中国数论名家著作选系列

"十三五"国家重点图书

Algebraic Number Theory

代数数论

冯克勤 编著

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

中国数论名家著作选系列

"十三五"国家重点图书

代数数论

Algebraic Number Theory

冯克勤 编著

由黑龙江省精品图书出版工程专项资金资助出版

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

内 容 简 介

代数数论是研究代数数域和代数整数的一门学问. 本书的主要内容是经典代数数论,全书共分三部分:第一、二部分为代数理论和解析理论,全面介绍了19世纪代数数论的成就;第三部分为局部域理论,简要介绍了20世纪代数数论的一些内容. 附录中给出了本书用到的近世代数的基本知识和进一步学习代数数论的建议,每节末附有习题.

本书的读者对象是大学数学系教师和高年级学生,也可作为研究生教材使用.

图书在版编目(CIP)数据

代数数论/冯克勤编著. —哈尔滨:哈尔滨工业大学出版社,2018.5

ISBN 978-7-5603-6429-2

Ⅰ.①代… Ⅱ.①冯… Ⅲ.①代数数论 Ⅳ.①O156.2

中国版本图书馆 CIP 数据核字(2017)第005775号

策划编辑 刘培杰 张永芹
责任编辑 张永芹 李宏艳
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 哈尔滨市工大节能印刷厂
开 本 787mm×1092mm 1/16 印张23.75 字数454千字
版 次 2018年1月第5版 2018年1月第5次印刷
书 号 ISBN 978-7-5603-6429-2
定 价 68.00元

前言

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,用代数工具来研究数论问题.

数(shù)起源于数(shǔ).数论是历史最悠久的一个数学分支.在有文字历史之前,由于生产和生活实践的需要,用石子、树枝或结绳、刻痕来计数,人类就有了整数概念.在东方各文明古国,伴随文字的产生而创造了形式各异的数字和记数法(包括沿用至今的十进制记数法).数论的历史大约有 3 000 年.初等数论的主要课题是研究整数的性质和方程(组)的整数解,它也起源于古代的东方.中国最早的数学名著《周髀算经》的开篇就记载了西周人商高知道方程 $x^2+y^2=z^2$ 有整数解 $(x,y,z)=(3,4,5)$.另一部数学名著《孙子算经》(公元 4—5 世纪)载有"物不知数"问题,研究整数的同余性质,被世人称为"中国剩余定理".

东方古国的数论主要基于计算实践,具有鲜明的直观、实用和算法特性.而在古希腊数学(公元前 6 世纪—公元 3 世纪)中,整数作为认识世界的最基本手段和工具,数论具有崇高的位置.毕达哥拉斯(公元前 572—前 497)学派的名言为"万物皆数".古希腊的数学充满理性思辨的特征.欧几里得(公元前 330—前 275 年)的名著《几何原本》共 13 卷,其中有 3 卷讲述数论,书中讲述了初等数论的基石:算术基本定理(每个大于 1 的整数均可唯一地表示成有限个素数的乘积),证明了素数有无限多个(这可能是数论中第一个无限性的证明),得到了方程 $x^2+y^2=z^2$ 全部(无限多个)整数解的表达公式.古希腊的另一重要数论著作是丢番图(Diophantus)的《算术》(公元 3 世纪).书中研究了三百多个数论问题,列举了寻求一次和二次方程(组)有理数解和整数解的各种方法.这是世上

第一本脱离开几何而独立研究数论的著作. 对数论后来的发展具有特殊的意义.

人类文明逐渐转到欧洲. 在欧洲文艺复兴时代(公元 15 和 16 世纪),数学也得到复兴和发展. 但主要是基于天文、航海、建筑和绘画等需要的画法几何学,数论的进展不大. 17 和 18 世纪的数论中心在法国. 当时的大数论学家勒让德、拉格朗日、拉普拉斯、费马等都是法国人,唯一的例外是欧拉. 丢番图的《算术》一书于 1621 年被译成拉丁文. 1637 年,费马(Fermat,1601—1665)在阅读此书中讨论方程 $x^2+y^2=z^2$ 的那一页的空白处写了一个评注. 他认为对每个整数 $n\geqslant 3$,方程 $x^n+y^n=z^n$ 都没有正整数解. 他声称给出了这一猜想的一个巧妙的证明,但是空白处太小写不下. 自那以后,人们只看到费马对 $n=4$ 的情形给出的证明. 费马提出了许多数论猜想,这些猜想引起了欧拉对数论的兴趣. 经过多年的努力,欧拉(Euler,1707—1783)(肯定或否定地)解决了费马提出的诸多猜想,只剩下唯一的上述费马猜想,一直到 1994 年才由怀尔斯(Andrew Wiles,1953—)所证明.

