HIT

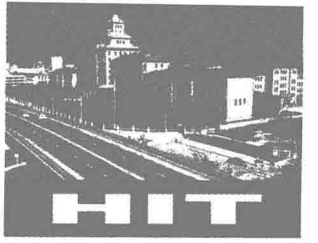
数论经典著作系列

Algebraic Number Theory

代数数论

[德]诺伊基希 著　　陶利群 译

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



数论经典著作系列

代数数论

Algebraic Number Theory

[德] 诺伊基希 著

陶利群 译

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

黑版贸审字 08-2015-031 号

内 容 简 介

本书是德国数学家 jürgen Neukirch 的名著,包含了他早前的著作《类域论》(Class Field Theory)中的内容.本书从 Arakelov 理论的观点出发介绍代数数论的经典内容,如代数整数,赋值论,类域论,ξ-函数与 L-级数等.书中提供了许多具体的例子帮助读者理解抽象的概念,许多地方的评述极富启发性,对许多结果的处理简洁优美,总之这是一本系统、全面的现代代数数论著作,是一本适合代数数论入门和进一步深入研究的参考书.

图书在版编目(CIP)数据

代数数论/(德)诺伊基希著;陶利群译. —哈尔滨:
哈尔滨工业大学出版社,2015.9
书名原文:Algebraic Number Theory
ISBN 978-7-5603-5593-1

Ⅰ.①代… Ⅱ.①诺…②陶… Ⅲ.①代数数论
Ⅳ.①O156.2

中国版本图书馆 CIP 数据核字(2015)第 209579 号

策划编辑 刘培杰 张永芹
责任编辑 张永芹 聂兆慈 杜莹雪
封面设计 孙茜艾
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 27.75 字数 782 千字
版 次 2015 年 9 月第 1 版 2015 年 9 月第 1 次印刷
书 号 ISBN 978-7-5603-5593-1
定 价 88.00 元

英文版前言

对我而言, 为Jürgen Neukirch的关于代数数论的书的英译本写序言是一个哀伤的时刻. 要是他自己能写这个序言, 那该多好啊!

而我写这个序言也很困难, 因为本书包含Neukirch在德文版中的序言. 在那里, 他本人讲了写书的目的、书的内容以及他对该主题的个人观点. 我还能说些什么呢?

从Neukirch的序言, 我们很清楚地看到数论是他在数学中最喜爱的课题. 他对此饱含热情, 并且把这种热情移植到了他的学生们的心里面.

他吸引学生们, 学生们在Rogensberg围绕着他. 他告诉他们这个课题和它的美值得他们尽最大努力去学习, 因此他们总是很热切并且积极地去学习数论和算术代数几何的最新进展. 我清楚地记得在多个场合, 这支队伍出现在Oberwolfach研究组的会议上并显示它(在数学和足球场上)的力量.

在Oberwolfach研究组的会议上, 人们聚在一起学习一个不一定属于他们专业的课题. 往往最后到作最困难的报告时, Rogensberg成员会承担起来. 同时, 这个团队的许多成员在德国的各个大学任教.

我们发现Jürgen Neukirch书中的这种魅力, 它将成为激励年轻的学生们学习代数数论的源泉, 我相信它会吸引他们中的许多人.

在Neukirch的葬礼上, 他的女儿Christiane朗诵从她父亲那经常听到的Theodor Fontane的一首诗《Von Ribbeck先生在Havel村》. 这个故事说: 一个贵族总是慷慨地从花园里摘梨赠予孩子们, 当他即将死去时, 他请求在他的墓地上栽一棵梨树, 以便将来孩子们能从长大的树上摘梨吃.

我相信, 这是思考Neukirch的书的一个好方法: 这里有树的种子, 树长大后, 孩子们就能摘到果实.

G. Harder

英文版译者的话

当我在1991年第一次接受Jürgen Neukirch的要求去翻译他的书《代数数论》(Algebraische Zahlentheorie)时, 没有人想到他不能活着看到这本英文版. 他确实见过这本翻译本的初稿(我在1996年秋季给他最后几章), 并且他还花时间仔细看过前面四章.

整个正文是由专门的数学语言详细叙述的, 因此我都是将它直译过来, 即使作者有意将复杂的论证和陈列的公式整合成易于理解的句子, 我也没能简单地用英语复述出来. 但是, Jürgen Neukirch用德语非常认真地准备他的书, 各个段落更是经过深思熟虑而成. 当我开始此书的翻译工作时, 他告知我说他没有在每个过渡处追求诗意美, 只是用适当的语言准确地表达思想. 让读者来评判我在忠实地传达他的思想方面是否成功吧.

