高等学校試用教材

高等代数

下册

張禾瑞　郝鈵新編

高等教育出版社

高等学校試用教材

高 等 代 数

下 册

張禾瑞　郝鈵新编

高等教育出版社

本書是根据中华人民共和国教育部編訂的师范学院数学系高等代数試行教学大綱編写的。可作为师范学院数学系高等代数的試用教材，又师范專科学校使用本書作为試用教材，可根据其教学大綱删去書中某些章节。

全書分上、下册出版。

高　等　代　数

下　册

張禾瑞　郝鈵新編

高等教育出版社出版 北京宣武門內承恩寺7号

(北京市書刊出版業營業許可証出字第054号)

民族印刷厂印刷　新华書店發行

統一書号 13010·490　開本 850×1168 1/32　印張 4 9/16

字数 117,000　印数 43,501—61,500 定價(6) ¥ 0.55

1958年8月第1版　1959年11月北京第?次印刷

目 录

第六章　体上一个不定元的多項式

§ 28. 多項式环

現在回到多項式的討論。

我們的目的首先是要在一般体上来建立多項式的理論。但是为了以后討論上的某些方便，我們先在一个环上来討論多項式。

令 $\bar{R}$ 是一个有單位元 1 的可換环，R 是 $\bar{R}$ 的一个子环，并且含有 $\bar{R}$ 的單位元。

在 $\bar{R}$ 中任意取出一个元素 α。作 α 与 R 的元素的乘积的和，我們会得到形如

$$a_0+a_1\alpha+\cdots+a_n\alpha^n \tag{1}$$

的 $\bar{R}$ 的元素，其中 $a_0, a_1, \cdots, a_n$ 是 R 的元素。

定义 1. 表示式 (1) 叫做环 R 上元素 α 的一个多項式。a_i 叫做多項式(1)的系数。$a_i\alpha^i$ 叫做多項式(1)的一个項。

R 上 α 的多項式常用符号 $f(\alpha), g(\alpha)\cdots$, 来表示。

用 $R[\alpha]$ 来表示 $\bar{R}$ 中一切形如 (1) 的元素所構成的集合，那末 $R[\alpha]$ 是环 $\bar{R}$ 的一个部分集合。利用环里的計算規則，我們容易算出 $R[\alpha]$的兩个元素的和与积。

令
$$f(\alpha)=a_0+a_1\alpha+\cdots+a_n\alpha^n,$$
$$g(\alpha)=b_0+b_1\alpha+\cdots+b_m\alpha^m$$

是 $R[\alpha]$ 的兩个任意元素，并且 $m\leqslant n$。那末

$$f(\alpha)+g(\alpha)=(a_0+b_0)+(a_1+b_1)\alpha+\cdots+(a_n+b_n)\alpha^n,$$

此处当 $m<n$ 时，$b_{m+1}=b_{m+2}=\cdots=b_n=0$;

$$f(\alpha)g(\alpha)=c_0+c_1\alpha+\cdots+c_{m+n}\alpha^{m+n},$$

此外

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0 = \sum_{i+j=k} a_i b_j$$

(其中 $i>n$ 时 $a_i=0$, $j>m$ 时 $b_j=0$)。

以上的两个式子告訴我們，$R[\alpha]$的两个任意元素的和与积仍然屬于 $R[\alpha]$。另一方面，$R[\alpha]$ 的任意元素 $a_0+a_1\alpha+\cdots+a_n\alpha^n$ 的負元也屬于 $R[\alpha]$，因为

$$-(a_0+a_1\alpha+\cdots+a_n\alpha^n) = -a_0-a_1\alpha-\cdots-a_n\alpha^n.$$

因此 $R[\alpha]$是 $\bar{R}$ 的一个子环。

定义 2. $R[\alpha]$叫做环 R 上元素 α 的多項式环。

$R[\alpha]$显然包含 α 并且包含 R 作为它的子环。另一方面，設 R' 是 $\bar{R}$ 的一个既含 α 又含 R 的子环，那末 R' 一定含有一切形如(1)的元素，亦卽包含环 $R[\alpha]$。这样，多項式环 $R[\alpha]$是 $\bar{R}$中包含元素 α 及环 R 的最小子环。$R[\alpha]$显然与 R 有共同的單位元。

