Textbooks for University

# Linear Algebra

彭国华　李德琅

高等教育出版社
Higher Education Press

ISBN 7-04-019282-9

9 787040 192827 >

定价 26.20 元

Textbooks for University

# Linear Algebra

彭国华　李德琅

高等教育出版社
Higher Education Press

**内容提要**

本书用英语写成，包含多项式和线性代数的基本内容，逻辑清晰，章节安排自然合理，有近550道配套习题，许多习题十分新颖。主要内容包括：整数和多项式，线性方程组，线性映射，矩阵和行列式，线性空间和线性映射，线性变换，欧几里得空间，线性型，双线性型以及二次型。本书适合数学系本科生作为高等代数教材使用，也可作为双语教学和线性代数的参考教材。

**图书在版编目(CIP)数据**

Linear Algebra/彭国华，李德琅.—北京：高等教育出版社，2006.5

ISBN 7-04-019282-9

Ⅰ.线… Ⅱ.①彭…②李… Ⅲ.线性代数-高等学校-教材-英文 Ⅳ.O151.2

中国版本图书馆CIP数据核字(2006)第022027号

**策划编辑** 李艳馥 **责任编辑** 崔梅萍 **封面设计** 王 雎 **责任绘图** 尹文军
**版式设计** 范晓红 **责任校对** 杨凤玲 **责任印制** 毛斯璐

| | | | |
|---|---|---|---|
| 出版发行 | 高等教育出版社 | 购书热线 | 010-58581118 |
| 社 址 | 北京市西城区德外大街4号 | 免费咨询 | 800-810-0598 |
| 邮政编码 | 100011 | 网 址 | http://www.hep.edu.cn |
| 总 机 | 010-58581000 | | http://www.hep.com.cn |
| | | 网上订购 | http://www.landraco.com |
| 经 销 | 蓝色畅想图书发行有限公司 | | http://www.landraco.com.cn |
| 印 刷 | 北京未来科学技术研究所有限责任公司印刷厂 | 畅想教育 | http://www.widedu.com |

| | | | |
|---|---|---|---|
| 开 本 | 787×960 1/16 | 版 次 | 2006年5月第1版 |
| 印 张 | 22.75 | 印 次 | 2006年5月第1次印刷 |
| 字 数 | 410 000 | 定 价 | 26.20元 |



**物料号 19282-00**

# 前　言

高等代数是数学系本科一年级的课程。在教学过程中我们逐渐感到有必要编写一本新的高等代数教材。一方面是为了与中学教学内容的衔接，另一方面也是为了顺应时代的需要。由于对课程内容和教学理念有许多一致的看法，两位作者准备联合编写一本高等代数教材。讲义初稿从 2000 年起着手编写，2001 年 9 月完成，并于当年秋季起一直在四川大学数学学院一年级所有班级中连续使用。由于书稿是在电脑上直接写成的，而敲打汉字对我们来说又是件痛苦的事，因此我们就顺便用英文写成。从近五年的连续使用情况来看，学生反映教材章节安排自然合理，逻辑清晰，举例适当。大多数学生认为习题新颖、量大，难易结合且和教学内容互补搭配。

我们以如何求解线性方程组为出发点，进而考虑解的结构，自然引申出向量、矩阵、行列式、线性空间等概念并展开讨论。第一章预先讨论了一元多项式和多元多项式的基本概念和结论，为后面学习线性代数做准备。在第二章里，我们以讨论解线性方程组的解为中心，引入了向量和矩阵的概念并讨论了它们的基本关系和性质。第三章主要讨论了矩阵的运算和行列式。我们首先建立了在固定的标准单位向量组下向量空间上的线性映射和矩阵的一一对应关系，然后将矩阵的加法和乘积自然定义为线性映射加和乘的矩阵。进而借助映射诱导出矩阵的许多性质。这一章里我们还专门讨论了分块矩阵的运算准则和例子。在讨论行列式时，我们借助初等矩阵，给出矩阵乘积行列式的公式，并没有用到行列式的定义。这些是与大多数的其他同类教材不同的地方。第四章、第五章分别讨论了线性空间、线性映射和线性变换。在第五章里我们还讨论了λ-矩阵、若尔当标准形和一般数域上的有理标准形。第六章是关于欧几里得空间的，主要包含内积空间、正交变换、对称变换、正交矩阵、对称矩阵等基本内容。我们把二次型放到了第七章。这一章先讲了线性型和双线性型。作为应用，我们讨论了二次型和正定二次型的基本性质，包括二次型的标准形问题。

