Number Theory
—The First Chapters

数学·统计学系列

数论开篇

陆洪文　田廷彦　编著

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

07

数学·统计学系列

数论开篇

Number Theory——The First Chapters

陆洪文 田廷彦 编著

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

内容提要

本书为丛书中的第一部，涵盖了初等数论的大部分内容，包括整除、同余、数论函数、二次剩余和原根等，此外也涉及有限域的基本知识。本书内容精炼扼要，习题丰富（不少比较新颖或具有一定难度），另有5个附录供读者进一步研究。

本书适合大学理科师生、参加奥数比赛的高中生、教练员以及广大数学爱好者参考。

图书在版编目(CIP)数据

数论开篇/陆洪文，田廷彦编著. —哈尔滨：
哈尔滨工业大学出版社，2012.6
ISBN 978－7－5603－3611－4

Ⅰ.①数… Ⅱ.①陆… ②田… Ⅲ.①数论
Ⅳ.①O156

中国版本图书馆CIP数据核字(2012)第131434号

策划编辑 刘培杰 张永芹
责任编辑 王勇钢
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11.25 字数250千字
版 次 2012年6月第1版 2012年6月第1次印刷
书 号 ISBN 978－7－5603－3611－4
定 价 28.00元

序

数论，顾名思义，就是研究数的理论。数，原本只是指整数，甚至只是指自然数。随着研究的不断深入，数论研究的范围也不断扩张，起初是各个数域，即代数数域，到了20世纪后期，扩张到局部域和整体域，从整体上说，现代数论应该称为算术代数几何。21世纪以来，由于陶哲轩等人的研究，组合数论也有了长足的发展。

古代数论，在中国和古希腊都有很好的研究，例如，中国古代的《孙子算经》和秦九韶的《数书九章》关于“中国剩余定理”的研究，古希腊 Eratosthenes 和 Euclid 关于素数的研究、Pythagoras 学派关于无理数$\sqrt{2}$的研究以及 Diophantine 关于不定方程的研究都是古代数论的辉煌成就。

文艺复兴后，从17世纪开始，到18世纪，由于 Fermat，Euler，Lagrange，Legendre，Waring 的研究，渐渐奠定了近代数论的基础，特别要指出的是 Fermat 大定理和 Waring－Goldbach 问题大大地推动了数论的发展。

站在18世纪和19世纪之交的数学王子 Gauss，以他的 *Disquisitiones Arithemeticae*、素数定理、二元二次型、二次互反律以及 Gauss 和等，为数论建立了完整的理论，开辟了前进的方向。

在整个19世纪，数论有了巨大的发展，除Gauss以外，Galois，Riemann，Dedekind，Kummer，Jacobi，Chebyshev，Eisenstein，von Mangoldt，Hadamard，Kronecker，Möbius，de la Vallée Poussin，Hermite，Lindemann，Sylvester，Weber，Stickelberger，Frobenius，Minkowski等群星灿烂，建立了代数数论，Riemann Zeta函数的研究导致素数定理的证明，自然对数的底e和圆周率π的超越性的证明，模函数与模形式的开创性研究，Kronecker－Weber青春之梦的提出和证明等，成绩辉煌。

站在19世纪和20世纪之交的数学巨人Hilbert以其*Zahlbericht*统一了代数数论、数学23问题、类域论猜想与Waring问题的解决等引领数论的进一步发展。20世纪的数论成绩巨大。Hardy，Littlewood，Brun，Schnirelmann，Vinogradov，Linnik，Renyi，华罗庚，Bombieri，陈景润，王元，潘承洞关于Goldbach猜想的工作，离光辉的顶峰只有“一步之遥”；Takagi（高木贞治），E. Artin和Hasse等人完成了类域论；Poincaré，Fuchs，Klein，Hecke，Petersson，Rankin，Ramanujan，Siegel从19世纪末到20世纪前期完成了模形式、自守形式的理论；从20世纪60年代起，表示论和代数几何引入数论，Weil，Selberg，Taniyama，Shimura，Tate，Shafarevich，Birch，Swinnerton－Dyer，Deligne，Mazur，Faltings，Langlands，Maass，Wiles，Gross，Zagier，张寿武等人，分别提出或者证明了Weil猜想、Ramanujan－Petersson猜想（权大于1）、Mordell猜想、椭圆曲线T－S猜想、椭圆曲线BSD猜想、Langlands纲领、自守L函数特殊值的几何不变量表示式、虚二次数域的Gauss类数猜想直至Wiles证明了期待了350年的Fermat大定理。另外Thue，Siegel，Gelfond，Schneider，Baker，Roth，Mahler，Schmid等人对超越数和代数数的有理逼近作出巨大推进。