一般来說，把 $R[\alpha]$的一个元素表成 R 上 α 的多項式的方法不是唯一的。我們看一个例子。

令 $\bar{R}$ 是实数体。R 是整数环。在 $\bar{R}$ 中取元素 $\alpha=\sqrt{2}$。我們看 $R[\alpha]$的元素

$$2-5\sqrt{2}+(\sqrt{2})^2.$$

这个元素显然可以写成

$$4-5\sqrt{2}.$$

实际上，利用等式$(\sqrt{2})^2=2$，我們可以把 $R[\sqrt{2}]$的每一个元素

$$a_0+a_1\sqrt{2}+\cdots+a_n(\sqrt{2})^n$$

写成形如
$$b_0+b_1\sqrt{2}$$

的一个多項式。这个現象是由于 $\alpha=\sqrt{2}$ 滿足等式

$$\alpha^2-2=0$$

而發生的，这个等式的左端是整数环 R 上 α 的一个系数不为零的多項式。

定义 3. 令 α 是环 R 的扩环 $\bar{R}$ 的一个元素。若是存在等式

$$a_0+a_1\alpha+\cdots+a_n\alpha^n=0,$$

其中 $a_0, a_1, \cdots, a_n$ 都屬于 R，且至少有一个 a_i 不等于零，那末 α 就叫做环 R 上的一个代数元。

若是在 R 中不能找到不都等于零的元素 $a_0, a_1, \cdots, a_n$ 使以上等式成立，那末 α 就叫做环 R 上的一个不定元(或超越元)。

我們以下主要地將要討論不定元的多項式。这种多項式在代数上占一个非常重要的地位。

不定元我們將用字母 $x, y, z, \cdots$ 来代表。

令 $R[x]$ 是环 R 上一个不定元 x 的多項式环。

首先，$R[x]$ 具有以下重要性質。

定理 1. $R[x]$ 的元素只能用一种方法表成 R 上 x 的多項式，这就是說，若是 $R[x]$ 的兩个多項式 $f(x)$ 与 $g(x)$ 相等，那末除去系数为零的項外，它們含有完全相同的項。

事实上，設 $f(x)$ 与 $g(x)$ 是 $R[x]$ 的兩个多項式。在必要的时候，对 $f(x)$ 与 $g(x)$ 或其中的一个添加一些系数为零的項，总可以把它們写成以下形式：

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

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

現在假定 $$f(x)=g(x),$$

那末 $$f(x)-g(x)=0,$$

因而 $$(a_0-b_0)+(a_1-b_1)x+\cdots+(a_n-b_n)x^n=0.$$

但 x 是 R 上的一个不定元，所以由最后等式得：

$$a_i-b_i=0,\quad i=1, 2, \cdots, n,$$

或 $$a_i=b_i,\quad i=1, 2, \cdots, n.$$

这样，$f(x)$ 与 $g(x)$ 含有完全相同的系数不为零的項。

基于定理 1，我們可以对于 $R[x]$ 的多項式引入次数以及值这兩个概念。它們在关于不定元的多項式的討論中，都占一个很重

要的地位。

定义 4. 設环 R 上一个不定元 x 的多項式

$$f(x)=a_0+a_1x+\cdots+a_nx^n, \text{ 并且 } a_n\neq 0.$$

那末 a_n 叫做 $f(x)$ 的最高系数，非負整数 n 叫做 $f(x)$ 的次数。

由于定理 I 成立，按照这个定义，$R[x]$ 的每一个不等于零的多項式都有一个唯一确定的次数，特別，R 的非零元素的次数是零。多項式 0 沒有次数，我們叫它做零多項式。

关于多項式的次数以下事实成立。

i) 若 $f(x)$ 与 $g(x)$ 是 $R[x]$ 的兩个不等于零的多項式，那末或者 $f(x)$ 与 $g(x)$ 的和等于零，或者和的次数不超过 $f(x)$ 与 $g(x)$ 的次数中較大的一个。

ii) 若环 R 沒有零因子，$f(x)$ 与 $g(x)$ 是 $R[x]$ 的兩个不等于零的多項式，那末 $f(x)$ 与 $g(x)$ 的乘积的次数等于 $f(x)$ 与 $g(x)$ 的次数的和。