本书配备了大约 550 道习题。一些重要的概念和结论被放到习题里，目的是希望学生可以通过自己独立思考得出这些结论。比如，我们把结式、特征子

空间以及张量积等内容都安排到习题里。我们相信这些题目有助于理解高等代数的概念和理论，演练所学技巧，有助于培养逻辑思维能力、抽象思维能力、运算能力、解决实际问题的能力和创新能力，有助于提高学生的数学素养。

英语毕竟不是我们的母语，何况我们的英语水平也有限，因此书中肯定有许多语言错误，请读者帮忙指出。本书的逻辑体系和其他的高等代数教材有所不同，涉及数学的部分也会有许多错误和不当之处，也请读者和专家们不吝赐教。

我们对张慎语、谭友军两位老师在本书修改过程中给予的帮助表示感谢。我们也特别感谢四川大学数学学院 2001 级至 2005 级的所有同学们，但愿我们的这本书至少达到了中文教材同样的学习效果，没有削减他们学习数学的兴趣。

彭国华
李德琅

# Contents

**1 Integers and Polynomials** ........ 1

1.1 Integers ........ 1
1.2 Number Fields ........ 5
1.3 Polynomials ........ 6
1.4 Polynomial Functions and Roots ........ 16
1.5 Polynomials over Rational Number Field ........ 19
1.6 Polynomials of Several Variables ........ 23
1.7 Symmetric Polynomials ........ 27
1.8 Exercises ........ 33

**2 Systems of Linear Equations** ........ 47

2.1 Systems of Linear Equations and Elimination ........ 47
2.2 Vectors ........ 56
2.3 Matrices ........ 64
2.4 Structure of Solutions of A System of Linear Equations ........ 73
2.5 Exercises ........ 80

**3 Linear Maps, Matrices and Determinants** ........ 89

3.1 Linear Maps of Vector Spaces and Matrices ........ 89
3.2 Operations of Linear Maps and Matrices ........ 94
3.3 Partitioned Matrices ........ 104
3.4 Elementary Matrices and Invertible Matrices ........ 109
3.5 Determinants ........ 117
3.5.1 Permutation and Determinant ........ 117
3.5.2 Properties of Determinant ........ 122

3.5.3 Expansion of Determinant ........ 128
3.5.4 Applications of Determinant ........ 136
3.6 Exercises ........ 139

**4 Linear Spaces and Linear Maps** ........ 156
4.1 Linear Spaces ........ 156
4.2 Dimension, Basis, Coordinates ........ 158
4.3 Basis Change and Coordinate Transformations ........ 161
4.4 Linear Maps and Isomorphism ........ 164
4.5 Matrices of Linear Maps ........ 171
4.6 Subspaces and Direct Sum ........ 175
4.7 Space Decomposition and Partitioned Matrices ........ 183
4.8 Exercises ........ 187

**5 Linear Transformations** ........ 202
5.1 Linear Transformations ........ 202
5.2 Similarity of Matrices ........ 204
5.3 $\lambda$-Matrices ........ 207
5.4 Eigenvalues, Eigenvectors and Characteristic Polynomials ........ 210
5.5 Invariant Subspaces ........ 215
5.6 Equivalence of $\lambda$-matrices ........ 218
5.7 Invariant Factors and Elementary Divisors ........ 226
5.8 Condition for Similarity of Matrices ........ 234
5.9 Jordan Canonical Forms of Matrices ........ 237
5.10 Rational Canonical Forms of Matrices ........ 247
5.11 Exercises ........ 251

**6 Euclidean Spaces** ........ 268
6.1 Inner Product and Basic Properties ........ 268
6.2 Orthogonal Bases and Schmidt Orthonormalization ........ 272
6.3 Subspaces and Orthogonal Complements ........ 279
6.4 Isometry and Orthogonal Transformations ........ 282
6.5 Symmetric Matrices and Symmetric Transformations ........ 286
6.6 The Method of Least Squares—System of Linear Equations

Revisited ........ 293
6.7 A Brief Introduction to Unitary Spaces ........ 298
6.8 Exercises ........ 300

**7 Linear Forms, Bilinear Forms and Quadratic Forms** ........ 315
7.1 Linear Forms and the Dual Space ........ 315
7.2 Bilinear Forms ........ 319
7.3 Symmetric Bilinear Forms ........ 324
7.4 Quadratic Forms ........ 326
7.5 Quadratic Forms over Real and Complex Number Fields ........ 330
7.6 Positive Definite Quadratic Forms over Real Number Field ........ 336
7.7 Exercises ........ 341

**Bibliography** ........ 349

**Index** ........ 350

# Chapter 1

# Integers and Polynomials

## 1.1 Integers

Number is the most basic concept in mathematics. We already know natural numbers, integers, rational numbers, real numbers and complex numbers from middle school. Some basic properties of integers are discussed here.

