在他于 1974 年所写的《Basic Number Theory》一书中);志村五郎(Shimura)等人关于代数数论与自守函数的联系(数域的非阿贝尔扩张理论),以及由 Selberg 所创建而近年来由美国数学家 Langlands 等人所发展的将代数数论与无限群表示论和调和分析相结合的杰出工作. 这些工作将代数数论与近代数学的许多学科交织在一起,形成现代数学最为活跃的领域之一. 与此同时,代数数论也愈来愈深入地运用到计算机科学、信息科学等应用学科当中(例如,人们普遍认为代数数论和置换群论是代数编码理论的两大支柱).

以上我们远远未能描绘出代数数论发展的全部图景. 但是从这种粗线条的勾画中,可以体察到代数数论有着光辉的历史和广阔的前景. 历史上很少有这样的科学分支,有如此众多的杰出数学家为它献身,体现了如此丰富的数学思想. 这使得代数数论既成熟而又年轻充满活力. 它是近代代数学的重要发源地(库默尔的"理想数"产生了"理想"这一概念,戴德金研究代数整数不可避免地引进了"模"的概念,……),它为现代代数学提供了丰富的背景性材料和促进因素(motivation).

在本书中,我试图向大家展现从高斯到哈塞的这段故事,叙述代数数论的最基本内容. 本书共分两大部分. 第一部分是代数理论,介绍代数数论中的代数结果和方法,包括代数数域的整数环、单位群、理想的素因子分解和分歧理论,理想类群和类数. 最后给出 Kronecker - Weber 定理(每个阿贝尔数域均是分圆域的子域)的一个证明和库默尔关于费马问题结果(第一种情形)的证明. 第二

部分是解析理论，我们首先精练地介绍解析数论的思想和方法，采用青年数论学家 D. Zagier 于 1982 年在中国介绍的方法给出素数定理一个极为简单的证明（并且说明这种方法也可以证明算术级数中的素数定理和素理想定理）. 然后叙述代数数论中的解析理论：密度定理、哈塞的类数解析公式和库默尔关于分圆域类数的一系列结果. 在整本书中，正像它的历史所展示的那样，我们把二次域和分圆域作为最典型的两类数域进行较为详尽的剖析.

这本书的前身是作者于 1981～1982 年度在中国科学技术大学为数学系四年级学生所开专业课的讲义. 1983～1984 年张贤科又为代数数论研究生讲过. 这次出版时，为了使内容更加精练，略去了局部域的理论和高斯二元二次型理论以及二次域的种（genus）理论等. 每节中均有一些例题和习题，每章中都介绍一些研究课题和近年来的发展情况. 阅读本书需要抽象代数中关于群、环、域的基本知识和代数技巧（或许后者更重要一些），为了使本书不至于太厚，我们假定读者了解这方面的内容而略去不讲. 作为一种补救的办法，在书的末尾（附录 B）极为扼要地介绍了关于群、环、域的部分概念和结果.

作者在写作过程中自始至终受到北京大学丁石孙教授和聂灵沼教授的关心和鼓励，对于本书的纲要和内容的取舍他们提供了很好的意见. 在与他们多次数学性的交谈和半数学性的聊天中，作者都得到很大的教益. 张贤科同志对本书也提出许多中肯的意见. 在这本书出版之后，本人愿意聆听更多人的批评、指教、意见和建议.

最后，我愿借此对我的数论启蒙老师华罗庚教授、王元教授和吴方教授表示深切的谢意.