在翻译中, 我建议用一个新词, 这得到了Jürgen Neukirch的同意. 我称之为充满因子、理想等, 而它们通常被称为Arakelov因子等(Jürgen Neukirch在德语版中避免了使用这个术语). 让时间来裁决哪个说法更好吧.

我非常感谢Frazer Javis仔细阅读我的全部手稿, 因此免除了我在英文翻译上的各种差错. 但是无需说, 我本人对尚存的所有缺陷负全责.

在Jürgen Neukirch于1997年初过早地去世后, EvaMaria Strobel夫人接手并极好地完成Jürgen Neukirch留下的工作. 她曾用无限的关怀和耐心对待原来的德文版, 并且帮助Jürgen Neukirch校对过译本的前四章. 要是没有她的学识、责任和精力, 这本书将不会存在. 要特别说的是, 细心的读者指出过的德文版中积累的相当数量的细小更正和修改已被现在的英文版所采纳. Kay Winberg慷慨地帮助检查过其中的一些. 我们衷心希望本书的出版会让它的作者感到欣慰.

Raymond Seroul, Strasbourg运用精湛的TEX技能对即将排印的稿件做了最后的准备, 我对此表示由衷的谢意.

感谢Springer员工全程照看这个计划直到完成. 其中, 我要特别感谢Joachim Heinze多年来极少干预, 但有效地管理使这项翻译工作得以实现.

Norbert Schappacher

1999年3月于Strasbourg

德文版序言

在所有的数学分支中, 数论占有理想化的地位, 这类似于数学在科学中的地位. 数论没有义务为不源于自身的需要服务, 本质上它自动地设立其目标, 然后成功地守护使其和谐不被打扰. 简单制定其基本问题的可能性, 陈述问题的特别清晰性, 神秘接触的规律, 不管是发现的, 未发现的, 或者仅是猜测的; 最后但并非最次要的一点是数论中特别令人满意的推理方式的魅力——所有这些特色总是在吸引大批忠实的追随者到数论圈中来.

但是, 不同的数论专家们可能以不同的方式献身于他们的科学. 一些人尽可能地推进必要的理论发展直到得出他们想要的具体结果. 其他人则努力追求更广泛清晰的概念, 孜孜不倦地搜寻各种明显的算术现象背后深藏的论据. 两种观点都有道理, 并且通过相互启发, 相互影响特别有效地成长. 几本漂亮的教科书说明了前一种观点的成功, 它针对具体的问题. 我们特别选择其中一本, S.I.Borevicz与I.R.Šafarevič写的《数论》[14]. 这本书内容虽然异常丰富, 却易读, 因此我们特别推荐给大家.

我在构想本书时心里有一个不同的目标. 它确实给学生提供了一个本质上自封的代数数论简介, 只假定读者有基础代数知识(从等式$2 = 1 + 1$开始). 但是不像上面引用的那些教科书那样, 本书循序渐进地强调依赖现代概念的理论方面. 在做的过程中, 为了让读者对数论本来的具体目标不致视而不见, 我们特别努力限制使用抽象的数量. 近几十年来, 数论与算术代数几何结合, 经历了革命性发展, 因此如今尽可能多地以统一的观点介绍数论的想法似乎有必要. 这种已经带来了巨大成功的新的几何观点——例如它出现在Weil猜想、Mordell猜想、与Birch和Swinnerton-Dyer猜想有关的问题的背景中, 大都以无条件、广泛地应用概念上的方法为基础.

的确, 这些引人注目的结果很难在本书中触及, 因为它们需要高维理论, 而本书有意局限于代数数域, 即1维情形. 但是我认为有必要将这些发展考虑进去来展示代数数论, 将它们当作远焦, 从高观点中借用重点和论据, 从而将代数数域的理论整合到高维理论, 或者至少避免给这种整合造成障碍. 这就是我在只要可行的情况下选择函子的观点和更深远的论据, 而放弃聪明的技巧, 并且作了一番特别的努力将有代数曲线精神的几何解释放在前面的原因.

就让我放弃在前言描述各个章节的内容的惯例吧, 因为简单翻几页就可以用一种更有趣的方式得到同样的信息. 但是我想强调写书时我的几点基本指导原则. 第1章为代数数域的整体类域理论打基础, 而第2章则是为它的局部类域理论奠定基础, 这些基础最终在第3章的前三节汇总, 目的是为了介绍代数曲线中的经典概念和结果与Riemann-Roch定理的思想之间的完美类比. 这种讲解受到近年来得到很大重视的Arakelov观点的支配. 这种方法连同它错综复杂的正规化可能是第一次在教科书中得到广泛的探讨. 但是我最终决定不用Arakelov除子这个术语, 尽管它如今已经被广泛使用. 要是不这样就意味着在许多其他概念上要加上Arakelov的名字, 从而为这个初等材料介绍太笨重的术语. 因为Arakelov本人也仅为算术曲面介绍他的除子, 我的决定似乎就更有理由了. 数域情形相应的思想

可追溯到Hasse, 而且显然在例如S.Lang的书[95]中得到强调.

