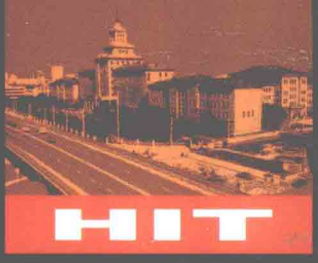


HIT

数论经典著作系列

Algebraic Number Theory

代数数论

潘承洞　潘承彪　著

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

Algebraic Number Theory

代数数论

潘承洞 潘承彪 著

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

内 容 简 介

本书在初等数论的基础与观点之上，以尽可能少的抽象代数概念与方法，来具体地介绍代数数论中最经典、最基本、因而也是最初等的内容．它取材恰当，概念的引进自然、清楚，从具体到抽象、特殊到一般的写法，以及配有适当的例题和习题，使初学者容易理解、掌握，而且所得到的实质性结论并不比通常的代数数论教材要少．

本书适用于大中师生和数学爱好者．

图书在版编目(CIP)数据

代数数论/潘承洞，潘承彪著．—哈尔滨：哈尔滨工业大学出版社，2011.3

ISBN 978-7-5603-3202-4

Ⅰ.代… Ⅱ.①潘…②潘… Ⅲ.①代数数论 Ⅳ.①O156.2

中国版本图书馆 CIP 数据核字(2011)第 031083 号

策划编辑 刘培杰 张永芹
责任编辑 刘 瑶
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 21.75 字数 402 千字
版 次 2011 年 3 月第 1 版 2011 年 3 月第 1 次印刷
书 号 ISBN 978-7-5603-3202-4
定 价 48.00 元

⊙第三版序

去年，刘培杰先生慎重表示哈尔滨工业大学出版社愿意再版承洞和我20年前写的《代数数论》一书，这有些出乎我的意外。因为，国内外的代数数论书已经有了不少，而这本书的内容只是其中很少的一部分，它可能是国内现在的常见的代数数论书中最简单、最基本、最具体的入门书。它不涉及任何现代思想、概念、方法和理论，只是较系统地讲述了在20世纪前期就得到的代数数论的一些基本知识，而且其中一些结论从更高的观点是很容易简单地推出来的(把本书和其他代数数论书一对照就可看出)。

经再三考虑我同意了这一建议，因为从某种意义上讲，这样的书对初学者是有一定好处的，这一层意思在第一版序言中已经说了，这本书本来就是为他们写的。几十年来，我见到过一些数学工作者宣称自己解决了某个重要猜想或得到了重大成果的论文，但仔细一看，虽然有的用了“新思想”、“新方法”，却是在根上犯了初等数论中的不可改正的简单错误，一切都成了无本之木，无源之水。我想，让年轻学生在仰望灿烂星空、无比兴奋和陶醉的同时，能静下心来了解一点新东西产生的土壤，脚踏实地地打好一个坚实的基础，为未来的学习和研究确立一个严肃正确的学风，这本书或许是有一点好处的。

本来考虑要增加一些内容，但由于出版计划的安排，来不及写了，以后有机会再补上。在校对书样时也发现了一些疏误，请读者对本书的缺点错误不吝指正。

本书责任编辑刘瑶女士不仅改正了书中不少笔误和疏漏，提出了有益的建议，还改进了编排。在此表示衷心感谢！

最后，衷心感谢刘培杰先生和他的数学工作室，使本书有机会再次出版。

潘承彪

2011 年 3 月 17 日

⊙第二版序

最近,一些同志问我要我们写的《初等代数数论》,一打听才知道出版社已经没有存书了.承蒙山东大学出版社的大力支持,决定再版本书,对此表示衷心的感谢.

使我们高兴的是,一些使用过本书的老师和学生反映较好,认为它取材恰当,概念的引进自然、清楚,从具体到抽象、特殊到一般的写法,以及配有适当的例题和习题,使初学者容易理解、掌握,而且所得到的实质性结论(例如,有关类数、Fermat 大定理的结论)并不比通常的代数数论教材要少.并认为由此再进一步学习代数数论可收到更好的效果.这一点正是我们所期望的,并在序言中已经说到了.当然,要学习代数数论是不能停留在这样的水平的.

至今,最好的代数数论入门书可能仍是 E. Hecke 于 1923 年写的《Lectures on the Theory of Algebraic Numbers》.但该书对初学者可能有一定困难,而且没有习题.如果配合它同时学习我们的书可能会好些.这也是我们写该书的目的之一.