冯克勤

2015 年 2 月 2 日

目 录

第一部分　代数理论

第二部分 解析理论

第一部分　代数理论

代数数域和代数整数环

第 1 章

1.1 代数数域

有理数域 $\mathbf{Q}$ 的有限(次)扩域 K 叫作代数数域,简称数域. 这是代数数论的基本研究对象. 如果扩张次数 $[K:\mathbf{Q}]$ 是 n,则 K 也叫作 n 次(数)域. 由于有限扩张必然是代数扩张,所以数域 K 中每个元素均是 $\mathbf{Q}$ 上的代数元素. 根据代数基本定理(附录 B,(18)),复数域 $\mathbf{C}$ 是 $\mathbf{Q}$ 的代数封闭扩域. 从而数域 K 中每个元素均可看成是复数,而每个数域 K 均可看成是 $\mathbf{C}$ 的子域. 如果 $K\subseteq\mathbf{R}$($\mathbf{R}$ 表示实数域),则称 K 为实域,否则称 K 为虚域. 元素 $\alpha\in\mathbf{C}$ 如果是 $\mathbf{Q}$ 上的代数元素(即存在 $f(x)\in\mathbf{Q}[x]$, $\deg f(x)\geqslant 1$,使得 $f(\alpha)=0$),我们称 α 为代数数,否则便叫作超越数. 所有代数数全体构成域 Ω,叫作 $\mathbf{Q}$ 的代数闭包. 事实上每个数域均是 Ω 的子域,而 $\mathbf{C}$ 是大于 Ω 的. 换句话说,超越数是存在的. 例如,可以证明 π 和 e 均是超越数,并且超越数比代数数还要多(习题 1).

关于域的代数扩张的一般事实请参见附录 B,3. 在这一节里,我们就数域的情形再做一些补充.

1.1.1 单扩张定理

设 L/K 是数域的扩张(即 L 和 K 均是数域,并且 $K\subseteq L$). 由于扩张 $L/\mathbf{Q}$ 和 $K/\mathbf{Q}$ 均是有限的,从而 L/K 也是有限扩张.

令扩张次数为$[L:K]=n$,而$\omega_1,\cdots,\omega_n$是向量空间L的一组K-基,则L中每个元素均可唯一地写为

$$k_1\omega_1+\cdots+k_n\omega_n \quad (k_i\in K)$$

特别地,有$L=K(\omega_1,\omega_2,\cdots,\omega_n)$,即$L/K$是有限生成扩张. 我们现在要进一步证明:

定理1 每个数域扩张L/K均是单扩张. 即存在$\gamma\in L$,使得$L=K(\gamma)$.

证明 我们只要对$L=K(\alpha,\beta)$的情形证明定理即可,因为一般情形$L=K(\omega_1,\cdots,\omega_n)$可由此对$n$归纳证得. 现设$L=K(\alpha,\beta)$. 令$f(x),g(x)\in K[x]$分别是元素$\alpha$和$\beta$在$K$上的极小多项式,它们在$\mathbf{C}[x]$中分解为

$$f(x)=\prod_{i=1}^{n}(x-\alpha_i),g(x)=\prod_{j=1}^{m}(x-\beta_j) \quad (\alpha_i,\beta_j\in\mathbf{C})$$

其中,$n=\deg f,m=\deg g$. 不妨设$\alpha=\alpha_1,\beta=\beta_1$. 由于$f(x)$和$g(x)$均是$K[x]$中不可约多项式,从而它们均无重根. 即$\alpha_i(1\leqslant i\leqslant n)$两两相异,而$\beta_j(1\leqslant j\leqslant m)$也两两相异. 现在于有限集合

$$\{(\alpha_i-\alpha_j)/(\beta_k-\beta_l)\mid 1\leqslant k\neq l\leqslant m,1\leqslant i\leqslant j\leqslant n\}$$

之外取一个有理数c,不难看出mn个复数$\alpha_i+c\beta_j$两两相异. 令$\gamma=\alpha_1+c\beta_1=\alpha+c\beta$. 则多项式$h(x)=f(\gamma-cx)$属于$K(\gamma)[x]$,$h(\beta_1)=0$,而$\beta_2,\cdots,\beta_m$均不为$h(x)$的根. 于是在$\mathbf{C}[x]$中$(h(x),g(x))=x-\beta_1$. 注意域上两个多项式的最大公因子可以用辗转相除法求得,而这个过程在$K(\gamma)[x]$中和$\mathbf{C}[x]$中都是一样的,因此在$K(\gamma)[x]$中也有$(h(x),g(x))=x-\beta_1$. 特别地,$x-\beta_1\in K(\gamma)[x]$,这就表明$\beta=\beta_1\in K(\gamma)$,于是$\alpha=\gamma-c\beta\in K(\gamma)$,从而$K(\alpha,\beta)\subseteq K(\gamma)$. 另一方面,由于$\gamma=\alpha+c\beta,c\in K$,从而$K(\gamma)\subseteq K(\alpha,\beta)$显然成立. 这就证明了$K(\alpha,\beta)=K(\gamma)$,从而也证明了定理1.