曾经在决定是否将类域论收入到书中的第4~6章时犹豫过. 因为我不久前已经出版过了关于这个主题的书[108], 再探讨这个理论就明显有疑问. 但在经历很长的思考后, 最终我没有其他选择. 一本关于代数数域的读物, 如果没有类域论的至顶结论及其关于L-级数的重要结果将是一个残缺的东西, 从而饱受不可接受的不完整的痛苦. 这给了我修改和增补旧作的机会, 加了不少例子以丰富有点枯涩的讲解, 提前做了一些注释作为参考, 增加了有益的习题.

在最后一章关于ζ函数和L-级数做了许多工作. 这些函数的重要性在近几十年提到了中心位置, 而教科书却没有充分地注意它们. 但我没有把Tate基于调和分析处理Hecke L-级数的方法收入, 尽管它可能会很好地适合书中更具概念性方面的内容. 事实上, Tate自己清晰的处理已经无法再改进, 并且它在其他地方已经重复过多了. 相反, 我选择回到Hecke的方法. 由于它的原版不容易理解, 为了显示其中的诸多优势, 我们需要对它作一个现代处理. 这一点已经做到, 很明显还有机会完全用函数方程介绍Artin L-级数, 但是很奇怪, 现有的书都没有做过.

很难决定把Iwasawa理论, 一个相对近又完全贴合本书的主题代数数域的理论排除掉. 因为它反映代数曲线的重要几何性质, 所以它本该是我们经常重复的论点: 数论是几何的一个特别漂亮的支持. 但是, 我的确相信, 在此情形下人们只有用平展(étale)上同调(这里, 我们既不能假定也不能合理发展它), 几何才真正令人信服. 也许因为排除它导致的不满会足够强烈到产生这一卷的续集去专门讨论代数数域的上同调.

最开始, 本书不仅打算作为代数数论的原始资料, 还想作为一门课的方便的教材. 这种打算被意外增多的因理论内部需要而不得不添加的材料日益阻碍. 但是我认为本书还没有失去它的特性. 实际上这方面它已经通过了第一次测试. 稍微细心规划一下, 前三章的基本内容能在一个学年内讲授完(可能的话, 包括无限Galois理论). 接下来的学期将为第4~6章的类域论提供珍贵而足够的空间.

§1.11 ~ §1.14的大部分可以在导论课程中去掉. 尽管§1.12关于级的结果跟后文无关, 我认为把它插入书中特别重要. 一方面, 级组成在许多Diophantine问题中起重要作用的乘子环. 更重要的是, 它们代表类似于奇异代数曲线的东西. 因为上同调理论对于代数数域越来越重要, 又因为它对于没有奇异概型就不能构造的代数K-理论更是如此, 是时候给级一个适当的处理了.

在§2.6中关于Hensel域的特殊处理可以局限于完备赋值域, 因此可以将它与§2.4合并. 如果时间仓促, §2.10关于高阶分歧理论可以完全省略.

第3章的前三节应该在授课时介绍, 因为他们强调代数数论的经典结果的一个新方法. 随后的关于Grothendieck-Riemann-Roch定理的理论是学生讨论班的一个好课题, 而不适合一门导论课.

最后, 如果学生已经熟悉射有限群和无限Galois理论, 在介绍类域论时可以节省大量的时间. §5.4~§5.7关于形式群, Lubin-Tate理论和高阶分歧理论, 可以省略不讲. 还可以减掉些, 如关于Hilbert符号的§5.3、§6.7和§6.8, 这样仍然留下一个完全成熟的理论, 但却不如人意, 因为剩下的是一个抽象而没有跟经典问题发生任何联系的领域.

关于各个章节后的习题再说几句. 它们中有一些不算是习题, 而是因不适合放在正文里故而加上的注释. 我们鼓励读者查阅文献证明自己这方面的才能. 我应该指出我本人没有做完所有的习题, 因此可能在问题的提法上偶尔会有错误. 愿读者对作者可能有的这种疏忽的反应被以下Goethe的诗句缓解:

错误曾伴随我们. 但是一些天使的需要
轻柔地诱导我们拼搏的心灵向上, 朝着真理.