本书原来名为《初等代数数论》,其理由在序言中已作说明,这是我所坚持的,但承洞并不赞成,因为其内容以至方法并不"初等",这是有道理的.所以,现在再版时更名为《代数数论》,这是更合适的.经过十多年的教学,觉得本书的取材、讲述是适当的,所以全书仍保持原状未作改动,我仅对所发现的疏漏和印刷错误作了更正,添加了一本参考书及两个注.当然,一定还有不少不当之处,望读者不吝指正.

本书责任编辑孙秀英同志提出了许多有益的建议，排版质量明显提高，她的高效率的工作使本书能这样快地和读者见面，对此我表示衷心感谢！

承洞离开我们已经整整三年了．只能由我写几句以作说明．

潘承彪

2000 年 12 月 27 日

⊙第一版序

代数数论最经典、最基本的概念、方法和结论，对于学习数学的人来说是十分重要的，这些内容应当构成大学数学系的一门必修课程.

数学的概念与方法愈来愈抽象化与一般化，大概是它本身发展中不可避免的现象.高观点、抽象地讲述数学对专家来说可能是一件十分方便的事情，但给初学者带来很大的困难，而且对今后数学的发展可能并不是一件好事.

本书在初等数论的基础与观点之上，以尽可能少的抽象代数概念与方法，来具体地介绍代数数论中最经典、最基本、因而也是最初等的内容.所以本书取名为《初等代数数论》.但这些内容正是代数数论发展起来的泉源.限于篇幅，本书没有讨论二元二次型的算术理论，尽管它也是代数数论开始发展起来的一个方面.

一个新概念或新方法，只有当它能解决已有的概念、方法所不能解决(或解决起来很复杂)的问题，显示出它的优越性时，才能证明引进它是必要的，并为人们所真正接受.因此，我们应该知道从原有的(一般说来是较初等的)概念与方法能得到些什么结论，和怎样得到这些结论的.这也有助于对新概念与新方法的理解和掌握.此外，我们认为计算是重要的，这不仅对应用数学是这样，对基础数学也是如此.这些也是我们写本书所遵循的想法.

从本书的前面五章中，可以看到初等数论的内容是如何推广到所谓“二次代数整数环”——除有理整数环外最简单的代数整数环——上去，以及这种推广是如何有助于解决初等数论中的一些困难问题.学习这五章可对代数数论要研究的对象、基本内容有一个极初步的了解，这些内容对只想稍为知道一些代数数论知识的人，可能是足够了.

关于代数数论的发展历史和近期进展，我们建议读者去阅读有关参考书及三本数学百科全书中的有关条目([23]，[24]，[26]，特别是[26]的条目“代数数论[algebraic number theory]”)，书中不作介绍了.大学生应该养成参考阅读百科全书的习惯，这是很有益的.

本书所需要的预备知识是：初等数论(为方便起见，在第2章中不加证明地列出了它的主要内容)及高等代数中的多项式理论和线性代数知识(可参看[22]).仅在极个别的地方用到了一些微积分.各章配有数量不等的习题.

丁石孙教授和赵春来同志仔细了解了我们写这本书的想法和审阅了书稿，提出了宝贵的指导意见与许多具体修改意见.按照他们的意见，一一作了相应的修改、说明.对此我们表示衷心的感谢！本书的写作得到了高校科技基金的资助；山东大学出版社对本书的出版给予了大力支持；本书的责任编辑曹振坤同志不仅改正了书中不少笔误，而且提出了有益建议使本书更便于阅读，我们表示衷心的感谢！

我们两人对代数数论都没有研究，本书是我们教学体会的一点总结，缺点、错误在所难免，请大家指正.