到了21世纪，刚刚过去的十年是数论的又一个辉煌的十年。Langlands纲领和算术代数几何百花齐放，Lafforgue和吴宝珠对Langlands纲领作出巨大推进。Terence Tao（陶哲轩）等证明了存在任意长的素数算术级数。

数论的应用也越来越广泛和深入，从电子通信、密码学、近似计算到准晶都可以发现数论越来越重要的作用。

本书只是数论的开篇，即为介绍最初步的数论而已。从20世纪70年代以来，作者一直在中国科技大学和同济大学教授初等数论这门课程，起初是向中国科技大学数学系一年级的本科生教授，后来又向同济大学电信学院一、二年级本科生教授。前者是作为数学的基础课，后者是作为电信学院的基础课。

在教学中，本书的内容只教授了一部分，但是作为数论的开篇，全部的内容似乎都应该知道。不论是大学数学系本科生，还是有关专业的本科生，本书对他们也都会有用。田廷彦先生毕业于上海交通大学数学系本科，是我多年的朋友。他对数论非常有兴趣，收罗很多初等数论的好习题。这次，他不但对本书

全面细致地进行了校对，特别要提出的是，他编写了附录，本书的多数习题也是他安排的，符号和名词的索引也出于他的劳动。因此作者对他特别致谢。

陆洪文

2012 年 6 月于上海同济大学

目　录

序　幕

——从自然数、整数、分数、有理数、实数和复数谈起

自然数

人类已经有一百多万年的历史了，在这一百多万年的人类进化史中，数字是人类智慧的最初的结晶. 数数，是每一个幼儿智慧开化的第一步，“一二三四五，上山打老虎”这个儿歌，我们每一个人都不会忘记. 这就是“自然数”引入每一个人的思维的第一步.

自然数的全体，记之为

$$\mathbb{N} \triangleq \{1,2,3,4,5,\cdots\}$$

在老子的《道德经》第四十二章，有下述的话：

道生一，一生二，二生三，三生万物.

秦始皇在统一中国、首登皇帝宝座之时，说：

朕为始皇帝. 后世以计数，二世三世至于万世，传之无穷.

“愚公移山”中的愚公在回答智叟的疑问时，说：

虽我之死，有子存焉；子又生孙，孙又生子；

子又有子，子又有孙；子子孙孙无穷匮也.

上述中国古代的人物都是说：第一代生第二代，第二代生第三代，第三代生第四代，等. 上一代生下一代，生生不息，以至无穷. 这就是自然数的思想.

著名的德国数学家克罗内克(L. Kronecker，1823—1891) 曾有一个高论：

上帝创造了自然数，其余的一切都是人做的.

著名意大利数学家皮亚诺(G. Peano，1858—1932) 于1889年明确提出了关于自然数的皮亚诺公理：

1. 1是自然数.

2. 每一个确定的自然数a，都有一个确定的后继数a'，a'也是自然数(一个数的后继数就是紧接在这个数后面的数. 例如，1的后继数是2，2的后继数是3等).

3. 如果自然数b，c的后继数都是自然数a，那么$b=c$.

4. 1不是任何自然数的后继数.

5. 任意关于自然数的命题，如果证明了它对自然数1是对的，又假定它对自然数n为真时，可以证明它对n的后继数n'也真，那么，命题对所有自然数都

真.(这条公理保证了数学归纳法的正确性)

(若将0也视做自然数,则公理中的1要换成0.在本书中,不将0视做自然数)这个公理把前面的通俗说法,在数学上严格化了.也可以把一个自然数的后继形象化地称为其下一代.

