基础数学丛书

整数与多项式

Integers and Polynomials

● 冯克勤　余红兵　编著

$$a = bq + r$$

$$n = \varepsilon p_1^{a_1} \cdots p_k^{a_k}$$

$$a \equiv b \pmod{m}$$

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

$$\Phi_n(x) = \prod_{\substack{k=1 \\ (k,n)=1}}^{n} (x - \zeta^k)$$

CHEP
高等教育出版社

Springer
施普林格出版社

(京) 112 号

图书在版编目(CIP)数据

整数与多项式 / 冯克勤，余红兵 编著. — 北京：高等教育出版社；海德堡：施普林格出版社，1999

ISBN 7-04-007890-2

Ⅰ. 整… Ⅱ. ① 冯… ② 余… Ⅲ. ① 整数 ② 多项式 Ⅳ. 0121.1

中国版本图书馆 CIP 数据核字(1999)第 41499 号

书　　名 整数与多项式
作　　者 冯克勤　余红兵

出版发行 高等教育出版社　施普林格出版社
社　　址 北京市东城区沙滩后街 55 号　**邮政编码** 100009
电　　话 010—64054588　**传　　真** 010—64014048
网　　址 http://www.hep.edu.cn

经　　销 新华书店北京发行所
印　　刷 北京民族印刷厂

开　　本 880×1230　1/32　**版　　次** 1999 年 10 月第 1 版
印　　张 6.5　**印　　次** 1999 年 10 月第 1 次印刷
字　　数 190 000　**定　　价** 15.00 元

序

整数(论),也称为初等数论,主要研究整数性质和方程(组)的整数解;多项式,则是代数学中一个非常基本的研究对象.

整数和多项式,初看起来,彼此并不相同,但两者有许多共同的,以及可以类比的内容.特别地,整数和多项式中许多概念、结果和方法,是近世代数中抽象概念的非常基本的模型和源泉.此外,由于计算机科学和数字通信技术的飞速进步,包括数论和代数学在内的广义离散数学得到了广泛和深入的应用.无论培养数学研究人材,还是培养数学应用人材,大学的数论和代数教学都应当有所加强.

中国科学技术大学从 1977 年起为数学系一年级学生开设了初等数论必修基础课.本书是在二十余年教学经验基础上,由原讲义改写而成.编写本书主要有两个目的:一个是较为系统地讲授整数和多项式理论的基本知识;另一个是为学习近世代数(群、环、域)提供具体的素材和实例,所以书中比较注重培养学生的代数学观点,表现整数理论与多项式理论的联系和相似之处.根据教学实践,我们相信,这样作对于培养学生抽象思考能力和代数学的思想方法,都是有好处的.

本书的主体为两个部分.第一部分的五章(共十四节)讲述整数的基础知识;第二部分的四章(共十二节)讲述多项式;另有一章作为附录,简要介绍本书内容在数字通信的信息安全方面的一些应用.根据以往的经验,作为一学期每周三(或四)学时的教材内容,可删去第 14 节,第 18 节和第 23 节不讲.

本书中每一节都配有少量的习题,其中较为基本的则标有"*"号.书末给出了部分习题的提示和注释,供读者参考.

作者感谢中国科学技术大学数学系的程艺教授、李尚志教授对编写本书的支持和鼓励；感谢单墫教授、李克正教授对本书写作提出的建议；感谢高等教育出版社徐可先生对本书出版的大力帮助；最后，我们感谢余华敏小姐耐心地打印了本书的初稿.

作 者

一九九九年五月

目　录

第一部分　整　数

第二部分 多 项 式

引　言

1. 正整数与整数. 正整数，也叫作自然数，就是我们熟知的

$$1, 2, 3, \cdots.$$

正整数的集合记作 **N**. 正整数的形成源于经验，其公理化定义是由皮亚诺(Peano) 作出的，这里不作讨论. 我们只提及(没有证明) 正整数的一些基本性质.

正整数中可以作**加法运算**：对任意 $a, b \in \mathbf{N}$，有唯一确定的正整数，称为 a 与 b 的和，记作 $a + b$，具有下面的运算规律

(1) 加法结合律　$(a + b) + c = a + (b + c)$；
(2) 加法交换律　$a + b = b + a$.

正整数中还可作**乘法运算**：对任意 $a, b \in \mathbf{N}$，有唯一确定的正整数，称为 a 与 b 的积，记作 $a \cdot b$(或 ab)，具有下面的运算规律

(3) 乘法结合律　$(ab) \cdot c = a \cdot (bc)$；
(4) 乘法交换律　$ab = ba$；
(5) $1 \cdot a = a \cdot 1 = a$；
(6) 分配律　$a(b + c) = ab + ac$.