潘承洞　潘承彪

1991年5月12日于山东大学

符　　号

以下是本书中常用的符号，未加特别说明时均按以下意义理解．不常用的符号在所用章节中说明．

$\mathbf{N}$	全体正整数(即自然数)1,2,3,…组成的集合
$\mathbf{Z}$	全体有理整数(即正、负整数及零) …,−3,−2,−1,0,1,2,3,…组成的集合
$\mathbf{Q}$	全体有理数组成的集合
$\mathbf{R}$	全体实数组成的集合
$\mathbf{C}$	全体复数组成的集合
$\{a\mid\cdots\}$	由满足条件"…"的元素 a 组成的集合
$a\in S$	元素 a 属于集合 S
$a\notin S$	元素 a 不属于集合 S
$S\cup T$	集合 S 与 T 的并集
$S\cap T$	集合 S 与 T 的交集
$S\subseteq T$	集合 T 包含 S,即 S 是 T 的子集
$S\subset T$	集合 T 包含 S,且 $S\neq T$,即 S 是 T 的真子集
命题 $U\Rightarrow$命题 V	命题 V 成立是命题 U 成立的必要条件,即由命题 U 成立可推出命题 V 成立
命题 $U\Leftarrow$命题 V	命题 V 成立是命题 U 成立的充分条件,即由命题 V 成立可推出命题 U 成立
命题 $U\Leftrightarrow$命题 V	命题 U 成立的必要和充分条件是命题 V 成立,即命题 U 和 V 等价
$a\mid b$	a 整除 b,见§2.1 定义 1,§3.1 定义 1 及§3.1 的几点说明(1)
$a\nmid b$	a 不整除 b,见§2.1 定义 1,§3.1 定义 1 及§3.1 的几点说明(1)
$(a,b,\cdots,c)$	$a,b,\cdots,c$ 的最大公因式数(式、元、…),见§2.1 定义 7,定义 7′,§3.1 定义 7 及§3.1 的几点说明(1)
$[a,b,\cdots,c]$	$a,b,\cdots,c$ 的最小公倍数(式、元、…)见§2.1 定义 8,定义 8′,§3.1 定义 8 及§3.1 的几点说明(1)

$[x]$	不超过实数 x 的最大整数
$b \equiv a \pmod{m}$	b 同余于 a 模 m，见 §1.3 的定理 1 之后，§2.2 定义 1，§3.2 定义 1 及 §6.1 定义 2
$b \not\equiv a \pmod{m}$	b 不同余于模 m，参见上一符号
$a \bmod m$	由所有同余于 a 模 m 的元素组成的集合，即剩余类（同余类），见 §1.3 定理 1 之后，§2.2 定义 2，§3.2 定义 2 及 §6.1 定义 3
$m\mathbf{Z}$	见 §1.4 例 2
$\mathbf{Z}_m$	见 §2.2 定义 2
$\mathbf{Z}_m^*$	见 §2.2 定义 4
$\varphi(m), \varphi(\mu), \varphi(\boldsymbol{a})$	Euler互素函数，见 §2.2 定义 4，§3.2 定义 4 及 §8.6定义 2
ρ_k	$e^{2\pi i/k}$，$k \in \mathbf{N}$
$\cong$	同构符号，见 §1.3 末例 9 前，§1.4 末
$((a))$，$((a_1, \cdots, a_r))$，$((V))$	理想符号，见 §1.6 的式(5)，(6)，(7)以及式(5)前的定义.通常理想符号用单括号$(\cdots)$，但也有用其他符号的(见参考文献[7]，[21])，这里为了表示理想和最大公因数的联系与区别，采用双括号$((\cdots))$
$M[x], M[x_1, \cdots, x_s]$	环 M 上的一元、多元多项式环，见 §1.4 例 4
$M(x), M(x_1, \cdots, x_s)$	整环 M 上的一元、多元多项式环的分式域，见 §1.7
$M(a_1, \cdots, a_s)$	整环 M 添加元素 $a_1, \cdots, a_s$ 生成的域，见 §1.5，§4.3 定义 1，注意符号 $\tilde{\mathbf{Q}}(a)$，$\tilde{\mathbf{Q}}(a_1, \cdots, a_s)$ 另有定义
$\mathbf{Q}_{(1)}[X], \mathbf{Z}_{(1)}[X]$	见 §4.1 开头
A	$\mathbf{Q}$ 上的全体代数数组成的集合，见 §4.1 定义 1 之后
$\tilde{A}$	$\mathbf{Q}$ 上的全体代数整数组成的集合，见 §4.1 定义 1 之后
A_n	$\mathbf{Q}$ 上的全体 n 次代数数组成的集合，见 §4.2 定义 1 之后
$\tilde{A}_n$	$A_n \cap \tilde{A}$
$\tilde{F}$	表示 $F \cap \tilde{A}$，F 是代数数域，见 §4.3 定义 8
$\tilde{\mathbf{Q}}(\alpha), \tilde{\mathbf{Q}}(\alpha_1, \cdots, \alpha_s)$	表示 $\mathbf{Q}(\alpha) \cap \tilde{A}$，$\tilde{\mathbf{Q}}(\alpha_1, \cdots, \alpha_s) \cap \tilde{A}$. 见 §4.3 定义 8
$T(\alpha), N(\alpha)$	见 §4.2 定义 2，但在 §3.3(见定义 1)及 §3.4(见定义 1)中另有含意
$T_\alpha(\theta), N_\alpha(\theta)$	见 §4.3 定义 3