由这个公理,可以定义自然数的加法,自然数 m 和自然数 n 的和,即自然数 m 加自然数 n,定义为 m 的第 n 代,记之为 $m+n$.用第5条公理,可以证明 $m+n=n+m$,即自然数的加法是交换的.当然也可以证明自然数的加法是结合的,即任意三个自然数 m,n 和 k,均有 $(m+n)+k=m+(n+k)$.

还可以定义自然数的乘法,自然数 m 和自然数 n 的积,即自然数 m 乘自然数 n,定义为

$$m\times n \triangleq \underbrace{n+\cdots+n}_{m\text{个}}$$

可以证明自然数的乘法是交换的和结合的.

整数

人类历史的发展,又引进了负数和零,从而得到了全体整数的集合

$$\mathbb{Z} \triangleq \{0,\pm1,\pm2,\pm3,\pm4,\pm5,\cdots\} \triangleq \{\pm n \mid n\in\mathbb{N}\}\cup\{0\}$$

整数集 $\mathbb{Z}$ 中,可以定义加法、减法和乘法,这些运算满足以下的法则($\mathbb{Z}1\sim\mathbb{Z}11$):

$\mathbb{Z}$ 一.整数集 $\mathbb{Z}$ 在加法下,构成了一个以"0"为加法恒等元的加法群,具体来说,有:

$\mathbb{Z}1.\ \forall m,n\in\mathbb{Z},\ m+n\in\mathbb{Z}$.

$\mathbb{Z}2.$ 加法满足交换律,即 $\forall m,n\in\mathbb{Z},m+n=n+m$.

$\mathbb{Z}3.$ 加法满足结合律,即 $\forall m,n,k\in\mathbb{Z},(m+n)+k=m+(n+k)$,这个共同值记之为 $m+n+k$.

$\mathbb{Z}4.$ "0"为加法恒等元,即 $\forall m\in\mathbb{Z},\ m+0=0+m$.

$\mathbb{Z}5.$ 负元的存在性,即 $\forall m\in\mathbb{Z},\exists n\in\mathbb{Z}$,使得 $m+n=n+m=0$.这个 n,称为 m 的负元,记之为 $n=-m$. m 的负元是唯一的.

由加法的上述法则,减法的定义为:$\forall m,n\in\mathbb{Z},m-n\triangleq m+(-n)$.由此,可以证明减法是加法的逆运算.

$\mathbb{Z}$ 二.整数集 $\mathbb{Z}$ 的乘法满足:

$\mathbb{Z}6.\ \forall m,n\in\mathbb{Z},m\times n\in\mathbb{Z}$,$m\times n$ 简记为 mn;对 $m\times n\in\mathbb{N}$,$m\times(-n)=-mn$,$(-m)\times n=-mn$,以及 $(-m)\times(-n)=mn$.

$\mathbb{Z}7.$ 乘法满足交换律,即 $\forall m,n\in\mathbb{Z},\ mn=nm$.

$\mathbb{Z}$8. 乘法满足结合律，即 $\forall m,n,k \in \mathbb{Z}$，$m(nk)=(mn)k$，这个共同值记之为 mnk.

$\mathbb{Z}$9. “1”为乘法恒等元，即 $\forall m \in \mathbb{Z}$，$1\times m=m\times 1=m$.

$\mathbb{Z}$10. 加法与乘法之间满足分配律，即 $\forall m,n,k \in \mathbb{Z}$，$(m+n)\times k=mk+nk$.

$\mathbb{Z}$11. $\forall m \in \mathbb{Z}$，$0\times m=m\times 0=0$.

由此，我们称 $\mathbb{Z}$ 为整数环，更精密些，称 $\mathbb{Z}$ 为有理整数环.

分数或者有理数

在人们发生分配问题时，又引入了分数，也就是“有理数”，得到全体有理数的集合

$$\mathbb{Q} \triangleq \left\{ \frac{m}{n} \mid m,n \in \mathbb{Z}, n \neq 0 \right\}$$

而且对

$$\frac{m}{n},\frac{k}{l} \in \mathbb{Q},\ \frac{m}{n}=\frac{k}{l} \Leftrightarrow ml=kn \quad (nl \neq 0)$$

对分数 $\frac{m}{n} \in \mathbb{Q}$，$m$ 称为分子，n 称为分母；用 $m \triangleq \frac{m}{1}$，就可以把 $\mathbb{Z}$ 嵌入 $\mathbb{Q}$，即整数 m 是分子为 m、而分母为 1 的分数.