19 世纪,数论得到重大的进步. 其主要标志是深刻的解析方法和代数工具引入数论当中,产生了数论的两个新的分支:解析数论和代数数论. 解析数论的创始人为德国数学家黎曼(Riemann,1826—1866),代数数论的奠基者为德国数学家高斯(Gauss,1777—1855)和库默尔(Kummer,1810—1893),世界数论中心也由法国转到德国.

代数数论至今整整有 200 年的历史. 1801 年高斯出版了著作《算术探究》(*Disquisitiones Arithmeticae*),深入地研究了二元二次型 $ax^2+bxy+cy^2=n$ 的整数解问题(其中 a,b,c,n 均为整数). 以方程 $x^2+y^2=n$ 为例,它把此方程写成 $n=(x+\mathrm{i}y)(x-\mathrm{i}y)$,其中 $\mathrm{i}=\sqrt{-1}$. 高斯研究形如 $a+\mathrm{i}b$ 的数(其中 a 和 b 是整数),这种数现在称为高斯整数. 高斯整数所成的集合 $\mathbb{Z}[\mathrm{i}]$ 中可以进行加减乘运算,这是一个交换环,叫高斯整数环. 于是,正整数 n 可以表示成两个整数的平方和当且仅当 n 可以表示成两个高斯整数的乘积. 高斯证明了环 $\mathbb{Z}[\mathrm{i}]$ 中具有与通常整数环 $\mathbb{Z}$ 类似的唯一因子分解性质,由此完全解决了方程 $x^2+y^2=n$ 的整数解问题,即完全解决了哪些正整数 n 可以是两个整数的平方和,并且给出方程 $x^2+y^2=n$ 的整数解个数的计算公式. 对于一般的二元二次型 $ax^2+bxy+cy^2=n$,需要研究环 $\mathbb{Z}[\sqrt{d}]$,其中 $d=4ac-b^2$. 他发现这些环当中有许多不具有唯一因子分解性质,从而使问题变得复杂. 高斯研究这些环和对应的二次域 $\mathbb{Q}(\sqrt{d})$ 的深刻性质,引入了一系列重要数学概念(理想类数、genus 理论、基本单位等),开创了二次域的理论研究.

1847 年,库默尔用同样的想法研究费马猜想. 对每个奇素数 p,他把费马方程分解成

$$z^p = x^p + y^p = (x+y)(x+\zeta_p y)\cdots(x+\zeta_p^{p-1}y)$$

其中 $\zeta_p = e^{\frac{2\pi i}{p}}$. 于是考虑比整数环$\mathbb{Z}$更大的环$\mathbb{Z}[\zeta_p]$. 如果这个环具有唯一因子分解性质,库默尔证明了方程 $x^p + y^p = z^p$ 没有正整数解,即费马猜想对 $n = p$ 成立. 他证明了当 $p \leqslant 19$ 时,$\mathbb{Z}[\zeta_p]$具有唯一因子分解性质,从而用统一方法证明了费马猜想对 n 为不超过 22 的所有正整数($n \geqslant 3$)都是对的. 他也证明了$\mathbb{Z}[\zeta_{23}]$不具有唯一因子分解性质. 进而,他提出了"理想数"的概念,证明了:即使$\mathbb{Z}[\zeta_p]$不具有唯一因子分解性质(即$\mathbb{Z}[\zeta_p]$的理想类数 h_p 大于 1),但只要 h_p 不被 p 除尽,则方程 $x^p + y^p = z^p$ 也没有正整数解. 他还给出判别 p 是否除尽 h_p 的初等方法(详见本书第六章),由此证明了对于 100 以内的所有奇素数 p,除了 37,59,67 之外,费马猜想对于 $n = p$ 均正确. 库默尔研究了环$\mathbb{Z}[\zeta_p]$的一系列深刻的性质(理想类数、分圆单位、理想数等),开创了对分圆域的理论研究.