1.1.2 数域的嵌入

设L/K是数域的扩张. 正如附录B,3中所述,每个域的单同态$\sigma:L\to\mathbf{C}$均叫作L在$\mathbf{C}$中的一个嵌入. 如果σ在K上的限制$\sigma|_K$是域K上的恒等自同构(即对每个$k\in K$均有$\sigma(k)=k$),则称σ是K-嵌入. 利用上面的单扩张定理我们可以证明:L恰好有$[L:K]$个K-嵌入. 事实上,我们可以证明下面更为一般的结论:

定理2 设L/K是数域的扩张.$[L:K]=n$. 则每个嵌入$\sigma:K\to\mathbf{C}$均可以n种不同的方法扩充到L上. 换句话说,恰好存在n个不同的嵌入$\tau_i:L\to\mathbf{C}$$(1\leqslant i\leqslant n)$,使得$\tau_i|_K=\sigma$.

证明 由单扩张定理我们可以令$L=K(\gamma)$. 令$f(x)=c_0+c_1+\cdots+c_{n-1}x^{n-1}+x^n\in K[x]$是$\gamma$在$K$上的极小多项式,则$\deg f=n$,而$L$中元素均可唯

一地表示成

$$\alpha = k_0 + k_1\gamma + \cdots + k_{n-1}\gamma^{n-1} \quad (k_i \in K)$$

(附录 B,(12)及其注记)

设$\tau: L \to \mathbf{C}$是一个嵌入并且$\tau|_K = \sigma$,则

$$\tau(\alpha) = \sigma(k_0) + \sigma(k_1)\tau(\gamma) + \cdots + \sigma(k_{n-1})\tau(\gamma)^{n-1}$$

从而τ由它在γ上的值所完全决定. 考虑多项式

$$\sigma f(x) = \sigma(c_0) + \sigma(c_1)x + \cdots + \sigma(c_{n-1})x^{n-1} + x^n \in \sigma(K)[x]$$

由于$\sigma: K \to \sigma(K)$是域的同构,不难看出σf是$\sigma(K)[x]$中的n次不可约多项式,从而它有n个不同的复根$\rho_1, \cdots, \rho_n$. 由于

$$\sigma f(\tau(\gamma)) = \sigma(c_0) + \sigma(c_1)\tau(\gamma) + \cdots + \sigma(c_{n-1})\tau(\gamma)^{n-1} + \tau(\gamma)^n = \tau(f(\gamma)) = 0$$

这就表明$\tau(\gamma)$必为某个ρ_i. 从而σ到L上的扩充至多有n个. 现在对每个$i(1 \leqslant i \leqslant n)$,作映射

$$\tau_i: L \to \mathbf{C}, \tau_i(k_0 + k_1\gamma + \cdots + k_{n-1}\gamma^{n-1}) = \sigma(k_0) + \sigma(k_1)\rho_i + \cdots + \sigma(k_{n-1})\rho_i^{n-1}$$

易验证这是域的同态. 设$k_0 + k_1\gamma + \cdots + k_{n-1}\gamma^{n-1} \in \operatorname{Ker}\tau_i$(同态$\tau_i$的核),则$\sigma(k_0) + \sigma(k_1)\rho_i + \cdots + \sigma(k_{n-1})\rho_i^{n-1} = 0$,从而

$$\sigma f(x) \mid \sigma(k_0) + \sigma(k_1)x + \cdots + \sigma(k_{n-1})x^{n-1}$$

于是$f(x) \mid k_0 + k_1 x + \cdots + k_{n-1}x^{n-1}$(为什么). 但是$f(x)$为$K[x]$中$n$次不可约多项式,所以只能是$k_0 = k_1 = \cdots = k_{n-1} = 0$. 这就表明$\operatorname{Ker}\tau_i = (0)$,即$\tau_i$是嵌入. 又显然$\tau_i|_k = \sigma$并且$\tau_i(\gamma) = \rho_i$. 而$\rho_i(1 \leqslant i \leqslant n)$是两两相异的,从而$\tau_i(1 \leqslant i \leqslant n)$是$\sigma$到$L$上的$n$个不同的扩充. 这就证明了定理2.