有理数之间有四则运算，但是除数不能是零，在这些运算下，全体有理数的集合 $\mathbb{Q}$ 构成了一个有理数域，具体来说，有：

$\mathbb{Q}$ 一. $\mathbb{Q}$ 在加法下，构成了一个以“0”为加法恒等元的加法群，具体来说，有：

$\mathbb{Q}$1. $\forall \frac{m}{n},\frac{k}{l} \in \mathbb{Q}$，$\frac{m}{n}+\frac{k}{l} \triangleq \frac{ml+nk}{nl} \in \mathbb{Q}$.

$\mathbb{Q}$2. 加法满足交换律，即 $\forall \frac{m}{n},\frac{k}{l} \in \mathbb{Q}$，$\frac{m}{n}+\frac{k}{l}=\frac{k}{l}+\frac{m}{n}$.

$\mathbb{Q}$3. 加法满足结合律，即 $\forall \frac{m}{n},\frac{k}{l},\frac{u}{v} \in \mathbb{Q}$，$\frac{m}{n}+\left(\frac{k}{l}+\frac{u}{v}\right)=\left(\frac{m}{n}+\frac{k}{l}\right)+\frac{u}{v}$，这个共同值记之为 $\frac{m}{n}+\frac{k}{l}+\frac{u}{v}$.

$\mathbb{Q}$4. “0”为加法恒等元，即 $\forall \frac{m}{n} \in \mathbb{Q}$，$\frac{m}{n}+0=0+\frac{m}{n}=\frac{m}{n}$.

$\mathbb{Q}$5. 负元的存在性，即 $\forall \frac{m}{n} \in \mathbb{Q}$，$\exists \frac{k}{l} \in \mathbb{Q}$，使得 $\frac{m}{n}+\frac{k}{l}=\frac{k}{l}+\frac{m}{n}=0$. 这个 $\frac{k}{l}$，称为 $\frac{m}{n}$ 的负元，记之为 $\frac{k}{l}=-\frac{m}{n}$. $\frac{m}{n}$ 的负元是唯一的：$-\frac{m}{n}=\frac{-m}{n}$.

由加法的上述法则，减法的定义为：$\forall\ \frac{m}{n},\frac{k}{l}\in\mathbb{Q}$，$\frac{m}{n}-\frac{k}{l}\triangleq\frac{m}{n}+\left(-\frac{k}{l}\right)\triangleq\frac{ml-nk}{nl}$. 由此，可以证明减法是加法的逆运算.

$\mathbb{Q}$ 二. 全体非零有理数的集合

$$\mathbb{Q}^*\triangleq\{r\in\mathbb{Q}\mid r\neq 0\}$$

在乘法下，构成了一个以“1”为乘法恒等元的交换的乘法群，具体来说，有：

$\mathbb{Q}6.\ \forall\ \frac{m}{n},\frac{k}{l}\in\mathbb{Q}$，$\frac{m}{n}\times\frac{k}{l}\triangleq\frac{mn}{nl}\in\mathbb{Q}$.

$\mathbb{Q}7.$ 乘法满足交换律，即 $\forall r,s\in\mathbb{Q}$，$r\times s=s\times r$；$r\times s$ 简记为 rs.

$\mathbb{Q}8.$ 乘法满足结合律，即 $\forall r,s,t\in\mathbb{Q}$，$r(st)=(rs)t$，这个共同值，记之为 rst.

$\mathbb{Q}9.$ “1”为乘法恒等元，即 $\forall r\in\mathbb{Q}$，$r\times 1=1\times r=r$.

$\mathbb{Q}10.$ 乘法逆元，简称为逆元的存在性，即 $\forall r\in\mathbb{Q}^*$，$\exists s\in\mathbb{Q}^*$，使得 $rs=sr=1$；这个非零的有理数 s 称为有理数 r 的逆元，记之为 $s=r^{-1}$；$r=\frac{m}{n}\in\mathbb{Q}^*$ 的逆元是唯一的：$r^{-1}=\frac{n}{m}\in\mathbb{Q}^*$.