We denote the set of all integers by $\mathbb{Z}$. Then $a \in \mathbb{Z}$ means that $a$ is an integer. Let $a$, $b \in \mathbb{Z}$, then $a+b$, $a-b$, $ab$ are all integers. But the quotient $a/b, b \neq 0$, may not be an integer. This phenomenon causes many stories about integers. Here we mention a few.

Suppose that $a$ and $b$ are integers. If there is an integer $q$ such that $a=bq$, we say that $b$ **divides** $a$, or that $b$ is a **factor** (or **divisor**) of $a$. Sometimes we write $b \mid a$ to denote this fact. If $b \mid a$, we say that $a$ is a **multiple** of $b$. We also write $b \nmid a$ to denote the fact that $b$ doesn't divide $a$. Clearly $1$, $-1$, $a$, $-a$ are factors of $a$. They are called the **trivial factors** of $a$.

It is easy to see that if $d \mid a$ and $d \mid b$ then $d \mid ax+by$ for $x$, $y \in \mathbb{Z}$. It follows that if $d \mid a$, $d \nmid b$ then $d \nmid a+b$.

If $p>1$ and $p$ has no non-trivial factor, we call $p$ a **prime number**.

If an integer $c$ is a divisor for both $a$ and $b$, we say that $c$ is a **common divisor** of $a$ and $b$. If $d$ is a positive common divisor of $a$ and $b$ such that any common divisor $c$ of $a$ and $b$ is a factor of $d$, we call $d$ the **greatest common divisor** of $a$ and $b$. This is denoted by $d=\gcd(a,b)$ or simply $d=(a,b)$. Two integers $a$ and $b$ are called **coprime**, or **relatively prime**, if $(a,b)=1$. We define the greatest common divisor of $a_1, \cdots, a_n$ similarly and denote it as $\gcd(a_1, \cdots, a_n)$ or simply $(a_1,\cdots,a_n)$. It can be proved that

$$(a_1,\cdots,a_n)=((a_1,a_2),a_3,\cdots,a_n).$$

Given two integers $a$ and $b$ with $b\neq 0$, we may always find integers $q$, $r$ with $0\leqslant r<|b|$ such that

$$a=bq+r.$$

The number $q$ is usually called the *quotient* of $a$ divided by $b$ and $r$ is called the least non-negative *remainder* of $a$ divided by $b$. This procedure is called **division algorithm.**

We may use the following algorithm to compute the greatest common divisor of $a$ and $b$.

First we mention that

$$\text{“}a=bq+r\Rightarrow(a,b)=(b,r)\text{”}.$$

Because every common divisor of $a$ and $b$ is also a common divisor of $b$ and $r$ and vice versa.

Suppose that $a$, $b$ are not all zero. Since $(a,b)=(b,a)=(-a,b)$, we may suppose that $b>0$ and $a=bq+r$ with $0\leqslant r<b$. If $a=0$ then$(a,b)=(0,b)=b$. If $r=0$ we get $(a,b)=b$. If $r\neq 0$ we may find integers $q_1$, $r_1$ with $0\leqslant r_1<r$ such that

$$b=rq_1+r_1.$$

If $r_1=0$ we have $(a,b)=(b,r)=r$. If $r_1\neq 0$, we repeat this procedure to find $q_2,r_2,q_3,r_3,\cdots$with $0\leqslant r_k<r_{k-1}$ such that

$$r_{k-2}=r_{k-1}q_k+r_k$$

until

$$r_k=0.$$

That is,

$$\begin{aligned}
a&=bq+r,\\
b&=rq_1+r_1,\\
r&=r_1q_2+r_2,\\
&\vdots\\
r_{k-3}&=r_{k-2}q_{k-1}+r_{k-1}, \quad r_{k-1}>0,\\
r_{k-2}&=r_{k-1}q_k+r_k, \quad r_k=0.
\end{aligned}$$

Then

$$(a,b)=(b,r)=(r,r_1)=\cdots=(r_{k-2},r_{k-1})=(r_{k-1},r_k)=r_{k-1}.$$

That is, $(a,b)$ is just the last non-zero remainder in the above procedure.