在定理2中特别取σ为域K的恒等自同构,我们就得到:

系1 每个数域扩张L/K均恰好有$[L:K]$个从L到$\mathbf{C}$的K-嵌入.

设$L = K(\gamma)$, $f(x) \in K[x]$是γ在K上的极小多项式. $\deg f = n = [L:K]$. 令$\gamma_i(1 \leqslant i \leqslant n)$是$f$的$n$个不同的根(其中有一个为$\gamma$),它们即是$\gamma$的全部$K$-共轭元素(附录B,3). 根据定理2的证明,可知$\tau_i: L = K(\gamma) \xrightarrow{\sim} K(\gamma_i) \subseteq \mathbf{C}, \tau_i(\gamma) = \gamma_i(1 \leqslant i \leqslant n)$就是$L$的全部$n$个嵌入,从而$K(\gamma_i)(1 \leqslant i \leqslant n)$(它们不必不同)就是$L$的全部$K$-共轭域. 当$K(\gamma_i) = L(1 \leqslant i \leqslant n)$即$L$为$K$-自共轭域的时候,$L/K$即为伽罗瓦扩张(或者叫正规扩张). 这也等价于说:$\gamma_i \in L(1 \leqslant i \leqslant n)$. 这时,每个$K$-嵌入$\tau_i: L \to \mathbf{C}$均是域$L$的$K$-自同构. 从而伽罗瓦群$\operatorname{Gal}(L/K) = \{\tau_1, \tau_2, \cdots, \tau_n\}$. 而对于一般的情形,由于$K(\gamma_1, \gamma_2, \cdots, \gamma_n)$是$f(x)$在$K$上的分裂域,从而$K(\gamma_1, \cdots, \gamma_n)/K$是伽罗瓦扩张(附录B,3,(15)). 并且不难看出$K(\gamma_1, \gamma_2, \cdots, \gamma_n)$是$K$的包含$L$的最小伽罗瓦扩张,称$K(\gamma_1, \cdots, \gamma_n)$为扩张$L/K$的正规闭包.

如果$K = \mathbf{Q}$,即L是$n = [L:\mathbf{Q}]$次数域,$L = \mathbf{Q}(\gamma)$. 令$f(x) \in \mathbf{Q}[x]$是γ在$\mathbf{Q}$

上的极小多项式，则存在恰好 n 个域的嵌入 $\tau_i: L=\mathbf{Q}(\gamma)\xrightarrow{\sim}\mathbf{Q}(\gamma_i)\subseteq\mathbf{C}$，使得 $\tau_i(\gamma)=\gamma_i(1\leqslant i\leqslant n)$，其中 $\gamma_i(1\leqslant i\leqslant n)$ 是 $f(x)$ 的 n 个不同的根（注意：数域的嵌入必为 $\mathbf{Q}$ - 嵌入）. 不妨设前 r_1 个是实根而后 r_2 对是虚根，即

$$\gamma_i\in\mathbf{R}\quad(1\leqslant i\leqslant r_1)$$

$$\gamma_{r_1+j}=\overline{\gamma}_{r_1+r_2+j}\notin\mathbf{R}\quad(1\leqslant j\leqslant r_2, r_1+2r_2=n)$$

于是 L 的前 r_1 个共轭域 $\mathbf{Q}(\gamma_i)$ 为实域，我们称这 r_1 个嵌入 $\tau_i: L=\mathbf{Q}(\gamma)\xrightarrow{\sim}\mathbf{Q}(\gamma_i)\subseteq\mathbf{R}$ 为实嵌入. 而后 r_2 对共轭域为虚域，并且 $\mathbf{Q}(\gamma_{r_1+j})=\mathbf{Q}(\gamma_{r_1+r_2+j})\subsetneq\mathbf{R}(1\leqslant j\leqslant r_2)$，称这 r_2 对嵌入 $\tau_i(r_1+1\leqslant i\leqslant n)$ 为复嵌入，并且称 τ_{r_1+j} 和 $\tau_{r_1+r_2+j}$ 是彼此共轭的嵌入，记为 $\overline{\tau}_{r_1+j}=\tau_{r_1+r_2+j}(1\leqslant j\leqslant r_2)$.