正整数中有**大小**(即顺序) 关系. 如果 $a = b + c (c \in \mathbf{N})$，则记作 $a > b$ 或 $b < a$. 可以证明，对任意两个数 a, b，三个关系

(7) $a < b$，　$a = b$，　$a > b$

中，有且仅有一个成立；并且

(8) 由 $a<b, b<c$ 推出 $a<c$；

(9) 由 $a<b$ 推出 $a+c<b+c$；

(10) 由 $a<b$ 推出 $ac<bc$.

正整数的最重要，最本质的性质是下面的

归纳公理 设 $S \subseteq \mathbf{N}$，满足条件(i) $1 \in S$；(ii) 如果 $n \in S$，则 $n+1 \in S$. 那么 $S=\mathbf{N}$.

归纳公理是我们常用的数学归纳法的基础.

定理 1 设 $P(n)$ 是关于正整数的一个命题. 如果

(i) 当 $n=1$ 时，$P(1)$ 成立；

(ii) 由 $P(n)$ 成立可推出 $P(n+1)$ 成立.

则 $P(n)$ 对所有正整数 n 都成立.

由归纳公理还可推出正整数的下面两个非常基本的性质：

定理 2(最小数原理) 设 T 是 $\mathbf{N}$ 的一个非空子集. 则必有 $t_0 \in T$，使得对任意 $t \in T$ 有 $t_0 \leqslant t$，即 t_0 是 T 中的最小正整数.

定理 3(最大数原理) 设 T 是 $\mathbf{N}$ 的一个非空子集. 若 T 有上界，即存在正整数 m，使得对任意 $t \in T$ 有 $t \leqslant m$. 那么，必有 $t_0 \in T$，使得对任意 $t \in T$ 有 $t \leqslant t_0$，即 t_0 是 T 中的最大正整数.

用最小数原理可以证明下面的第二数学归纳法.

定理 4 设 $P(n)$ 是关于正整数 n 的一个命题. 如果

(i) 当 $n=1$ 时，$P(1)$ 成立；

(ii) 设 $n>1$，由 $P(k)$ 对所有正整数 $k<n$ 成立，可推出 $P(n)$ 成立.

则 $P(n)$ 对所有正整数 n 成立.

通过引入记号 0(零) 及 $-a$ 可将正整数扩充为整数. 整数的集合记作 **Z**.

Z 上可定义加法与乘法. 对于加法，它适合运算规律(1)，(2)；并且，数 0 满足 $0+a=a+0=a$；以及，对每个 $a\in\mathbf{Z}$ 有唯一的 $x\in\mathbf{Z}$，使 $a+x=0$，将 x 记作 $-a$. 于是，对任意 $a,b\in\mathbf{Z}$，方程 $a+x=b$ 在 **Z** 中有唯一的解，这个解记作 $b-a$，即 **Z** 中可以作加法的逆运算——减法. 在代数学中，我们将可作加、减运算，并且适合上述运算规律的集合称为**加法群**. 因此，**Z** 是一个加法群.

Z 中的乘法适合运算规律(3)，(4)，(5)，(6). 我们将既能作加、减运算，还能作上述乘法运算的集合，称为(**交换**) **环**. 注意，对于乘法，$0\cdot a=0$；并且 $ab=0$ 当且仅当 $a=0$ 或者 $b=0$. 具有这种性质的环，称作**无零因子环**. 因此 **Z** 是一个无零因子环，从而其中(乘法) 消去律成立. (我们在第二章中将遇到与此不同的环.)

整数中也有**大小**(顺序) 的概念，它适合规律(7)，(8)，(9) 以及(10) 当 $c>0$.

整数中还引入了**绝对值**的概念：

$$|a|=\begin{cases}a, & a\in\mathbf{N},\\ 0, & a=0,\\ -a, & -a\in\mathbf{N}.\end{cases}$$

因此，$|a|$ 总是一个非负整数. 绝对值有下面的性质：

(11) $|ab|=|a||b|$，

(12) (三角不等式) $|a+b|\leqslant|a|+|b|$.

现在我们简短地提一下有理数、实数和复数的代数结构.