This is called **Euclidean algorithm.**

Let $S=\{am+bn \mid m,n\in Z\}$ be the set of all numbers $am+nb$ with $m,n\in Z$. Let $d$ be the smallest positive integer in $S$. We claim that $d=(a,b)$. First $d\mid a$. Actually, if $a=qd+r$ with $0\leqslant r<d$ and $d=am_1+bn_1$, then

$$r=a-qd=a-q(am_1+bn_1)=a(1-qm_1)+b(-qn_1)\in S.$$

But $d$ is the smallest positive integer in $S$, so $r=0$. Similarly $d\mid b$. So $d$ is a common factor of $a$ and $b$. On the other hand, every common factor of $a$ and $b$ divides $d=am_1+bn_1$. So there exist integers $u$, $v$ such that

$$(a,b)=au+bv.$$

In fact, we may use Euclidean algorithm to find $u$ and $v$. Since

$$d=r_{k-1}$$

and

$$\begin{aligned}r_{k-1}&=r_{k-3}-q_{k-1}r_{k-2}\\ r_{k-2}&=r_{k-4}-q_{k-2}r_{k-3}\\ &\vdots\\ r_1&=b-q_1r\\ r&=a-bq,\end{aligned}$$

then

$$\begin{aligned}(a,b)=r_{k-1}&=r_{k-3}-q_{k-1}(r_{k-4}-q_{k-2}r_{k-3})\\ &=(1+q_{k-1}q_{k-2})r_{k-3}-q_{k-1}r_{k-4}\\ &\vdots\end{aligned}$$

Iteratively we go back to $a$ and $b$ to get $u$, $v$.

**Example 1.1** For $a=329$, $b=182$, we use Euclidean algorithm to get

$$\begin{aligned}329&=182\cdot 1+147\\ 182&=147\cdot 1+35\\ 147&=35\cdot 4+7\\ 35&=7\cdot 5.\end{aligned}$$

Then $(329,182)=7$ and

$$\begin{aligned}7&=147-35\cdot 4=147-(182-147\cdot 1)\cdot 4\\ &=147\cdot 5-182\cdot 4=(329-182\cdot 1)\cdot 5-182\cdot 4\\ &=329\cdot 5+182\cdot(-9)\end{aligned}$$

So $(329,182)=329\cdot 5+182\cdot(-9)$.

We note that the integers $u$, $v$ satisfying $d=au+bv$ are not uniquely determined. For instance, if $d=au+bv$, then $d=a(u-tb)+b(v+ta)$ for any $t\in Z$.

Let $p$ be a prime. For any integer $a$, let $d=(a,p)$, then $d=p$ or 1 according to $p\mid a$ or not.

If a prime number $p$ divides $ab$, then $ab=pq$ for some $q\in\mathbb{Z}$. If $p\nmid a$, then $(p,a)=1$ and $au+pv=1$ for some $u$, $v\in\mathbb{Z}$. Therefore $abu+pvb=b$ and $p(qu+vb)=b$. Consequently $p\mid b$. Herein we have proved that $p\mid ab$ implies that $p\mid a$ or $p\mid b$.

It is easy to prove by induction on $r$ that if $p$ is a prime, then

$$\text{“}p\mid a_1a_2\cdots a_r \Rightarrow p\mid a_i \text{ for some } i\text{”}$$

**Theorem 1.1 (Fundamental Theorem of Arithmetic)** *Any integer greater than 1 is a product of prime numbers. If*

$$a=p_1p_2\cdots p_r=q_1q_2\cdots q_s,$$

*where $p_i$, $q_i$ are primes, then $r=s$ and we may rearrange $q_i$ if necessary so that $p_i=q_i$, $i=1, 2, \cdots, r$.*

*Proof.* Let $n>1$ be an integer. We prove first that $n$ is a product of some primes. If $n$ is a prime, then we are done. For general case we make use of induction. Suppose that any integer $m$ with $1<m<n$ is a product of primes and that $n$ is not a prime. Then there exits a non-trivial factor of $n$. That is $n=n_1n_2$ with $1<n_1$, $n_2<n$. The divisors $n_1$, $n_2$ are both products of primes by our hypothesis, and so is $n$. Secondly suppose that

$$a=p_1p_2\cdots p_r=q_1q_2\cdots q_s.$$

Since $p_1$ is a prime and $p_1\mid a$, $p_1$ divides some $q_i$. We may suppose that $p_1$ divides $q_1$ by suitable arrangement of the order of $q_i$. Therefore

$$p_1=(p_1,q_1)=q_1,$$

since both $p_1$ and $q_1$ are primes. Also we have

$$p_2\cdots p_r=q_2\cdots q_s.$$

Similarly, by suitable arrangement of the order of $q_i$, we get $p_2=q_2,\cdots$, and finally $r$ must equal $s$. □

If $a$ is an integer other than 0, $\pm1$, then $a=\pm\prod_{i=1}^{r}p_i^{n_i}$, where $p_1,\cdots,p_r$ are different primes and $n_i>0$. The decomposition is unique up to the order of the factors.