例 1　每个二次（数）域均可唯一地表示成 $\mathbf{Q}(\sqrt{d})$，其中 d 为无平方因子整数（习题 2）. 当 $d>0$ 时这是实域，称作是实二次域. 而当 $d<0$ 时 $\mathbf{Q}(\sqrt{d})$ 是虚域，称作是虚二次域. 由于 $\mathbf{Q}(\sqrt{d})/\mathbf{Q}$ 必然是伽罗瓦扩张，可知对于实二次域 $r_1=2, r_2=0$，而对于虚二次域 $r_1=0, r_2=1$. $\mathbf{Q}(\sqrt{d})/\mathbf{Q}$ 的伽罗瓦群为 $G=\{I,\sigma\}$，其中 I 表示恒等自同构，而 $\sigma(a+b\sqrt{d})=a-b\sqrt{d}(a,b\in\mathbf{Q})$，即将 $\mathbf{Q}(\sqrt{d})$ 中每个元素 $a+b\sqrt{d}$ 映成它的共轭元素 $a-b\sqrt{d}$. 有时也将 σ 称作是二次域 $\mathbf{Q}(\sqrt{d})$ 的共轭自同构.

例 2　分圆域 $\mathbf{Q}(\zeta_{p^n})$，其中 $\zeta_{p^n}=\mathrm{e}^{2\pi i/p^n}$ 是 p^n 次本原单位根，而 p 为素数，$n\geqslant 1$. 以下简记 $\zeta=\zeta_{p^n}$. 易知 ζ 是多项式

$$\begin{aligned}f(x)&=x^{(p-1)p^{n-1}}+x^{(p-2)p^{n-1}}+\cdots+x^{p^{n-1}}+1\\&=\frac{x^{p^n}-1}{x^{p^{n-1}}-1}\in\mathbf{Z}[x]\end{aligned}$$

的根. 我们现在证明 $f(x)$ 是 $\mathbf{Q}[x]$ 中的不可约多项式. 为此令

$$g(x)=f(x+1)=x^{(p-1)p^{n-1}}+c_{p^n-p^{n-1}-1}x^{p^n-p^{n-1}-1}+\cdots+c_1x+c_0\in\mathbf{Z}[x]$$

由于

$$g(x)=\frac{(x+1)^{p^n}-1}{(x+1)^{p^{n-1}}-1}\equiv\frac{x^{p^n}}{x^{p^{n-1}}}=x^{p^n-p^{n-1}}\pmod p$$

从而 $p\mid c_i(0\leqslant i\leqslant p^n-p^{n-1}-1)$. 进而 $c_0=g(0)=f(1)=p$，于是 $p^2\nmid c_0$. 所以由 Eisenstein 判别准则（附录 B，(7)）可知 $g(x)$ 是 $\mathbf{Q}[x]$ 中不可约多项式，从而 $f(x)$ 也是如此. 这就表明 $f(x)$ 是 ζ 在 $\mathbf{Q}$ 上的极小多项式，并且 $[\mathbf{Q}(\zeta_{p^n}):\mathbf{Q}]=\deg f=p^n-p^{n-1}$. ζ 的全部共轭元素（即 $f(x)$ 的全部根）显然是 $\zeta^i(1\leqslant i\leqslant p^n, p\nmid i)$（即为 $x^{p^n}-1$ 之根但不为 $x^{p^{n-1}}-1$ 之根者），它们均属于 $\mathbf{Q}(\zeta)$，从而 $\mathbf{Q}(\zeta)/\mathbf{Q}$ 是伽罗瓦扩张. 令 $\sigma_i\in\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$，使得 $\sigma_i(\zeta)=\zeta^i(1\leqslant i\leqslant p^n-1, p\nmid i)$，则

$$\sigma_i\cdot\sigma_j(\zeta)=\sigma_i(\zeta^j)=\sigma_i(\zeta)^j=\zeta^{ij}=\sigma_{ij}(\zeta)$$