在本书的写作过程中，我曾得到多方面的帮助. 感谢Springer Verlag大度地考虑我的愿望. 我的学生I.Kausz, B.Köck, P.Kölcze, Th.Moser, M.Spiess曾严格检查或多或少的部分书稿，使我改进了许多地方，并且避免了多处错误和内容上的含混不清. 我的朋友W.-D.Geyer, G.Tamme和K.Wingberg对我提出许多有价值的建议使本书受益，C.Deninger和U.Jannsen建议我对Hecke的theta级数和L-级数理论给出新的处理，对此我表示感谢. 感谢Eva-Maria夫人，她画了许多图，帮助我校对和设计正文，不知疲倦地处理最细微的细节. 衷心感谢所有帮助过我的人，还有那些没有提到的人. 非常感谢Martina夫人用TEX软件编辑的手稿. 这本书能面世本质上是由于她的高超技能、永远可靠、和蔼可亲，这些特点贯穿她对长篇手稿的处理工作，贯穿她的许多修改、添加、更正工作，她总是力求做到最好.

Jürgen Neukirch
1992年2月于Regensburg

目 录

第 1 章　代数整数

§1.1　Gauss整数

等式

$$2=1+1,\quad 5=1+4,\quad 13=4+9,\quad 17=1+16,\quad 29=4+25,\quad 37=1+36$$

说明前面几个素数能够表示成两个平方数之和. 除了2之外, 它们都是$\equiv 1 \bmod 4$, 并且一般地, 任何形如$p=a^2+b^2$的素数都满足$p\equiv 1 \bmod 4$, 因为每个平方数都$\equiv 0$或者$\equiv 1 \bmod 4$, 这是显然的. 它的逆不是显然的, 这个了不起的结论也成立：

定理 1.1.1　对所有素数$p\neq 2$有：

$$p=a^2+b^2(a,b\in\mathbb{Z}) \implies p\equiv 1 \bmod 4.$$

关于有理整数环$\mathbb{Z}$的这个算术法则可以在更大的**Gauss整数**环

$$\mathbb{Z}[\mathrm{i}]=\{a+b\,\mathrm{i}\,|a,b\in\mathbb{Z}\},\ \mathrm{i}=\sqrt{-1}$$

中得到自然地解释.

命题 1.1.2　$\mathbb{Z}[\mathrm{i}]$是Euclid环, 因此特别地, 它是唯一分解环.

证明: 我们证明$\mathbb{Z}[\mathrm{i}]$关于函数$\mathbb{Z}[\mathrm{i}]\to\mathbb{N}\cup\{0\},\alpha\mapsto|\alpha|^2$是Euclid环. 因此, 对于$\alpha,\beta\in\mathbb{Z}[\mathrm{i}],\beta\neq 0$, 我们需要证明存在Gauss整数$\gamma,\rho$使得

$$\alpha=\gamma\beta+\rho,\ 并且|\rho|^2<|\beta|^2.$$

显然我们只需要找到$\gamma\in\mathbb{Z}[\mathrm{i}]$使得$|\frac{\alpha}{\beta}-\gamma|<1$. 因为Gauss整数构成复平面$\mathbb{C}$的一个**格**(那些关于基$1,\mathrm{i}$有整数坐标的点). 复数$\frac{\alpha}{\beta}$落在这个格的某个网格中, 且它到最近格点的距离不大于该网格的对角线的长度$\frac{\sqrt{2}}{2}$. 因此存在某个元$\gamma\in\mathbb{Z}[\mathrm{i}]$使得$|\frac{\alpha}{\beta}-\gamma|\leqslant\frac{\sqrt{2}}{2}<1$. □

基于环$\mathbb{Z}[\mathrm{i}]$的结果, 可得到定理1.1.1：只需要证明$\mathbb{Z}$中的素数$p\equiv 1 \bmod 4$不是$\mathbb{Z}[\mathrm{i}]$中的素元. 事实上, 如果证明了它, 则有分解

$$p=\alpha\cdot\beta,$$

α,β是$\mathbb{Z}[\mathrm{i}]$中的两个非单位元. 定义$z=x+\mathrm{i}\,y$的**范**为

$$N(x+\mathrm{i}\,y)=(x+\mathrm{i}\,y)(x-\mathrm{i}\,y)=x^2+y^2,$$

即$N(z)=|z|^2$. 范是乘性的, 因此我们有

$$p^2=N(\alpha)\cdot N(\beta).$$

因为α,β不是单位, $N(\alpha),N(\beta)\neq 1$(见习题1.1.1), 从而$p=N(\alpha)=a^2+b^2$, 其中$\alpha=a+b\,\mathrm{i}$.