以上 $\mathbb{Q}6\sim\mathbb{Q}9$ 中的 $\mathbb{Q}$，严格来说应该是 $\mathbb{Q}^*$，但是它们对 $\mathbb{Q}$ 也同样成立. $\mathbb{Q}^*$ 称为 $\mathbb{Q}$ 的乘法群.

由乘法的上述法则，除法的定义为：$\forall r,s\in\mathbb{Q}$，$r\neq 0$，$s\div r\triangleq\frac{s}{r}\triangleq s\times r^{-1}$. 由此，可以证明除法是乘法的逆运算.

$\mathbb{Q}$ 三. 加法与乘法之间满足分配律，即：

$\mathbb{Q}11.\ \forall r,s,t\in\mathbb{Q}$，$r(s+t)=rs+rt$；它的一个值得特别提出的推论是

$\mathbb{Q}12.\ \forall r\in\mathbb{Q}$，$0\times r=r\times 0=0$.

上述的“群、环、域”的称呼，针对的是非常具体的整数与分数，将来，我们会更一般化地来进行阐述和运用.

实数域 $\mathbb{R}$

一个无穷的有理数列

$$\{r_n\}\triangleq\{r_n\in\mathbb{Q}\mid 1\leqslant n<\infty\}\triangleq\{r_n\}_1^\infty\triangleq r_1,r_2,r_3,\cdots,r_n,\cdots$$

称为是一个柯西序列(Cauchy Sequence)，如果对任给的(任意小的)正有理数 $\varepsilon>0$，均 $\exists N=N(\varepsilon)\in\mathbb{N}$，使得

$$|r_n-r_m|<\varepsilon\quad\text{当 } n,m>N$$

这里，$|r|$ 是 r 的绝对值.

两个有理数柯西序列$\{r_n\}$，$\{s_n\}$称为等同，记之为$\{r_n\} \equiv \{s_n\}$，如果对任给的(任意小的)正有理数$\varepsilon > 0$，均$\exists N = N(\varepsilon) \in \mathbb{N}$，使得

$$|r_n - s_n| < \varepsilon \quad 当 n > N$$

这个等同关系具有自反性、对称性和传递性，于是所有的有理数柯西序列在这个等同关系下，被分成了一些有理数柯西序列等同类，每一个这样的类，就被称为实数.

把有理数r等同于有理数柯西序列$\{r_n\}$(这里，$r_n \equiv r, \forall n \in \mathbb{N}$)所在的类. 所以有理数也是实数.

实数的四则运算

以《$\{r_n\}$》记有理数柯西序列$\{r_n\}$所在的有理数柯西序列等同类，则实数《$\{r_n\}$》与实数《$\{s_n\}$》的和、差、积定义为

$$和：《\{r_n\}》+《\{s_n\}》\triangleq《\{r_n\}+\{s_n\}》\triangleq《\{r_n+s_n\}》$$

$$差：《\{r_n\}》-《\{s_n\}》\triangleq《\{r_n\}-\{s_n\}》\triangleq《\{r_n-s_n\}》$$

$$积：《\{r_n\}》\times《\{s_n\}》\triangleq《\{r_n\}\times\{s_n\}》\triangleq《\{r_n\times s_n\}》$$

为定义除法，首先容易知道：

《$\{r_n\}$》$\neq 0$，当且仅当在有理数柯西序列等同类《$\{r_n\}$》中存在一个有理数柯西序列$\{r_n\}$使得$r_n \neq 0, \forall n \in \mathbb{N}$，不妨设所取的有理数柯西序列$\{r_n\}$就满足这个要求.

当实数《$\{r_n\}$》$\neq 0$时，实数《$\{s_n\}$》可以被《$\{r_n\}$》除，并定义为

$$《\{s_n\}》\div《\{r_n\}》\triangleq《\{s_n r_n^{-1}\}》$$

以$\mathbb{R}$记全体有理数柯西序列等同类的集合，则它在上述四则运算下构成了一个域，称之为实数域，具体的有如下的($\mathbb{R}1 \sim \mathbb{R}12$)：

$\mathbb{R}$一. $\mathbb{R}$在加法下，构成了一个以“0”为加法恒等元的加法群，具体来说，有：

$\mathbb{R}1$. 加法封闭性：$\forall \alpha, \beta \in \mathbb{R}, \alpha + \beta \in \mathbb{R}$.