事实上，設 $f(x)$ 与 $g(x)$ 的次数各是 m 与 n：

$$f(x)=a_0+a_1x+\cdots+a_mx^m,\ a_m\neq 0,$$

$$g(x)=b_0+b_1x+\cdots+b_nx^n,\ b_n\neq 0,$$

并且 $m\leqslant n$。那末

$$f(x)+g(x)=(a_0+b_0)+(a_1+b_1)x+\cdots+(a_n+b_n)x^n, \tag{2}$$

$$f(x)g(x)=a_0b_0+(a_0b_1+a_1b_0)x+\cdots+a_mb_nx^{m+n}. \tag{3}$$

由(2)若和 $f(x)+g(x)\neq 0$，那末它的次数显然不能超过 n。另一方面，因为 R 沒有零因子，而 $a_m\neq 0$，$b_n\neq 0$，所以 $a_mb_n\neq 0$。因此由(3)，$f(x)g(x)$ 的次数是 $m+n$。

由事实(ii)，若 R 沒有零因子，那末 $R[x]$ 的兩个不等于零的多項式 $f(x)$ 与 $g(x)$ 的乘积 $f(x)g(x)$ 是一个系数不全为零的多項式，因而由不定元的定义，$f(x)g(x)\neq 0$。这就是説，环 $R[x]$ 也沒有零因子。

設給定了环 $R[x]$ 的一个多項式

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

以及环 R 的一个元素 c。那末在 $f(x)$ 的表示式中把 x 用 c 来代替，就得到 R 的一个形如

$$a_0+a_1c+\cdots+a_nc^n$$

的元素。这个元素叫做当 $x=c$ 时多项式 $f(x)$ 的值，并且用 $f(c)$ 来表示。

令 $f(x)$ 与 $g(x)$ 是 $R[x]$ 的两个多项式而 c 是 R 的任一元素。由定理 1 以及等式(2)与(3)容易看出：若 $f(x)=g(x)$，那末 $f(c)=g(c)$；并且若

$$\varphi(x)=f(x)+g(x),\quad \psi(x)=f(x)g(x),$$

那末 $$\varphi(c)=f(c)+g(c),\quad \psi(c)=f(c)g(c).$$

因此，由加法与乘法而得到的 $R[x]$ 的某些多项式間的任一关系式在用环 R 的元素 c 代替不定元 x 后都仍然成立。

以上的討論是在 R 上的不定元 x 存在的假定下进行的。自然会發生这样的問題：給了一个有單位元的可換环 R，是否总存在 R 上的不定元？下面的定理給这个問題一个肯定的答复。

定理 2. 給了一个有單位元的可換环 R，总存在以 R 为子环且与 R 有共同單位元的可換环 $\bar{R}$ 而 $\bar{R}$ 含有 R 上的不定元。

証 令 $\bar{R}$ 是由一切無穷序列

$$(a_0, a_1, a_2, \cdots)$$

所構成的集合，其中 a_i 是 R 的元素，但只有有限个 a_i 不等于零，換句話說，在每一个序列里，某一 a_n 以后的元素都是零。

兩个序列

$$(a_0, a_1, a_2, \cdots) \text{ 与 } (b_0, b_1, b_2, \cdots)$$

仅当 $$a_i=b_i (i=0, 1, 2, \cdots)$$

时才被認为相等。

我們替 $\bar{R}$ 規定兩个代数运算，分別叫做加法与乘法：

$$(a_0, a_1, a_2, \cdots)+(b_0, b_1, b_2, \cdots)=(a_0+b_0, a_1+b_1, a_2+b_2, \cdots);$$

$$(a_0, a_1, a_2, \cdots)(b_0, b_1, b_2, \cdots)=(c_0, c_1, c_2, \cdots);$$

此处
$$c_k=\sum_{i+j=k} a_i b_j,\ k=0, 1, 2, \cdots. \tag{4}$$

这样定义的加法是 $\bar{R}$ 的一个代数运算是显然的。至于乘法也是 $\bar{R}$ 的一个代数运算可以如下看出：若是当 $i>n$ 时 $a_i=0$ 而当 $j>m$ 时 $b_j=0$，那末当 $k>m+n$ 时 $c_k=0$。这就是說，乘积$(c_0, c_1, c_2, \cdots)$总是 $\bar{R}$ 的一个元。