最后, 为了证明形如$p=1+4n$的有理素数不是$\mathbb{Z}[\mathrm{i}]$的素元, 我们注意到同余式

$$-1\equiv x^2 \bmod p$$

有一个解$x=(2n)!$. 事实上, 由Wilson定理有$-1\equiv(p-1)!\bmod p$, 我们有

$$\begin{aligned}-1 &\equiv (p-1)!=[1\cdot 2\cdots(2n)][(p-1)(p-2)\cdots(p-2n)]\\ &\equiv [(2n)!][(-1)^{2n}(2n)!]=[(2n)!]^2 \bmod p.\end{aligned}$$

因此我们有$p|x^2+1=(x+\mathrm{i})(x-\mathrm{i})$. 但是因$\dfrac{x}{p}\pm\dfrac{\mathrm{i}}{p}\notin\mathbb{Z}[\mathrm{i}]$, p不整除因子$x+\mathrm{i},x-\mathrm{i}$中的任何一个, 从而不是唯一分解环中的素元.

等式$p=x^2+y^2$的例子说明：即使关于有理整数的很初等的问题都可能需要在更高层次的整数环中考虑. 但是我们针对这个等式已经引入的环$\mathbb{Z}[\mathrm{i}]$还不够, 这只是用来揭开一般代数整数理论的序篇的一个具体的例子. 出于同样的理由, 我们将更仔细地来看这个环.

当发展一个环的可除性理论时, 有两个基本问题最为显著：一方面要决定这个环的**单位**, 另一方面是决定它的**素元**. 对于第一个问题, 在目前的情形下特别容易得到答案. 数$\alpha=a+b\,\mathrm{i}\in\mathbb{Z}[\mathrm{i}]$是一个单位当且仅当它的范是1：

$$N(\alpha):=(a+\mathrm{i}\,b)(a-\mathrm{i}\,b)=a^2+b^2=1.$$

(习题1.1.1), 即$a^2=1,b^2=0$, 或者$a^2=0,b^2=1$. 因此我们得到:

命题 1.1.3 环$\mathbb{Z}[\mathrm{i}]$的单位元群由四个元组成：

$$\mathbb{Z}[\mathrm{i}]^*=\{1,-1,\mathrm{i},-\mathrm{i}\}.$$

为了回答素元, 即$\mathbb{Z}[\mathrm{i}]$的不可约元的问题, 我们先回顾一下：环中两个元α,β称为**相伴的**, 如果它们只相差一个单位因子, 记为$\alpha\sim\beta$; 每个与不可约元π相伴的元也不可约. 由定理1.1.1, 我们精确地列出$\mathbb{Z}[\mathrm{i}]$的所有素元如下:

定理 1.1.4 若不计相伴元, $\mathbb{Z}[\mathrm{i}]$中的素元π由以下给出：

(1) $\pi=1+\mathrm{i}$;

(2) $\pi=a+b\,\mathrm{i}$满足$a^2+b^2=p,p\equiv 1 \bmod 4, a>|b|>0$;

(3) $\pi=p$, $p\equiv 3 \bmod 4$,

这里p表示$\mathbb{Z}$中的一个素数.

证明: (1)和(2)中的数是素数, 这是因为由$\mathbb{Z}[\mathrm{i}]$中的分解$\pi=\alpha\cdot\beta$得到等式

$$p=N(\pi)=N(\alpha)\cdot N(\beta),$$

p为某个素数, 从而$N(\alpha)=1$或者$N(\beta)=1$, 因此α或β是一个单位.

数$\pi=p$, 其中$p\equiv 3 \bmod 4$, 是$\mathbb{Z}[\mathrm{i}]$中的素元, 因为分解式$p=\alpha\cdot\beta$, α,β为非单位, 意味$p^2=N(\alpha)\cdot N(\beta)$, 因此$p=N(\alpha)=N(a+b\mathrm{i})=a^2+b^2$, 由定理1.1.1得到$p\equiv 1 \bmod 4$.