$\mathbb{R}2$. 满足加法交换律.

$\mathbb{R}3$. 满足加法结合律.

$\mathbb{R}4$. “0”为加法恒等元.

$\mathbb{R}5$. 负元的存在性：即$\forall \alpha = 《\{r_n\}》 \in \mathbb{R}$，$\exists \beta = 《\{-r_n\}》 \in \mathbb{R}$，使得$\alpha + \beta = 0$. 这个$\beta$称为$\alpha$的负元，记之为$\beta = -\alpha$. α的负元是唯一的. 由此，可以证明减法是加法的逆运算.

$\mathbb{R}$二. 全体非零实数的集合

$$\mathbb{R}^* \triangleq \{\alpha \in \mathbb{R} \mid \alpha \neq 0\}$$

在乘法下，构成了一个以“1”为乘法恒等元的交换的乘法群，具体来说，

有：

$\mathbb{R}6$. $\mathbb{R}$ 在乘法下封闭，即 $\forall \alpha,\beta \in \mathbb{R}, \alpha \times \beta \in \mathbb{R}$.

$\mathbb{R}7$. 乘法满足交换律，即 $\forall \alpha,\beta \in \mathbb{R}, \alpha \times \beta = \beta \times \alpha$；$\alpha \times \beta$ 简记为 $\alpha\beta$.

$\mathbb{R}8$. 乘法满足结合律，即 $\forall \alpha,\beta,\gamma \in \mathbb{R}, \alpha(\beta\gamma) = (\alpha\beta)\gamma$，这个共同值记之为 $\alpha\beta\gamma$.

$\mathbb{R}9$. “1”为乘法恒等元，即 $\forall \alpha \in \mathbb{R}, \alpha \times 1 = 1 \times \alpha = \alpha$.

$\mathbb{R}10$. 乘法逆元，简称为逆元的存在性，即 $\forall \alpha \in \mathbb{R}^*, \exists \beta \in \mathbb{R}^*$，使得 $\alpha\beta = \beta\alpha = 1$. 这个非零的实数 β 称为非零实数 α 的逆元，记之为 $\beta = \alpha^{-1}$；$\alpha \in \mathbb{R}^*$ 的逆元是唯一的.

以上 $\mathbb{R}6 \sim \mathbb{R}9$ 中的 $\mathbb{R}$，严格来说应该是 $\mathbb{R}^*$，但是它们对 $\mathbb{R}$ 也同样成立. $\mathbb{R}^*$ 称为 $\mathbb{R}$ 的乘法群.

由乘法的上述法则，除法的定义为：$\forall \alpha,\beta \in \mathbb{R}, \beta \neq 0, \alpha \div \beta \triangleq \alpha \times \beta^{-1}$. 由此，可以证明除法是乘法的逆运算.

$\mathbb{R}$ 三. 加法与乘法之间满足分配律，即：

$\mathbb{R}11$. $\forall \alpha,\beta,\gamma \in \mathbb{R}$，$\alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma$；它的一个值得特别提出的推论是

$\mathbb{R}12$. $\forall \alpha \in \mathbb{R}, \alpha \times 0 = 0 \times \alpha = 0$.

用极限的说法，有理数柯西序列等同类即为有理数柯西序列的极限，即

$$\langle\langle \{r_n\} \rangle\rangle \triangleq \lim_{n\to\infty} r_n$$

也就是说，一个实数即是定义它的有理数柯西序列的极限. 在这个意义下，实数域是完备的，亦即实数的柯西序列的极限一定是某个有理数柯西序列的极限.

复数与复数域

全体复数构成的复数域

$$\mathbb{C} \triangleq \{a + b\mathrm{i} \mid a,b \in \mathbb{R}\}$$

这里 $\mathrm{i} = \sqrt{-1}$ 称为虚数单位.

对 $\alpha = a + b\mathrm{i}, \beta = c + d\mathrm{i} \in \mathbb{C}$，定义它们的加法与乘法为

$$\alpha + \beta = (a + c) + (b + d)\mathrm{i}, \text{与 } \alpha \times \beta = (ac - bd) + (ad + bc)\mathrm{i}$$

$\alpha = a + b\mathrm{i} = 0 \Leftrightarrow a = b = 0$. 对 $\alpha = a + b\mathrm{i} \in \mathbb{C}$，当 $b = 0$ 时，α 就是实数 a 了.