高斯和库默尔分别对于二次域和分圆域所做的深刻研究,成为用深刻代数工具研究数论问题的奠基性工作,由此产生了代数数论. 这门学问后来由德国数学家戴德金(Dedekind,1831—1916)和狄利克雷(Dirichlet,1805—1859)在理论上加以完善(例如:库默尔的"理想数"就是现今环论中的理想概念). 到了 1898 年,德国大数学家希尔伯特(Hilbert,1862—1943)在《数论报告》(*Zahlebericht*)中对于各种代数数域的性质加以系统总结和发展,经过整整 100 年,经典的代数数论由此定型.

解析数论的源头可以上溯到欧拉,1737 年,欧拉在研究无穷级数和无穷乘积的收敛性时,发现对于大于 1 的实数 s,有等式

$$\begin{aligned} &1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots + \frac{1}{n^s} + \cdots \\ &= \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots + \frac{1}{p^{ms}} + \cdots\right) \\ &= \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \end{aligned}$$

其中无穷乘积中 p 过所有素数,事实上,这个等式等价于算术基本定理,这就把数论和解析公式联系在一起. 取 $s = 1$,由于上式左边是发散的(即值为 $+\infty$),可知右边的素数有无限多个. 这是由解析特性推出数论结果的最简单例子. 沿用这种方法,狄利克雷构作了一批新的函数 $L(s,\chi)$(叫作 L - 函数),从它们的解析特性得到了不平凡的结果:若 l 和 k 是互素的正整数,则算术级数 $l, l+k, l+2k, \cdots$中一定有无限多个素数. 1859 年,黎曼把函数 $\zeta(s) = \sum_{n \geqslant 1} n^{-s}$看成复变量 $s = \sigma + it$(σ, t 为实数)的函数. 这个级数只在 $\sigma > 1$ 时收敛,但是他把此级数解析开拓成整个复平面上的亚纯函数,并且满足函数方程 $\zeta(s) = f(s)\zeta(1-s)$,其中 $f(s)$ 是一个熟知的复变函数(见本书第五章). 黎曼猜想 $\zeta(s)$ 的所有非

平凡零点的实数部分都是$\frac{1}{2}$,这就是至今未解决的黎曼猜想. 这个猜想对于研究素数的分布和许多数论问题都是重要的,这就开创了研究数论的解析方法. $\zeta(s)$也由此被后人称作黎曼 zeta 函数.

代数数论中也可采用解析方法. 对每个代数数域 K,戴德金构作了一个 zeta 函数 $\zeta_K(s)$. 当 s 的实数部分大于 1 时定义它的级数收敛并且有无穷乘积展开,它也可解析开拓成整个复平面上的亚纯函数,并且有函数方程把 $\zeta_K(s)$和 $\zeta_K(1-s)$联系起来. $\zeta_K(s)$的各种解析特性可以反映代数数域 K 和它的整数环 O_K 的代数和数论性质,所以解析方法也是代数数论的重要研究手段.

本书的主要内容是介绍经典代数数论,即 19 世纪代数数论的成就. 本书的前身是 1988 年出版的《代数数论入门》一书(上海科学技术出版社),经过十多年的讲授,这次把原书内容做了删节,改正了一些错误之处. 在原书两大部分(代数理论和解析理论)的基础上,增加了第三部分:局部域理论,介绍局部数域的基本结果,还介绍了代数数域的某些应用. 换句话说,我们增加了 20 世纪代数数论的一些内容. 最后,在结语中扼要介绍了 20 世纪代数数论的发展轮廓,希望读者对于近代和现代数论的情况有一些基本的了解.

本书的预备知识是初等数论和近世代数的基本知识和代数技巧. 附录 A 扼要地介绍了本书用到的近世代数中的一些基本概念和主要结果. 附录 B 对今后进一步深造代数数论提供一些参考性建议.

十多年来,有许多同事和学生对原书提出许多宝贵的意见,这里一并表示感谢. 作者也感谢"中国科学院研究生教材基金"对本书的出版所给予的资助,并且也欢迎读者的意见和建议,以便把书改得更好.