我們現在証明，$\bar{R}$ 对于这两个代数运算来説作成一个可换环，并且 $\bar{R}$ 有單位元。

$\bar{R}$ 对加法来説显然作成一个加群。$\bar{R}$ 的零元就是 $(0, 0, \cdots)$；元素$(a_0, a_1, a_2, \cdots)$的負元是$(-a_0, -a_1, -a_2, \cdots)$。

$\bar{R}$ 的乘法显然滿足交換律，因为在等式(4)中 a_i 与 b_i 的地位是对称的。

乘法也滿足結合律。令

$$(a_0, a_1, \cdots)(b_0, b_1, \cdots)=(d_0, d_1, \cdots),$$

$$[(a_0, a_1, \cdots)(b_0, b_1, \cdots)](c_0, c_1, \cdots)=(e_0, e_1, \cdots).$$

那末，由等式(4)，

$$d_s=\sum_{i+j=s} a_i b_j,$$

而

$$e_t=\sum_{s+k=t} d_s c_k=\sum_{s+k=t}\left(\sum_{i+j=s} a_i b_j\right) c_k=\sum_{i+j+k=t} a_i b_j c_k.$$

另一方面，令

$$(a_0, a_1, \cdots)[(b_0, b_1, \cdots)(c_0, c_1, \cdots)]=(e_0', e_1', \cdots).$$

同样可以算出

$$e_t'=\sum_{i+s=t} a_i\Big(\sum_{j+k=s} b_jc_k\Big)=\sum_{i+j+k=t} a_ib_jc_k.$$

这样 $$(e_0, e_1, e_2, \cdots)=(e_0', e_1', e_2', \cdots).$$

$\bar{R}$的加法与乘法被分配律联系着。令

$$[(a_0, a_1, \cdots)+(b_0, b_1, \cdots)](c_0, c_1, \cdots)=(d_0, d_1, \cdots),$$

$$(a_0, a_1, \cdots)(c_0, c_1, \cdots)+(b_0, b_1, \cdots)(c_0, c_1, \cdots)=(d_0', d_1', \cdots).$$

那末，由加法及乘法的定义，

$$d_k=\sum_{i+j=k}(a_i+b_i)c_j=$$

$$=\sum_{i+j=k} a_ic_j+\sum_{i+j=k} b_ic_j=d_k',$$

而 $$(d_0, d_1, d_2, \cdots)=(d_0', d_1', d_2', \cdots).$$

在$\bar{R}$中，等式

$$(a_0, 0, 0, \cdots)(b_0, b_1, b_2, \cdots)=(a_0b_0, a_0b_1, a_0b_2, \cdots) \qquad (5)$$

成立。由此得出$\bar{R}$有單位元，就是$(1, 0, 0, \cdots)$。

这样，$\bar{R}$是一个有單位元的可换环。

令R_0是$\bar{R}$中一切形如

$$(a, 0, 0, \cdots)$$

的元素所構成的集合。那末

$$(a, 0, 0, \cdots)+(b, 0, 0, \cdots)=(a+b, 0, 0, \cdots),$$

$$(a, 0, 0, \cdots)(b, 0, 0, \cdots)=(ab, 0, 0, \cdots).$$

而 $$a\to(a, 0, 0, \cdots)$$

显然是R与R_0間的一个同構对应。因此我們可以把R_0看成R而令

$$(a, 0, 0, \cdots) = a. \tag{6}$$

于是 $\bar{R}$ 含有 R 作为子环，并且 $\bar{R}$ 与 R 有相同的單位元 1。

最后我們証明，$\bar{R}$ 包含 R 上的一个不定元 x 而 $\bar{R}=R[x]$。

令
$$x = (0, 1, 0, \cdots).$$

利用归納法我們容易証明

$$x^k = (\overbrace{0, \cdots, 0}^{k\text{ 个}}, 1, 0, \cdots). \tag{7}$$

由加法的定义以及等式 (5), (6), (7) 容易看出，$\bar{R}$ 的每一个元素 $(a_0, a_1, \cdots, a_n, 0, 0, \cdots)$ 都可以写成以下形式：