$\mathbb{C}$ 之所以成为一个域，与前面一样，是因为（$\mathbb{C}1 \sim \mathbb{C}3$）：

$\mathbb{C}1$. $\mathbb{C}$ 在加法下，构成了一个以“0”为加法恒等元的加法群.

$\mathbb{C}2$. $\mathbb{C}^* \triangleq \{\alpha \in \mathbb{C} \mid \alpha \neq 0\}$ 在乘法下，构成了一个以“1”为乘法恒等元的交换的乘法群，$\mathbb{C}^*$ 称为复数域 $\mathbb{C}$ 的乘法群.

$\mathbb{C}3$. $\mathbb{C}$ 的加法与乘法之间满足分配律.

以上可以参考 Edmund Landau 的著作 *Foundations of Analysis*.

数论本来只是关于整数的理论，所以它的英文是 Number Theory. 但是20世纪以来的发展，数论几乎无所不包. 我们的《数论开篇》基本上只讨论整数和有理数，有时也涉及实数和复数，在第二章我们将引进素有限域，而在最后一章我们还要介绍一般的有限域.

为了以后引用的方便，在此，我们把上述有理数域、实数域、复数域的概念进行推广. 一个集合 F，称为一个域，如果它满足下列的条件(1 ～ 5)：

1. F 至少有两个不同的元素：0 与 1；

2. 在 F 中定义了一个加法运算 $+$，在加法运算 $+$ 之下，F 是一个以 0 为加法恒等元的加法群，具体来说，F 满足下列条件(2.1 ～ 2.5)：

2.1. $\forall a,b \in F$，$a+b \in F$.

2.2. $\forall a,b \in F$，$a+b=b+a$，这称为加法交换律.

2.3. $\forall a,b,c \in F$，$(a+b)+c=a+(b+c)$，这个共同值记之为 $a+b+c$，这称为加法结合律.

2.4. $\forall a \in F$，$a+0=0+a=a$，这就是 0 称为加法恒等元的含义，可以证明加法恒等元是唯一的.

2.5. $\forall a \in F$，有 $b \in F$，使得 $a+b=b+a=0$，对每一个固定的 $a \in F$，具有这种性质的元素 b 是唯一的，称为 a 的负元，记之为 $b=-a$.

3. 在 F 中定义了一个乘法运算 $\times$，集合 $F^* \triangleq F\backslash\{0\}$（即 F 去掉元素 0 所得的集合）在乘法下是一个以 1 为乘法恒等元的交换的乘法群，具体来说，F 满足下列条件(3.1 ～ 3.5)：

3.1. $\forall a,b \in F$，$a \times b \in F$，以后我们为简洁计，往往把乘号“$\times$”省略.

3.2. $\forall a,b \in F$，$ab=ba$，这称为乘法交换律.

3.3. $\forall a,b,c \in F$，$(ab)c=a(bc)$，这个共同值记之为 abc，这称为乘法结合律.

3.4. $\forall a \in F$，有 $1 \times a=a \times 1=a$，这就是 1 称为乘法恒等元的含义，可以证明乘法恒等元是唯一的.

3.5. $\forall a \in F^*$，有 $b \in F^*$，使得 $ab=ba=1$，对每一个 $a \in F^*$，具有这种性质的元素 b 是唯一的，称为 a 的乘法逆元，简称为逆元，记之为 $b=a^{-1}$.

4. 加法与乘法之间满足分配律：$\forall a,b,c \in F$，$(a+b)c=ac+bc$.

5. $\forall a \in F$，有 $0 \times a=a \times 0=0$.

用通俗的话来说，就是域 F 具有四则运算：加、减、乘、除，但是“除数”不能是“0”(零)，并且符合通常的那些规则(如上述 1 ～ 5 所表述的).

算术基本定理(整数的唯一素因子分解定理)

第一章

1.1 可除性与带余除法

整数除整数不一定得出整数,因此有下列的**带余除法**.