有理数的集合记作 **Q**，它是所有分数 $\frac{a}{b}$ 之集，其中 $a,b \in \mathbf{Z}$ 且 $b \neq 0$. 两个有理数 $\frac{a}{b}$ 与 $\frac{c}{d}$ 相等，等价于说 $ad = bc$. 由 $a = \frac{a}{1}$，可将整数 **Z** 看作 **Q** 的子集. 易于知道，对每个 $a \in \mathbf{Z}, a \neq 0$，$a$ 在 **Q** 中均有唯一的(乘法)"逆"，即存在唯一的 $r \in \mathbf{Q}$，使 $ra = 1$；并且 **Q** 是包含 **Z** 且具有这一性质的最小集合.

实数的集合记作 **R**. 通常我们将 **R** 看作所有十进小数的集合，因而 **Q** 是 **R** 的子集. 定义实数的一种方式是将其作为有理数的柯西(Cauchy)序列的极限，我们对此不作讨论. 然而，没有精确定义仍然可以使用实数，本书将像我们在初等数学中做过的那样对待实数. (历史上，实数也的确是在使用了几百年后，才给出了精确的定义.)

复数的集合记作 **C**，它们由所有形如 $a + bi$ 的数构成，这里 $a,b \in \mathbf{R}$，而 $\mathrm{i} = \sqrt{-1}$. 复数的实部、虚部、共轭、模、三角形式，以及几何意义等，都已在中学里学习过，这里不再讨论，我们只提及一个基本的等式(称为**欧拉**(Euler)**公式**)：

$$r(\cos\theta + \mathrm{i}\sin\theta) = re^{i\theta},$$

其中 r,θ 分别是复数的模及幅角，而 e 是自然对数的底.

与 **Z** 类似，**Q**，**R**，**C** 中可作加、减法与乘法，并且具有 **Z** 中相同的运算规律. 于是，**Q**，**R**，**C** 都是环.

但从代数观点看，**Q**，**R**，**C** 与 **Z** 有很大的不同. 在 **Z** 中，方程 $ax = 1$ 仅在 $a = 1$ 或 -1 时可解；但在 **Q**，**R** 或 **C** 中，每一个非零元均有(乘法)"逆"，即可以作除法运算. 用代数的语言，能作加，减，乘，除(分母不为零)四则运算(并且满足通常运算规律)的集合，称为**域**. 于是，**Q**，**R**，**C** 都是域，但 **Z** 不是域. 此外，**Q** 中每个元都是 **Z** 中两个元素之商，我们因此将 **Q** 称为 **Z** 的商域；又 $\mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$，我们说 **R** 是 **Q** 的扩域，**C** 是 **R** 的扩域.

2. 多项式. 我们用 D 代表 **Z**，**Q**，**R** 或 **C**. 设 n 是非负整数，表达式

(13)　$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$,

其中 $a_0, a_1, \cdots, a_n$ 属于 D，称为**系数在 D 中的一元多项式**，也可称为 D 上的一元多项式. 所有形如(13)的多项式的集合，记作 $D[x]$.

在微积分中，我们常将(13)称为多项式函数，即 x 视为 D 中的变量. 但在代数学中，我们将采用不同的观点，(13)中的 x 称为**不定元**——并非是 D 中不确定的元素，而仅是一个不属于 D 的形式符号，我们约定 x 与 D 中元素的(形式)运算适合 D 中元素的运算规律. 我们常用 $f(x), g(x), \cdots$ 或 $f, g, \cdots$ 等来代表多项式.

在多项式(13)中，a_ix^i 称为 **i 次项**，a_i 称为 i 次项的**系数**. 两个多项式 $f(x)$ 和 $g(x)$ **相等**(或恒等)，记作 $f(x) = g(x)$，是指 $f(x)$ 与 $g(x)$ 中同次项的系数相等. 系数全为零的多项式称为**零多项式**，简称零，记为 0.

在(13)中，如果 $a_n \neq 0$，则称 a_nx^n 为多项式(13)的**首项**，a_n 为**首项系数**，n 为多项式(13)的**次数**，记作 $n = \deg f(x)$，这通常简记为 $n = \deg f$.(多项式的次数与不定元的选取无关.)请注意，零次多项式即为 D 中非零元素，而零多项式是唯一不定义次数的多项式.