我们还需要验证$\mathbb{Z}[\mathrm{i}]$中的每个素元π与列出的某个素元相伴. 首先, 分解式

$$N(\pi)=\pi\cdot\bar{\pi}=p_1\cdots p_r,$$

p_i为有理素数, 说明$\pi|p$, p为某个p_i. 由此得到$N(\pi)|N(p)=p^2$, 因此$N(\pi)=p$或者$N(\pi)=p^2$. 在$N(\pi)=p$的情形, 我们得到$\pi=a+b\mathrm{i}$满足$a^2+b^2=p$, 从而π形如(2)或者当$p=2$时, 与$1+\mathrm{i}$相伴. 另一方面, 若$N(\pi)=p^2$, 则π与p相伴, 因为p/π是一个范为1的整元, 从而为一个单位. 而且此时必定有$p\equiv 3 \bmod 4$, 否则$p=2$ 或者$p\equiv 1 \bmod 4$, 由定理1.1.1, $p=a^2+b^2=(a+b\mathrm{i})(a-b\mathrm{i})$不是素元. 证毕. □

这个命题也完全解决了$\mathbb{Z}[\mathrm{i}]$中的素数$p\in\mathbb{Z}$如何分解的问题. 素数$2=(1+\mathrm{i})(1-\mathrm{i})$与素元$1+\mathrm{i}$的平方相伴. 事实上, 等式$1-\mathrm{i}=-\mathrm{i}(1+\mathrm{i})$就说明了$2\sim(1+\mathrm{i})^2$. 素数$p\equiv 1 \bmod 4$分裂为两个共轭的素因子

$$p=(a+b\mathrm{i})(a-b\mathrm{i}),$$

而素数$p\equiv 1 \bmod 4$在$\mathbb{Z}[\mathrm{i}]$中仍为素元.

Gauss整数在域

$$\mathbb{Q}(\mathrm{i})=\{a+b\mathrm{i}\,|a,b\in\mathbb{Q}\}$$

中起到的的作用与有理整数$\mathbb{Z}$在域$\mathbb{Q}$中的作用是一样的. 因此它们应该被看作$\mathbb{Q}(\mathrm{i})$中的“整数”. 整的概念是相对于基$1,\mathrm{i}$的坐标来说的. 然而, 我们有下面对Gauss整数的刻画, 它不依赖基的选取.

命题 1.1.5 $\mathbb{Z}[\mathrm{i}]$恰好是由$\mathbb{Q}$的扩域$\mathbb{Q}(\mathrm{i})$中满足首一多项式方程

$$x^2+ax+b=0,$$

系数$a,b\in\mathbb{Z}$的元素组成.

证明: 元素$\alpha=c+\mathrm{i}\,d\in\mathbb{Q}(\mathrm{i})$是多项式

$$x^2+ax+b\in\mathbb{Q}[x],\ \text{其中}a=-2c, b=c^2+d^2,$$

的根. 若c,d都是有理整数, 那么a,b也是. 反之, 若a,b都是整数, 那么$2c,2d$也是. 由$(2c)^2+(2d)^2=4b\equiv 0 \bmod 4$得$(2c)^2\equiv(2d)^2\equiv 0 \bmod 4$, 因为平方数总是$\equiv 0$或者$\equiv 1$. 因此$c,d$都是整数. □

上述命题把我们引向代数整数的一般概念, 它作为元素满足有理系数的首一多项式. 对于Gauss整数环, 我们在这一节已经得到关于单位、素元以及唯一分解问题的完美答案.

这些问题已经暗示一般代数整数理论中的基本问题. 但我们在特殊情形$\mathbb{Z}[\mathrm{i}]$中找到的答案不是典型的. 取而代之的是, 它们将展示新的特点.

习题1.1.1 $a\in\mathbb{Z}[\mathrm{i}]$是一个单位当且仅当$N(a)=1$.

习题1.1.2 证明: 在环$\mathbb{Z}[\mathrm{i}]$中, 关系式$\alpha\beta=\varepsilon\gamma^n$, 其中$\alpha,\beta$互素, ε是单位, 意味$\alpha=\varepsilon'\xi^n, \beta=\varepsilon''\eta^n$, 其中$\varepsilon',\varepsilon''$是单位.

习题1.1.3 证明方程

$$x^2+y^2=z^2$$

使得$x,y,z>0,(x,y,z)=1$(“Pythagoras三元数组”)的所有整数解, 若不计x,y的置换, 由公式

$$x=u^2-v^2,\ y=2uv,\ z=u^2+v^2$$

给出, 其中$u,v\in\mathbb{Z},u>v>0,(u,v)=1,u,v$不全为奇数.

提示： 由习题1.1.2证明必有$x+\mathrm{i}\,y=\varepsilon\alpha^2$, 其中$\varepsilon$是单位, $\alpha=u+\mathrm{i}\,v\in\mathbb{Z}[\mathrm{i}]$.

习题1.1.4 证明: 不可能给$\mathbb{Z}[\mathrm{i}]$一个序.

习题1.1.5 对于任意有理整数$d>1$, 环$\mathbb{Z}[\sqrt{-d}]=\mathbb{Z}+\mathbb{Z}\sqrt{-d}$的唯一单位是$\pm1$.