$T_F(\theta), N_F(\theta)$	见 §4.3 式(9)
$H\{x_1, \cdots, x_n\}$	见 §4.3 定义 4
$[E:F]$	见 §4.3 定义 6
$\Delta(r_1, \cdots, r_n)$	见 §4.3 定义 7
$\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}, \cdots$	粗黑体小写拉丁字母,表示模,见 §6.1 定义 1
$X_{\boldsymbol{m}}, R_X(\boldsymbol{m}), R(\boldsymbol{m})$	见 §6.1 定义 3
$N(\boldsymbol{m})$	即 $R(\boldsymbol{m})$. 见 §8.6 定理 10 后的说明
$l_{\boldsymbol{m}}, R_l(\boldsymbol{m})$	见 §6.1 性质(7)之后
$\Delta(\boldsymbol{m}), \Delta(F), \Delta(\tilde{F})$	见 §6.2 定义 3

⊙目 录

第 1 章　群、环、域 …… 1

§1.1　自然数、有理整数、有理数 …… 1
§1.2　集合的二元运算、半群 …… 4
§1.3　群 …… 6
§1.4　环、整环、域 …… 13
§1.5　由子集生成的子环、子域 …… 19
§1.6　环的理想、商环 …… 22
§1.7　整环的分式域、环和域的扩张 …… 27
习题 …… 29

第 2 章　初等数论的基础知识 …… 37

§2.1　**Z** 中的整除 …… 37
§2.2　**Z** 中的同余 …… 43
§2.3　**Z** 中的 n 次剩余、剩余特征、积性特征 …… 49
习题 …… 53

第 3 章　整环中算术的基本知识 …… 56

§3.1　整环中的整除概念 …… 56
§3.2　整环中的同余概念 …… 65
§3.3　**Z**[i]中的算术 …… 74
§3.3A　**Z**[i]中的整除 …… 74
§3.3B　**Z**[i]中的剩余系 …… 81

§3.3C $\mathbf{Z}[i]$中的整除理论的应用 …… 83
§3.4 $\mathbf{Z}[\sqrt{-5}]$中的算术 …… 88
§3.5 $\mathbf{Z}[x]$中的算术 …… 91
§3.6 Euclid 整环 …… 98
习题 …… 102

第 4 章 代数数 …… 107

§4.1 代数数与代数整数 …… 107
§4.2 代数数的不可约多项式与次数 …… 113
§4.3 代数数域与代数整数环 …… 119
习题 …… 133

第 5 章 二次域的算术 …… 139

§5.1 基本性质 …… 139
§5.2 倍数集合及完全剩余系 …… 150
§5.3 二次 Euclid 域 …… 152
§5.4 几个不定方程 …… 159
§5.5 特征和 …… 164
§5.6 四次互反律 …… 169
§5.7 三次互反律 …… 188
习题 …… 196

第 6 章 代数数域的整基 …… 203

§6.1 模 …… 204
§6.2 模的维数和基 …… 209
§6.3 纯三次域 …… 223
§6.4 分圆域 …… 227
§6.5 Fermat 大定理(一) …… 236
习题 …… 242

第 7 章 代数数域的单位 …… 248

§7.1 单位定理(一) …… 248
§7.2 Minkowski 线性型定理 …… 254
§7.3 单位定理(二) …… 259
习题 …… 261

第 8 章　理想理论 …… 262

§8.1　一点说明 …… 262
§8.2　理想唯一分解定理(一) …… 266
§8.3　理想的进一步性质 …… 271
§8.4　理想唯一分解定理(二) …… 277
§8.5　理想的结构 …… 282
§8.6　对理想的同余 …… 284
§8.7　二次域的素理想 …… 291
习题 …… 296

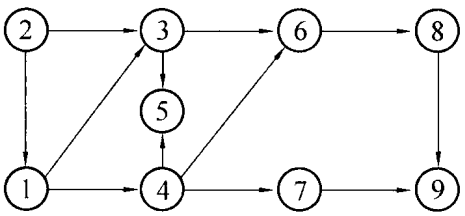
第 9 章　理想类群 …… 302

§9.1　理想类群 …… 303
§9.2　类数 …… 304
§9.3　多项式 $x^2 - x + m$ …… 310
§9.4　Fermat 大定理(二) …… 312
习题 …… 315

附表 …… 317

编辑手记 …… 320

参考文献 …… 324



各章之间的联系图

群、环、域

第 1 章

本章结合自然数 → 有理整数 → 有理数系的形成及初等数论知识,介绍群、环、域的概念及其最基本的知识,为讲述以后内容做必要准备.