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

也就是說，写成环 R 上 x 的一个多项式。因此 $\bar{R}=R[x]$。

現在假定

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0.$$

这一等式可以改写成

$$(a_0, a_1, \cdots, a_n, 0, \cdots) = (0, 0, \cdots),$$

由此就得
$$a_0 = a_1 = \cdots = a_n = 0.$$

这就是說，x 是 R 上的一个不定元。

这样，对于任何有單位元的可換环 R 我們总可以談論 R 上一个不定元 x 的多项式。

在函数論中多项式

$$a_0 + a_1x + \cdots + a_nx^n \tag{8}$$

被看成变量 x 的定义在某一数集上的函数。例如，以实数为系数的多项式(8)可以被看作定义在实数体上的函数。

以环 R 的元素为系数的多项式 (8) 也可以看成变量 x 的定义在环 R 上的一个函数，就是对于 x 的屬于 R 的每一个值 c，以

$$a_0 + a_1c + \cdots + a_nc^n$$

为对应函数值的函数。

因此很容易想到，是否可以把多项式看成函数来建立多项式

的理論，从而可以避免証明不定元的存在。为了回答这一問題，我們看以下的例子。

考察以 2 为模的剩余类环 R_2 上的多项式

$$f(x)=x+1 \text{ 与 } g(x)=x^2+1.$$

我們把这兩个多項式看作定义在 R_2 上的变量 x 的函数。变量 x 只能取兩个值：0 与 1。容易看出，对 x 的每一个值来說，函数 $f(x)$ 与 $g(x)$ 的值都相等：

$$f(0)=g(0)=1,$$

$$f(1)=g(1)=0.$$

按照函数論的观点，給了定义在同一集合上的变量 x 的两个函数，若是对于 x 的每一个值来說，它們的値都相等，那末就認为这兩个函数相等。因此，看成函数，多項式 $f(x)$ 与 $g(x)$ 相等。但是这兩个多項式所含的項是不相同的。