$D[x]$ 中的多项式可作加、减、乘法运算. 设

(14)　$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$,

(15)　$g(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_0$,

是 $D[x]$ 中两个多项式. 在表示 $f(x)$ 与 $g(x)$ 的和时，如 $n \geqslant m$，为了方便起见，我们令 $b_n = \cdots = b_{m+1} = 0$. 定义

$$f(x) + g(x) = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_0 + b_0).$$

易于验证，多项式的加法满足结合律与交换律(因为这些均归结为系数 a_i, b_i 的加法). 零多项式在 $D[x]$ 中加法的作用相当于数 0 在 D 中加法的作用：$0 + f(x) = f(x)$. 此外，对任意 $f(x)$，我们将其每一项的系数改变符号得到的多项式，记作 $-f(x)$，则 $f(x) + (-f(x)) = 0$. 定义

$f(x)-g(x)=f(x)+(-g(x))$，于是 $D[x]$ 中可作减法运算.

$D[x]$ 中还可以作乘法. 设 $f(x),g(x)$ 如(14),(15)式，定义 $f(x)$ 与 $g(x)$ 的积为

$$f(x)\cdot g(x)=a_nb_mx^{n+m}+(a_nb_{m-1}+a_{n-1}b_m)x^{n+m-1}+\cdots+(a_1b_0+a_0b_1)x+a_0b_0,$$

其中 k 次项的系数是 $\sum_{i+j=k}a_ib_j$.

同样易于验证，$D[x]$ 中的乘法满足结合律，交换律与分配律(因这也归结为 D 中元素的加法与乘法运算). 多项式 1 在 $D[x]$ 中乘法的作用相当与数 1 在 D 中乘法的作用：$1\cdot f(x)=f(x)$.

因此，$D[x]$ 对(上面定义的) 加法与乘法形成一个交换环，我们称之为 **D 上的一元多项式环**.

最后，我们简要地介绍一下 D 上的多元多项式. 设 $x_1,\cdots,x_n$ 为 n 个不定元，形如

$$ax_1^{i_1}\cdots x_n^{i_n}$$

的式子，称为一个 n 元**单项式**，其中系数 $a\in D$，$i_1,\cdots,i_n$ 为非负整数，而 $x_1^{i_1},\cdots,x_n^{i_n}$ 允许交换次序. 如果两个单项式中相同不定元的幂次均相等，则称它们为**同类项**. 有限个(不同类的)单项式的(形式)和

$$\sum_{i_1,\cdots,i_n}a_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n},\quad a_{i_1\cdots i_n}\in D,$$

称为 **系数在 D 中的 n 元多项式**，也称为 D 上的 n 元多项式. D 上所有 n 元多项式的集合记作 $D[x_1,\cdots,x_n]$. 我们常用 $F(x_1,\cdots,x_n)$，$G(x_1,\cdots,x_n),\cdots$ 或 $F,G,\cdots$ 等来代表 n 元多项式.

各个单项式的系数都是零的多项式，称为 $D[x_1,\cdots,x_n]$ 中**零多项式**，简称零，记作 0. 设 $F(x_1,\cdots,x_n)$ 与 $G(x_1,\cdots,x_n)$ 是 $D[x_1,\cdots,x_n]$ 中两个多项式，如果 F 与 G 中的单项式一一对应地为系数相等的同类项，则称 F 与 G **相等**(或恒等)，记作 $F=G$.

$D[x_1,\cdots,x_n]$ 中可定义加、减、乘法运算.

对 $F,G\in D[x_1,\cdots,x_n]$,F 与 G 的和,记作 $F+G$,是 D 上唯一确定的多项式,其中的项是 F 与 G 的诸单项式的和(将两者的同类项"合并"—— 就是将系数相加).此外,对于任意的 $F\in D[x_1,\cdots,x_n]$,改变其诸单项式的符号所得的多项式,记作 $-F$,并定义

$$F-G=F+(-G),$$

于是 $D[x_1,\cdots,x_n]$ 中可作减法运算.

$D[x_1,\cdots,x_n]$ 中两个单项式

$$ax_1^{i_1}\cdots x_n^{i_n}\quad 与\quad bx_1^{j_1}\cdots x_n^{j_n}$$

的积定义为 $abx_1^{i_1+j_1}\cdots x_n^{i_n+j_n}$;对任意 $F,G\in D[x_1,\cdots,x_n]$,F 与 G 的积,记作 FG,是 D 上唯一确定的多项式,其中的项是 F 与 G 中诸单项式两两(如上)乘积之和.

易于验证,$D[x_1,\cdots,x_n]$ 中的多元多项式,对于上述定义的加、减、乘法运算,满足与 $D[x]$ 中运算相同的运算规律,因此是一个交换环,我们称之为 **D 上的多元多项式环**.

第一部分

整　　数