定理 1.1 设 $a,b\in\mathbb{Z},b>0$,那么 $\exists q,r\in\mathbb{Z}$,使得

$$a=bq+r\quad 0\leqslant r\leqslant b-1$$

而且这对整数 q,r 为上述 a,b 所唯一确定.

证明 整个实数轴被无穷多个左闭右开长度均为 b 的小区间

$$[nb,(n+1)b)\quad n\in\mathbb{Z}$$

既无重复又无遗漏地占据着,因此作为实数之一的 a 必定落在这些小区间的某一个之中,也就是说,$\exists q\in\mathbb{Z}$,使得 $qb\leqslant a<(q+1)b$. 令 $r=a-bq$,则 $0\leqslant r<b$,又因为 r 是一个整数,所以 $r\leqslant b-1$. 另外,q 的唯一性由 a 所在小区间唯一确定而得出,从而也得出 r 的唯一性. 于是定理得证.

定义 1.1 定理中的 q 称为用 b 去除 a 所得的商,r 称为用 b 去除 a 所得的余数.

定义 1.2 设 $a,b\in\mathbb{Z},b\neq 0$,当存在 $\exists q\in\mathbb{Z}$,使得 $a=bq$,即用 b 去除 a 所得的余数是零,则称 b 除尽 a,也称 b 整

除 a,a 被 b 除尽,a 被 b 整除,并称 b 是 a 的因子(约数),记为 $b \mid a$. a 称为是 b 的倍数. 否则,即这种使得 $a=bq$ 成立的整数 q 不存在,就称 b 除不尽 a,记为 $b \nmid a$.

注记 通常我们只考虑正因子,即只考虑因子 $b>0$ 的情况,除非有特别的声明.

下面的定理显然成立:

定理 1.2

(1) 设 $a,b,d \in \mathbb{Z}$,$d \neq 0$,而 $d \mid a$,$d \mid b$,则 $\forall m,n \in \mathbb{Z}$,$d \mid am+bn$.

(2) 设 $a,b,c \in \mathbb{Z}$,$ab \neq 0$,而 $a \mid b$,$b \mid c$,则 $a \mid c$.

(3) 设 $a,b \in \mathbb{Z}$,$ab \neq 0$,而 $b \mid a$,则 $|b| \leqslant |a|$.

1.2 最大公因子、Euclid 算法与最小公倍数

最大公因子与 Euclid 算法

定义 1.3 对两个不全为零的整数 a,b,如果一个整数 d 既是 a 的因子(约数)也是 b 的因子,则 d 称为 a,b 的公因子. 由定理 1.2 的(3),可知 a,b 的公因子只有有限个,我们称最大的那一个为 a,b 的最大公因子,记为 g. c. d(a,b),在不发生歧义的时候,简记为 (a,b),它显然是一个正整数.

我们有

定理 1.3 对两个不全为零的整数 a,b,有

$$\text{g. c. d}(a,b)=\min\{ax+by \mid x,y \in \mathbb{Z},ax+by>0\}$$

注记 这里我们强调一下:这个定理表明,a 与 b 的最大公因子可以由 a,b 整系数线性表出,而且是可以由 a,b 整系数线性表出的最小正整数.

证明 令

$$d=\min\{ax+by \mid x,y \in \mathbb{Z},ax+by>0\}$$

d 当然是一个正整数. 于是有两个整数 s,t,使得 $d=as+bt$. 现在我们用 d 来除 a. 由带余除法(即定理 1.1),我们有 $q,r \in \mathbb{Z}$,使得 $a=dq+r$,$0 \leqslant r \leqslant d-1$. 我们断定 $r=0$. 假定 $1 \leqslant r \leqslant d-1$,则由 $r=a-dq=a(1-sq)+b(-tq)$,可知

$$r \in \{ax+by \mid x,y \in \mathbb{Z},ax+by>0\}$$

但是 $1 \leqslant r \leqslant d-1$,这与 d 的最小性矛盾. 因此,$r=0$,即 $d \mid a$. 同理 $d \mid b$. 于是 d 是 a,b 的一个公因子. 这样,我们有

$$d \leqslant \text{g. c. d}(a,b) \tag{1.1}$$

另一方面,令 $D \triangleq \text{g. c. d}(a,b)$,则 D 作为 a,b 的一个公因子,$D \mid a$ 且 $D \mid b$,而