冯克勤

目录

第一部分 代数理论

第二部分 解析理论

第三部分　局部域理论

第一部分

代数理论

代数数域和代数整数环

第一章

§1 代数数域

有理数域$\mathbb{Q}$的有限(次)扩域K叫作**代数数域**,简称作**数域**,这是代数数论的基本研究对象. 如果扩张次数$[K:\mathbb{Q}]$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$\mathbb{Q}$上的代数元素. 根据代数基本定理(附录A,(18)),复数域$\mathbb{C}$是$\mathbb{Q}$的代数封闭扩域,从而数域K中每个元素均可看成复数,而每个数域K均可看成$\mathbb{C}$的子域. 如果$K\subseteq\mathbb{R}$($\mathbb{R}$表示实数域),则称K为**实域**,否则称K为**虚域**. 元素$\alpha\in\mathbb{C}$,如果是$\mathbb{Q}$上的代数元素(即存在$f(x)\in\mathbb{Q}[x]$,$\deg f(x)\geqslant 1$,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$\mathbb{Q}$的**代数闭包**. 事实上每个数域均是Ω的子域,而$\mathbb{C}$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A,Ⅲ. 在这一节里,我们就数域的情形再做一些补充.

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$L/\mathbb{Q}$和$K/\mathbb{Q}$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

$$k_1\omega_1+\cdots+k_n\omega_n\quad(k_i\in K,i=1,\cdots,n)$$

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 1.1 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 α 和 β 在 K 上的极小多项式,它们在 $\mathbb{C}[x]$ 中分解为

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

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

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

之外取一个非零有理数 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 $\mathbb{C}[x]$ 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 $\mathbb{C}[x]$ 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 A,Ⅲ中所述,每个域的单同态 $\sigma:L\to\mathbb{C}$ 均叫作 L 在 $\mathbb{C}$ 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 1.2 设 L/K 是数域的扩张,$[L:K]=n$,则每个嵌入 $\sigma:K\to\mathbb{C}$ 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 $\tau_i:L\to\mathbb{C}(1\leqslant i\leqslant n)$,使得 $\tau_i|_K=\sigma$.

证明 由单扩张定理我们可以令 $L=K(\gamma)$. 命 $f(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}+x^n\in K[x]$ 是 γ 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

$$\alpha=k_0+k_1\gamma+\cdots+k_{n-1}\gamma^{n-1}\quad(k_i\in K,i=0,1,\cdots,n-1)$$

(附录 A,(12)及其注记). 设 $\tau:L\to\mathbb{C}$ 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$\tau$由它在$\gamma$上的值所完全决定. 考虑多项式

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

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

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

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$\tau_i:L\to\mathbb{C}$

$$\begin{aligned}&\tau_i(k_0+k_1\gamma+\cdots+k_{n-1}\gamma^{n-1})\\&=\sigma(k_0)+\sigma(k_1)\rho_i+\cdots+\sigma(k_{n-1})\rho_i^{n-1}\end{aligned}$$

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$f(x)\mid k_0+k_1x+\cdots+k_{n-1}x^{n-1}$(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1.2. □

在定理1.2中特别取σ为域K的恒等自同构,我们就得到:

系 设L/K为数域扩张,则从L到$\mathbb{C}$恰好有$[L:K]$个不同的K-嵌入.

注记 设$L=K(\gamma)$,$f(x)\in K[x]$是γ在K上的极小多项式,$\deg f=n=[L:K]$,则$f(x)$在$\mathbb{C}$中有n个不同的根$\gamma_i(1\leqslant i\leqslant n)$,其中有一个根$\gamma_1$为$\gamma$. 它们叫作$\gamma$的$K$-共轭元素(附录A,Ⅲ). 从定理1.2的证明可知映射

$$\tau_i:L=K(\gamma)\xrightarrow{\sim}K(\gamma_i),\tau_i(\gamma)=\gamma_i\quad(1\leqslant i\leqslant n)$$