§1.1 自然数、有理整数、有理数

由于计数的需要,人类逐步形成了**自然数**(即**正整数**)的概念及它们的运算.自然数记作

$$1,2,3,4,5,\cdots,n,\cdots \tag{1.1.1}$$

以 **N** 表示全体自然数组成的集合.Peano 公理(见本节末)刻画了自然数集合的本质属性.

自然数集合 **N** 中最简单的运算是加法"+":对任意的 n_1, $n_2 \in \mathbf{N}$,必有 $n \in \mathbf{N}$,使得

$$n = n_1 + n_2$$

但在 **N** 中不一定能进行加法的逆运算,即对任意的 $n, n_1 \in \mathbf{N}$,不一定有 $x \in \mathbf{N}$,使得

$$n = n_1 + x \tag{1.1.2}$$

如果这样的 x 存在,就记作

$$x = n - n_1$$

即 n, n_1(注意次序)可以作加法的逆运算 —— 减法"-".为了保证能进行加法的逆运算,就导致数零及负整数的引入.全体正、负整数及零就是通常所说的整数,为了以后避免混淆,我们称之为**有理整数**,即

$$\cdots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \cdots$$

全体有理整数组成的集合记作 $\mathbf{Z}$.在 $\mathbf{Z}$ 中不但可以作加法运算,而且也一定可以作它的逆运算 —— 减法,即对任意的 $n, n_1 \in \mathbf{Z}$,方程(1.1.2)必有解 $x \in \mathbf{Z}$.

自然数集合 $\mathbf{N}$ 中的另一基本运算是乘法"·",对任意的 $n_1, n_2 \in \mathbf{N}$,必有 $m \in \mathbf{N}$,使得

$$m = n_1 \cdot n_2$$

但在 $\mathbf{N}$ 中不一定能作乘法的逆运算,即对任意的 $m, n_1 \in \mathbf{N}$,不一定有 $x \in \mathbf{N}$,使得

$$m = n_1 \cdot x \tag{1.1.3}$$

如果这样的 x 存在,就记作

$$x = m \div n_1 \text{ 或 } m/n_1$$

即 m, n_1(注意次序)可以作乘法的逆运算 —— 除法"÷".为了保证在 $\mathbf{N}$ 中能进行乘法的逆运算,导致正分数即正有理数

$$a/b, a, b \in \mathbf{N}$$

的引入.全体正有理数组成的集合记作 $\mathbf{Q}^+$.在 $\mathbf{Q}^+$ 中一定能作乘法的逆运算,即对任意的 $m, n_1 \in \mathbf{Q}^+$,方程(1.1.3)必有解 $x \in \mathbf{Q}^+$.

这样,在 $\mathbf{Z}$ 中可作加法运算及其逆运算,$\mathbf{Z}$ 中也可作乘法运算,但不一定能进行乘法的逆运算;而在 $\mathbf{Q}^+$ 中,可作乘法及其逆运算,也可作加法运算,但不一定能作加法的逆运算.这是由于我们在上面仅对 $\mathbf{N}$ 中的一种运算 —— 加法或乘法 —— 单独考虑的结果.当在集合 $\mathbf{N}$ 中同时讨论两种运算 —— 加法和乘法时,就必须考虑这两种运算的关系,这就是熟知的分配律:对任意的 $a, b, c \in \mathbf{N}$,必有

$$a \cdot (b + c) = a \cdot b + a \cdot c \tag{1.1.4}$$

在引入**有理数**即分数

$$a/b, a, b \in \mathbf{Z}, b \neq 0$$

后,在全体有理数组成的集合 $\mathbf{Q}$ 中,就可以作加法和乘法运算,以及它们的逆运算(0不能做除数,即式(1.1.3)中的 $n_1 \neq 0$),而且保持分配律成立,即对任意的 $a, b, c \in \mathbf{Q}$,式(1.1.4)成立.

在 $\mathbf{Z}$ 和 $\mathbf{Q}$ 中还有一个重要的性质是:任意两个不为零的数相乘一定不等于零.

以上这些最简单、最基本,因而也是最重要的算术概念的极简单的回顾,反