There are infinitely many prime numbers. We owe the following proof to Euclid.

Suppose finite number of primes

$$p_1,p_2,\cdots,p_m$$

are given. Take

$$N = p_1 p_2 \cdots p_m + 1.$$

Then $N$ has at least one prime divisor $p$. But

$$p_i \nmid N, \quad 1 \leqslant i \leqslant m.$$

Therefore $p$ is a prime other than $p_1, \cdots, p_m$. This deduces that there are infinitely many prime numbers.

## 1.2 Number Fields

In mathematics, number is a basic concept and so are the operations like summation, subtraction, multiplication, division over numbers. We need to work on a set of numbers in which all the operations may be done freely.

**Definition 1.1** *A set F of complex numbers is called a* **number field** *if it satisfies the following conditions:*

(1) $1 \in F$;

(2) *if* $a, b \in F$, *then* $a \pm b$, $ab \in F$; *and*

(3) *if* $b \neq 0$, *then* $a/b \in F$.

For example, the set of all rational numbers is a number field which is denoted by $\mathbb{Q}$. It is easy to see that this is the smallest number field. Any number field $F$ contains 1 by the definition. Therefore it contains $2=1+1$, $3=1+2$, $\cdots$ and $0=1-1$, $-1=0-1$, $\cdots$. So all integers are in $F$. Furthermore $F$ contains all $a/b$, where $a$, $b$ are integers and $b \neq 0$. This proves that $F \supset \mathbb{Q}$.

The set of all real numbers is a number field, which is called the **real number field** and is denoted by $\mathbb{R}$.

The set of all complex numbers is a number field, which is called the **complex number field** and is denoted by $\mathbb{C}$.

The set of all numbers of the form

$$a + b\sqrt{2},$$

where $a$, $b \in \mathbb{Q}$, is a number field, which is denoted by $\mathbb{Q}(\sqrt{2})$. Since if $a$, $b$, $a_1$, $b_1$ are rational, then

$$(a+b\sqrt{2}) + (a_1 + b_1\sqrt{2}) = (a+a_1) + (b+b_1)\sqrt{2},$$

$$(a+b\sqrt{2}) - (a_1 + b_1\sqrt{2}) = (a-a_1) + (b-b_1)\sqrt{2},$$

$$(a+b\sqrt{2})(a_1+b_1\sqrt{2})=(aa_1+2bb_1)+(ab_1+ba_1)\sqrt{2},$$

and if $a_1+b_1\sqrt{2}\neq 0$, then

$$\frac{a+b\sqrt{2}}{a_1+b_1\sqrt{2}}=\frac{aa_1-2bb_1}{a_1^2-2b_1^2}+\frac{ba_1-ab_1}{a_1^2-2b_1^2}\sqrt{2}.$$

Another example of number field is the set $\mathbb{Q}(\pi)$ of all the numbers of the form

$$\frac{a_n\pi^n+a_{n-1}\pi^{n-1}+\cdots+a_0}{b_m\pi^m+b_{m-1}\pi^{m-1}+\cdots+b_0},$$

with $a_i$, $b_j\in\mathbb{Q}$ and that $b_0,\cdots,b_m$ are not all zero. It is easy to see that for two numbers of this kind $\alpha$, $\beta$ we have

$$\alpha\pm\beta,\alpha\beta\in\mathbb{Q}(\pi),\quad\text{and}\quad\frac{\alpha}{\beta}\in\mathbb{Q}(\pi)\text{ if }\beta\neq 0.$$

To finish the proof we need to know a fact that if $b_m,\cdots,b_0$ are not all zero then $b_m\pi^m+\cdots+b_0\neq 0$. Or in other words $\pi$ is transcendental. This is actually true but we can not prove it here. The proof of this fact needs some more knowledge from analysis.

*Remark* The condition (1) in Definition 1.1 may be replaced by

(1′) $F$ contains a non-zero number.