就是L到$\mathbb{C}$中的全部n个K-嵌入. 这是n个不同的嵌入方式,因为元素γ的象$\gamma_i(1\leqslant i\leqslant n)$彼此不同,对于$i=1$,$K(\gamma_1)=L$并且$\tau_1$是恒等自同构,$n$个与$L$同构的域$K(\gamma_i)(1\leqslant i\leqslant n)$叫作$L$的$K$-共轭域,它们不必彼此不同,特别当这些域彼此相同,从而均为$L=K(\gamma_1)$的时候,也就是$\gamma_i\in L(1\leqslant i\leqslant n)$的时候,$\tau_i(1\leqslant i\leqslant n)$均是域$L$的$K$-自同构,这时称$L/K$为**伽罗瓦扩张**,而$\operatorname{Gal}(L/K)=\{\tau_1,\cdots,\tau_n\}$是$L/K$的伽罗瓦群,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A,Ⅲ(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 $K=\mathbb{Q}$,即 L 是 $n=[L:\mathbb{Q}]$ 次数域,$L=\mathbb{Q}(\gamma)$. 令 $f(x)\in\mathbb{Q}[x]$ 是 γ 在 $\mathbb{Q}$ 上的极小多项式,则存在恰好 n 个域的嵌入 $\tau_i: L=\mathbb{Q}(\gamma)\xrightarrow{\sim}\mathbb{Q}(\gamma_i)\subseteq\mathbb{C}$,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 $\mathbb{Q}$ - 嵌入!). 不妨设前 r_1 个是实根而后 r_2 对是虚根,即

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

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

于是 L 的前 r_1 个共轭域 $\mathbb{Q}(\gamma_i)$ 为实域,我们称这 r_1 个嵌入 $\tau_i: L=\mathbb{Q}(\gamma)\xrightarrow{\sim}\mathbb{Q}(\gamma_i)\subseteq\mathbb{R}$ 为**实嵌入**. 而后 r_2 对共轭域为虚域,并且 $\mathbb{Q}(\gamma_{r_1+j})=\mathbb{Q}(\gamma_{r_1+r_2+j})\not\subset\mathbb{R}(1\leqslant j\leqslant r_2)$. 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 $\overline{\tau}_{r_1+j}=\tau_{r_1+r_2+j}(1\leqslant j\leqslant r_2)$.

如果 L 中又有另一元素 γ',使得 $L=\mathbb{Q}(\gamma')$,则 γ' 在 $\mathbb{Q}$ 上的极小多项式 $f'(x)$ 的次数也是 $n=[L:\mathbb{Q}]$,并且 $f'(x)$ 的 n 个根也有 r_1 个实根和 r_2 对虚根. 这是由于嵌入 $\tau_1,\cdots,\tau_n$ 是域 L 本身的特性,与生成元 γ 的选取方式无关. 换句话说,参数 r_1 和 r_2 是数域 L 的不变量,$r_1+2r_2=n$(当然,扩张次数 $[L:\mathbb{Q}]=n$ 也是 L 的不变量).

例 1 每个二次(数)域均可唯一地表示成 $\mathbb{Q}(\sqrt{d})$,其中 d 是无平方因子整数(习题 2). 当 $d>0$ 时它是实域,叫作实二次域. 而当 $d<0$ 时叫作虚二次域. $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ 是伽罗瓦扩张,由于 $\sqrt{d}$ 的极小多项式为 $f(x)=x^2-d$,它的两个根是 $\pm\sqrt{d}$,所以伽罗瓦群 $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ 为 $\{I,\sigma\}$,其中 I 是恒等自同构,而 $\sigma(\sqrt{d})=-\sqrt{d}$. 由于域 $\mathbb{Q}(\sqrt{d})$ 中每个元素唯一地表示成 $a+b\sqrt{d}$,其中 $a,b\in\mathbb{Q}$,可知 $\sigma(a+b\sqrt{d})=a-b\sqrt{d}$. 不难看出,对于实二次域,$r_1=2,r_2=0$. 而对于虚二次域,$r_1=0,r_2=1$.

例 2 分圆域 $\mathbb{Q}(\zeta_{p^n})$,其中 $\zeta_{p^n}=\mathrm{e}^{2\pi\mathrm{i}/p^n}$ 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

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

的根,我们现在证明 $f(x)$ 是 $\mathbb{Q}[x]$ 中的不可约多项式. 为此令 $g(x)=f(x+1)=x^{(p-1)p^{n-1}}+c_{p^n-p^{n-1}-1}x^{p^n-p^{n-1}-1}+\cdots+c_1x+c_0\in\mathbb{Z}[x]$. 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 A,(7))可知 $g(x)$ 是 $\mathbb{Q}[x]$ 中不可约多项式,从而 $f(x)$ 也是如此. 这就表明 $f(x)$ 是 ζ 在 $\mathbb{Q}$ 上的极小多项式,并且 $[\mathbb{Q}(\zeta_{p^n}):\mathbb{Q}] = \deg f = p^n - p^{n-1}$. ζ 的全部共轭元素(即 $f(x)$ 的全部根)显然是 ζ^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 $\mathbb{Q}(\zeta)$,从而 $\mathbb{Q}(\zeta)/\mathbb{Q}$ 是伽罗瓦扩张. 令 $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$,使得 $\sigma_i(\zeta) = \zeta^i$ $(1 \leqslant i \leqslant p^n - 1, p \nmid i)$,则