习题1.1.6 对于任意有理整数$d>1$, 环$\mathbb{Z}[\sqrt{d}]=\mathbb{Z}+\mathbb{Z}\sqrt{d}$有无穷多个单位.

习题1.1.7 证明环$\mathbb{Z}[\sqrt{2}]=\mathbb{Z}+\mathbb{Z}\sqrt{2}$是Euclid环. 进一步证明它的单位由$\pm(1+\sqrt{2})^n,n\in\mathbb{Z}$给出, 并决定它的素元.

§1.2 整性

一个**代数数域**是$\mathbb{Q}$的一个有限扩域K. K中元称为**代数数**. 一个代数数称为**整的**, 或者**代数整数**, 如果它是一个首一多项式$f(x)\in\mathbb{Z}[x]$的根. 整性的概念不仅适用于代数数, 它还在许多不同场合出现, 因此需要对它做一般的全面处理.

以下的环都视为有单位元的交换环.

定义 1.2.1 设$A\subseteq B$为环扩张. 元素$b\in B$称为在A上整的, 如果它满足一个首一方程

$$x^n+a_1x^{n-1}+\cdots+a_n=0,n\geqslant1,$$

其中$a_i\in A$. 若所有的$b\in B$在A上整, 则环B称为在A上整.

我们希望A上的两个整元的和与积还是整的, 但是很奇怪的是这一点并非显然. 这是下面对整性概念的抽象诠释的结果.

命题 1.2.2 有限个元$b_1,\ldots,b_n\in B$在A上都是整的当且仅当环$A[b_1,\ldots,b_n]$作为A-模是有限生成的.

要证明它, 我们需要下面线性代数中的一个结果.

命题 1.2.3 (行列展开) 设$A=(a_{ij})$是一个$(r\times r)$- 矩阵, a_{ij}属于某个任意的环. 设$A^*=(a_{ij}^*)$ 是其相伴矩阵, 即$a_{ij}^*=(-1)^{i+j}\det(A_{ij})$, 其中矩阵$A_{ij}$是从$A$中删去第$i$列和第$j$行得到. 我们有

$$AA^*=A^*A=\det(A)E,$$

其中E是秩r的单位矩阵. 对于任意向量$x=(x_1,\cdots,x_r)$, 有蕴含关系:

$$Ax=0\implies(\det A)x=0.$$

命题1.2.2的证明： 设$b \in B$在A上整, $f(x) \in A[x]$是一个次数为$n \geqslant 1$的首一多项式使得$f(b) = 0$. 对于任意多项式$g(x) \in A[x]$, 我们可以写成

$$g(x) = q(x)f(x) + r(x),$$

其中$q(x), r(x) \in A[x]$且$\deg(r(x)) < n$, 因此我们有

$$g(b) = r(b) = a_0 + a_1 b + \cdots + a_{n-1}b^{n-1}.$$

因此$A[b]$是由$1, b, \ldots, b^{n-1}$生成的A-模.

更一般地, 若$b_1, \ldots, b_n \in B$在A上是整的, 则对n作归纳可以得到$A[b_1, \ldots, b_n]$是A上的有限型. 事实上, 因为b_n在$R = A[b_1, \ldots, b_{n-1}]$上整, 由我们刚才所证得$R[b_n] = A[b_1, \ldots, b_n]$在$R$上是有限生成的. 由归纳假设$R$是一个有限型的$A$-模, 因此$A[b_1, \ldots, b_n]$在$A$上是有限生成的.

反过来, 若假定A-模$A[b_1, \ldots, b_n]$是有限生成的, 且$\omega_1, \cdots, \omega_r$是一个生成元系. 那么, 对任意$b \in A[b_1, \ldots, b_n]$, 我们得到

$$b\omega_j = \sum_{j=1}^{r} a_{ij}\omega_j, i = 1, \ldots, r, a_{ij} \in A.$$

从命题1.2.3我们有$\det(bE - (a_{ij}))\omega_i = 0, i = 1, \ldots, r$(这里$E$是秩$r$的单位矩阵), 又因为$1 = c_1\omega_1 + \cdots + c_r\omega_r$, 等式$\det(bE - (a_{ij})) = 0$给出$b$满足的系数在$A$中的首一方程. 这就证明了$b$事实上是在$A$上整的. □

根据这个命题, 如果$b_1, \ldots, b_n \in B$在A上整, 那么$A[b_1, \ldots, b_n]$中的任意元b也是如此, 因为$A[b_1, \ldots, b_n, b] = A[b_1, \ldots, b_n]$是有限生成的$A$-模. 特别地, 给定两个整元$b_1, b_2 \in B$, 则有$b_1 + b_2, b_1b_2$也是$A$上整元. 同时我们得到:

命题 1.2.4 设$A \subseteq B \subseteq C$为两个环扩张. 若$C$在$B$上整, B在A上整, 则C在A上整.