## 1.3 Polynomials

Let $F$ be a number field. A formal expression

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,\quad a_i\in F, i=0,\cdots,n,$$

is called a **polynomial over** $F$, where $x$ is an indeterminate. The set of all polynomials over the field $F$ is called the **polynomial ring** over $F$ and is denoted by $F[x]$.

The $a_i$'s are called the **coefficients** of $f$. If $a_n\neq 0$, we call $a_n$ the **leading coefficient** and $a_nx^n$ the **leading term**. In this case, $n$ is called **degree** of $f(x)$ and we write deg $f=n$ or $\partial f=n$. If $f(x)=c\neq 0$, then deg $f=0$ and vice versa. When $a_n=1$, we say that $f$ is **monic**.

A special polynomial is $f(x)=0$, which has no degree and is called the **zero polynomial**. It's remarked that some literature define the degree of zero polynomial to be $-\infty$.

Two polynomials

$$f(x)=a_nx^n+\cdots+a_1x+a_0$$

and

$$g(x)=b_nx^n+\cdots+b_1x+b_0$$

are equal if and only if $a_i=b_i$ for $0\leqslant i\leqslant n$.

Let's recall the summation symbol $\sum$, which may be used to denote the following fact:

$$a_0+a_1+\cdots+a_n=\sum_{i=0}^{n}a_i.$$

We can also write

$$a_0+a_1+\cdots+a_n=\sum_{0\leqslant i\leqslant n}a_i.$$

In such a way, a polynomial $f(x)=a_nx^n+\cdots+a_1x+a_0$ of degree $n$ may be written as

$$f(x)=\sum_{i=0}^{n}a_ix^i,\quad a_n\neq 0.$$

The symbol $\sum$ has the following properties:

(1)

$$\sum_{i=0}^{n}(a_i+b_i)=\sum_{i=0}^{n}a_i+\sum_{i=0}^{n}b_i.$$

(2)

$$\sum_{i=0}^{n}a_i\sum_{j=0}^{m}b_j=\sum_{k=0}^{m+n}c_k.$$

Here

$$c_k=\sum_{\substack{0\leqslant i\leqslant n\\0\leqslant j\leqslant m\\i+j=k}}a_ib_j=\sum_{i=0}^{n}a_ib_{k-i}$$

and we consent that $a_i=0$ if $i<0$ or $i>n$ and that $b_i=0$ if $j<0$ or $j>m$.

(3)

$$\sum_{i=0}^{n}\sum_{j=0}^{m}a_{ij}=\sum_{j=0}^{m}\sum_{i=0}^{n}a_{ij}.$$

Now we come to define operations over polynomials.

Let

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,$$
$$g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0,$$

where $a_n\neq 0$, $b_m\neq 0$, and $m\leqslant n$. We may write

$$g(x)=b_nx^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0,$$

with $b_n=\cdots=b_{m+1}=0$. Define

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

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

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

$$=\sum_{k=0}^{m+n}\Big(\sum_{i+j=k}a_ib_j\Big)x^k.$$

Note that we consent that $a_i=0$ if $i>n$ and $b_j=0$ if $j>m$. The leading coefficient of $f(x)g(x)$ is $a_nb_m$ by the definition of multiplication, hence

$$\deg(f(x)g(x))=\deg f(x)+\deg g(x).$$

It can be also proved that

$$\deg(f(x)+g(x))\leqslant\max\{\deg f(x),\deg g(x)\},$$

if $f(x)$, $g(x)$ and $f(x)+g(x)$ are not zero.

The operations satisfy the following rules.

1. Associativity for summation:

$$(f(x)+g(x))+h(x)=f(x)+(g(x)+h(x)),$$

2. Commutativity for summation:

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

3. Associativity for multiplication:

$$(f(x)g(x))h(x)=f(x)(g(x)h(x)),$$

4. Commutativity for multiplication:

$$f(x)g(x)=g(x)f(x),$$

5. Distributivity:

$$f(x)(g(x)+h(x))=f(x)g(x)+f(x)h(x),$$

6. Dispensability: if $f(x)\neq0$ and

$$f(x)g(x)=f(x)h(x),$$

then

$$g(x)=h(x).$$

The first five rules are easy to check by the definitions. For example, if

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,$$

$$g(x)=b_nx^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0,$$

$$h(x)=c_nx^n+c_{n-1}x^{n-1}+\cdots+c_1x+c_0,$$

then

$$(f(x)+g(x))+h(x)=((a_n+b_n)+c_n)x^n+\cdots+((a_1+b_1)+c_1)x+$$