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

这就表明 $\sigma_i \cdot \sigma_j = \sigma_{ij}$. 作映射

$$\chi: \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \to (\mathbb{Z}/p^n\mathbb{Z})^\times, \chi(\sigma_i) = \bar{i}$$

其中 $(\mathbb{Z}/p^n\mathbb{Z})^\times$ 表示环 $\mathbb{Z}/p^n\mathbb{Z}$ 的单位(乘法)群,而 $\bar{i}$ 表示剩余类 $i(\mathrm{mod}\ p^n)$. 由上述不难看出 χ 是群的同构. 但是当 $p \geqslant 3$ 时,从初等数论我们知道,乘法群 $(\mathbb{Z}/p^n\mathbb{Z})^\times$ 是由模 p^n 的某个原根 g 生成的 $p^n - p^{n-1}$ 阶循环群. 从而伽罗瓦群 $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$ 当 $p \geqslant 3$ 时,是 $p^n - p^{n-1}$ 阶循环群,生成元为 σ_g.

当 $p^n \geqslant 3$ 时,$\zeta_{p^n}^i$ $(1 \leqslant i \leqslant p^n, p \nmid i)$ 均不为实数. 从而对于分圆域 $\mathbb{Q}(\zeta_{p^n})$ $(p^n \geqslant 3)$ 我们有 $r_1 = 0, r_2 = \frac{1}{2}(p^n - p^{n-1})$.

例 3 纯三次域 $\mathbb{Q}(\sqrt[3]{2})$. 元素 $\sqrt[3]{2}$ 在 $\mathbb{Q}$ 上的极小多项式为 $x^3 - 2$. 于是 $\sqrt[3]{2}$ 的共轭元素为 $\sqrt[3]{2}, \sqrt[3]{2}\omega$ 和 $\sqrt[3]{2}\omega^2$,其中 $\omega = \zeta_3$. 由此可见 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 不是伽罗瓦扩张,其正规闭包为 $M = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$. 不难算出 $[M:\mathbb{Q}] = 6$ 而 $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$,并且对于域 $\mathbb{Q}(\sqrt[3]{2})$ 有 $r_1 = r_2 = 1$.

1.3 范与迹

设 L/K 为数域扩张,$[L:K] = n$. $\sigma_i: L \to \mathbb{C}$ $(1 \leqslant i \leqslant n)$ 是 L 的 n 个 K - 嵌入. 对于 $\alpha \in L$ 定义

$$N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha), T_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

分别称作元素 $\alpha \in L$ 对于扩张 L/K 的**范**和**迹**,从定义可知 $N_{L/K}$ 和 $T_{L/K}$ 有如下简单性质:

(a)对于 $\alpha, \beta \in L$, $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha) N_{L/K}(\beta)$, $T_{L/K}(\alpha + \beta) = T_{L/K}(\alpha) + T_{L/K}(\beta)$;

(b)对于 $\alpha \in K$, $N_{L/K}(\alpha) = \alpha^n$, $T_{L/K}(\alpha) = n\alpha$,其中 $n = [L:K]$.

下面的定理 1.3 给出范和迹的一种计算方法:

定理 1.3 设 L/K 为数域扩张，$[L:K]=n$，$\alpha\in L$，$f(x)=x^m-c_1x^{m-1}+\cdots+(-1)^m c_m\in K[x]$ 是 α 在 K 上的极小多项式，$m=[K(\alpha):K]$，则