证明： 取$c \in C$, 设$c^n + b_1c^{n-1} + \cdots + b_n = 0$为系数在$B$中的方程. 记$R = A[b_1, \ldots, b_n]$, 则$R[c]$为有限生成的$R$-模. 若$B$在$A$上整, 则因$R$在$A$上有限生成, $R[c]$甚至在A上是有限生成的, 因此c在A上整. □

由我们证明的结果, 环扩张$A \subseteq B$中元素的集合

$$\bar{A} = \{b \in B | b在A上整\}$$

作成一个环, 它称为A在B中的**整闭包**. 若$A = \bar{A}$, A称为**整闭**的. 由命题1.2.4立得整闭包$\bar{A}$本身在B中整闭. 若A是一个整环且K为其商域, 则A在K中的整闭包$\bar{A}$叫A的**正规化**, 且若$A = \bar{A}$, 简称A为整闭. 例如, 每个**唯一分解环**是整闭的. 事实上, 若$a/b \in K(a, b \in A)$在A上整, 即

$$(a/b)^n + a_1(a/b)^{n-1} + \cdots + a_n = 0, a_i \in A,$$

那么

$$a^n + a_1ba^{n-1} + \cdots + a_nb^n = 0.$$

因此每个整除b的素元π也整除a. 假定a/b是约化的, 就得到$a/b \in A$.

我们现在转向更特定的条件. 令A是一个整环, 在它的商域K中整闭, L/K是一个域扩张, B为A在L中的整闭包. 由命题1.2.4, B自动整闭. 每个元$\beta \in L$形如

$$\beta = \frac{b}{a}, b \in B, a \in A,$$

因为若

$$a_n\beta^n + \cdots + a_1\beta + a_0 = 0, a_i \in A, a_n \neq 0,$$

则$b = a_n\beta$在A上整, 整式方程

$$(a_n\beta)^n + \cdots + a_1'(a_n\beta) + a_0' = 0, a_i' \in A,$$

由β满足的方程乘以a_n^{n-1}得到. 而且, 由A是整闭的事实得出$\beta \in L$在A上整当且仅当它的**极小多项式**$p(x)$的系数在A中. 事实上, 设β是首一多项式$g(x) \in A[x]$的根, 则$p(x)$在$K[x]$中整除$g(x)$, 因此$p(x)$的所有根$\beta_1, \cdots, \beta_n$在A上整, 从而所有系数也整, 换句话说, $p(x) \in A[x]$.

域扩张L/K中的迹与范为研究L中的整元提供了重要的工具. 我们回顾一下:

定义 1.2.5 元$x \in L$的**迹**与**范**分别定义为K-向量空间L的自同态

$$T_x : L \longrightarrow L,\ T_x(\alpha) = x\alpha,$$

的迹与行列式

$$Tr_{L/K}(x) = Tr(T_x),\ N_{L/K}(x) = \det(T_x).$$

从T_x的特征多项式

$$f_x(t) = \det(t\,\mathrm{id} - T_x) = t^n - a_1t^{n-1} + \cdots + (-1)^n a_n \in K[t],$$

$n = [L : K]$, 我们看出迹与范为

$$a_1 = Tr_{L/K}(x)和a_n = N_{L/K}(x).$$

因为$T_{x+y} = T_x + T_y$, $T_{xy} = T_x \circ T_y$, 我们得到同态

$$Tr_{L/K} : L \longrightarrow K和N_{L/K} : L^* \longrightarrow K^*.$$

在L/K为可分扩张的情形, 迹与范有下面用Galois理论得到的解释.

命题 1.2.6 设L/K是可分扩张, $\sigma : L \to \bar{K}$取遍L到K的代数闭包的K-嵌入, 则有:
(i) $f_x(t) = \prod_{\sigma}(t - \sigma x)$;
(ii) $Tr_{L/K}(x) = \sum_{\sigma} \sigma x$;
(iii) $N_{L/K}(x) = \prod_{\sigma} \sigma x$.

证明: 特征多项式$f_x(t)$是x的极小多项式$p_x(t)$的幂

$$f_x(t) = p_x(t)^d, \quad d = [L : K(x)],$$

$$p_x(t) = t^m + c_1t^{m-1} + \cdots + c_m, \quad m = [K(x) : K].$$

事实上, $1, x, \ldots, x^{m-1}$是$K(x)/K$的一组基, 且若$\alpha_1, \ldots, \alpha_d$是$L/K(x)$ 的一组基, 则