$$N_{L/K}(\alpha)=c_m^{n/m},\ T_{L/K}(\alpha)=\frac{n}{m}c_1$$

证明 设 $\alpha_1=\alpha,\alpha_2,\cdots,\alpha_m$ 是 $f(x)$ 的 m 个根，由定义知

$$T_{K(\alpha)/K}(\alpha)=\alpha_1+\alpha_2+\cdots+\alpha_m=c_1$$

$$N_{K(\alpha)/K}(\alpha)=\alpha_1\alpha_2\cdots\alpha_m=c_m$$

根据定理 1.2，每个 K - 嵌入 $\tau_i:K(\alpha)\to\mathbb{C}(\tau_i(\alpha)=\alpha_i)$ 均可扩充成 $[L:K(\alpha)]=n/m$ 个嵌入 $\sigma_{ij}:L\to\mathbb{C}(1\leqslant j\leqslant n/m)$. 不难看出 $\{\sigma_{ij}\mid 1\leqslant i\leqslant m,1\leqslant j\leqslant n/m\}$ 是彼此不同的，从而构成 L 到 $\mathbb{C}$ 的全部 K - 嵌入，于是

$$\begin{aligned}N_{L/K}(\alpha)&=\prod_{i=1}^{m}\prod_{j=1}^{n/m}\sigma_{ij}(\alpha)=\prod_{i=1}^{m}\prod_{j=1}^{n/m}\tau_i(\alpha)=\prod_{i=1}^{m}\prod_{j=1}^{n/m}\alpha_i\\&=(\alpha_1\cdots\alpha_m)^{n/m}=c_n^{n/m}\\T_{L/K}(\alpha)&=\sum_{i=1}^{m}\sum_{j=1}^{n/m}\sigma_{ij}(\alpha)=\sum_{i=1}^{m}\sum_{j=1}^{n/m}\tau_i(\alpha)=\sum_{i=1}^{m}\sum_{j=1}^{n/m}\alpha_i\\&=\frac{n}{m}(\alpha_1+\cdots+\alpha_m)=\frac{n}{m}c_1\end{aligned}$$

□

注记 从定理 1.3 特别得到，对于每个 $\alpha\in L$，$N_{L/K}(\alpha)$ 和 $T_{L/K}(\alpha)$ 都是 K 中的元素. 再由性质(a)可知 $T_{L/K}:L\to K$ 是加法群同态，而 $N_{L/K}:L^\times\to K^\times$ 是乘法群同态，这里 $L^\times=L-\{0\}$.

定理 1.4(传递公式) 设 L/M，M/K 均是数域扩张，$\alpha\in L$，则

$$N_{L/K}(\alpha)=N_{M/K}(N_{L/M}(\alpha)),\ T_{L/K}(\alpha)=T_{M/K}(T_{L/M}(\alpha))$$

证明 令 $n=[L:M]$，$m=[M:K]$. $\sigma_1,\cdots,\sigma_n$ 为 L 到 $\mathbb{C}$ 中 n 个不同的 M - 嵌入，$\tau_1,\cdots,\tau_m$ 为 M 到 $\mathbb{C}$ 中 m 个不同的 K - 嵌入. 取 S 为扩张 L/K 的正规闭包. 令 $\tilde{\sigma}_i$，$\tilde{\tau}_j$ 分别为 σ_i 和 τ_j 到 S 上的一个扩充(定理 1.2)，它们都是伽罗瓦群 $\mathrm{Gal}(S/K)$ 中的元素. 从而 $(\tilde{\tau}_j\tilde{\sigma}_i)|_L(1\leqslant i\leqslant n,1\leqslant j\leqslant m)$ 均是 L 到 $\mathbb{C}$ 中的 K - 嵌入. 我们现在证明这 nm 个 K - 嵌入彼此不同：如果 $j\neq j'$，则存在 $b\in M$，使得 $\tau_j(b)\neq\tau_{j'}(b)$. 于是

$$\begin{aligned}(\tilde{\tau}_j\tilde{\sigma}_i)|_L(b)&=(\tilde{\tau}_j\tilde{\sigma}_i)(b)=\tilde{\tau}_j(b)\\&=\tau_j(b)\neq\tau_{j'}(b)=(\tilde{\tau}_{j'}\tilde{\sigma}_{i'})|_L(b)\end{aligned}$$

这就表明当 $j\neq j'$ 时 $(\tilde{\tau}_j\tilde{\sigma}_i)|_L\neq(\tilde{\tau}_{j'}\tilde{\sigma}_{i'})|_L$，如果 $j=j'$ 但是 $i\neq i'$，则存在 $c\in L$，使得 $\sigma_i(c)\neq\sigma_{i'}(c)$. 于是