这个例子說明，用函数論的观点在一般环 R 上来建立多項式的理論是不可能的，因为这样一来，定理 1 將不成立，而定理 1 正是多項式理論的基础。

对某些环 R 来說，把 $R[x]$ 的多項式看成函数后定理 1 仍然成立。这一点以后会看到。

習　題

1. 令 R_5 是以 5 为模的剩余类环。我們約定把 R_5 的元素 c_k 用 k 来表示（$k=0, 1, 2, 3, 4$）。計算 R_5 上多項式

$$x^4+2x^3+3x^2+1 \text{ 与 } 2x^2+4x+2$$

的乘积。

2. 設 $\bar{R}$ 是环 R 的一个子环，x 是 R 上的一个不定元。証明 $\bar{R}[x]$ 是 $R[x]$ 的一个子环。

3. 設 x 与 y 都是环 R 上的不定元，証明 $R[x]$ 与 $R[y]$ 同构。

4. 証明，多項式环 $R[x]$ 的每一个次数大于零的多項式都是 R 上的一个不定元。

5. 令 y 是多項式环 $R[x]$ 的一个元素。証明，当且仅当 x 可以表成 y 的多項式时，$R[x]$ 与 $R[y]$ 相等。

6. 証明，多項式环 $R[x]$ 能与它的一个真正子环同構。

§29. 体上多項式的整除性

在以下几节里，我們專討論一个任意体 P 上一个不定元 x 的多項式。如果不特别声明，論及的多項式都是 $P[x]$的多項式。

在多項式环 $P[x]$里可以建立整除性的理論，与整数的整除性理論完全平行。例如，我們可以引入多項式的最大公因式的概念以及把一个多項式分解为"素"多項式的乘积。

定义 1. 令 $f(x)$ 与 $g(x)$ 是 $P[x]$ 的兩个多項式。假如存在 $P[x]$ 的多項式 $h(x)$，使

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

我們就說，$g(x)$整除 $f(x)$ 或 $f(x)$能被 $g(x)$整除。这时 $g(x)$叫做 $f(x)$的一个因式。

由这个定义，我們可以直接推出关于多項式整除性的一些基本性質。

(一)若多項式 $f(x)$能被多項式 $g(x)$整除，而 $g(x)$ 又能被多項式 $h(x)$ 整除，那末 $f(x)$能被 $h(x)$整除。

事实上，由所給的条件得：

$$f(x)=g(x)\varphi(x),\quad g(x)=h(x)\psi(x).$$

因此
$$f(x)=h(x)[\psi(x)\varphi(x)],$$

即 $f(x)$能被 $h(x)$整除。

(二)若多項式 $f(x)$ 与 $g(x)$ 都能被多項式 $h(x)$ 整除，那末它們的和与差也能被 $h(x)$整除。

事实上，由等式

$$f(x)=h(x)\varphi(x) \text{ 与 } g(x)=h(x)\psi(x)$$

得
$$f(x)\pm g(x)=h(x)[\varphi(x)\pm\psi(x)].$$

(三)若多項式 $f(x)$ 与 $g(x)$中至少有一个能被多項式 $h(x)$整除，那末乘积 $f(x)g(x)$也能被 $h(x)$整除。

事实上，設 $f(x)$ 能被 $h(x)$ 整除：

$$f(x)=h(x)\varphi(x).$$

那末
$$f(x)g(x)=h(x)[\varphi(x)g(x)].$$

所以 $f(x)g(x)$ 能被 $h(x)$ 整除。

由(二)与(三)得出以下性質：

(四)若多項式 $f_1(x), f_2(x), \cdots, f_n(x)$ 中的每一个都能被多項式 $h(x)$ 整除，那末多項式

$$f_1(x)g_1(x)+f_2(x)g_2(x)+\cdots+f_n(x)g_n(x)$$

也能被 $h(x)$ 整除，此处 $g_1(x), g_2(x), \cdots, g_n(x)$ 是任意多項式。

(五)每一个多項式都能被任一零次多項式，亦即被体 P 的任一不等于零的元素整除。

事实上，設 $f(x)=a_0+a_1x+\cdots+a_nx^n$ 是任一多項式而 c 是体 P 的任一不等于零的元素。那末

$$f(x)=c\left(\frac{a_0}{c}+\frac{a_1}{c}x+\cdots+\frac{a_n}{c}x^n\right),$$

这就是説，$f(x)$ 能被 c 整除。

(六)每一个多項式 $f(x)$ 都能被 $cf(x)$ 整除，此处 c 是体 P 的任一不等于零的元素。

事实上，

$$f(x)=c^{-1}[cf(x)].$$

(七)两个多項式 $f(x)$ 与 $g(x)$ 可以互相整除的充分与必要条件是

$$f(x)=cg(x),$$

其中 c 是体 P 的一个不等于零的元素，換一句話說，$f(x)$ 与 $g(x)$ 最多只差一个零次的因式。

事实上，假定

$$f(x)=cg(x),$$

那末 $g(x)$ 整除 $f(x)$，而由性質(六) $f(x)$ 也整除 $g(x)$。

反过来,設 $f(x)$ 与 $g(x)$ 可以互相整除:

$$f(x)=g(x)\varphi(x), \tag{1}$$

$$g(x)=f(x)\psi(x). \tag{2}$$

若 $f(x)=0$ 那末

$$g(x)=0,\ \ \psi(x)=0.$$

而

$$f(x)=g(x).$$

若 $f(x)\neq0$, 考察由(1),(2)兩式导出的等式

$$f(x)=f(x)[\varphi(x)\psi(x)]$$

就可以看出, $\varphi(x)\psi(x)$ 是一个零次多項式,因而 $\varphi(x)$ 与 $\psi(x)$ 也都必須是零次多項式。这样, $\varphi(x)$ 是 P 的一个不等于零的元素 c, 而

$$f(x)=cg(x).$$

現在我們要証明一个重要定理, 它是多項式整除性理論的基础。通过这个定理以及它的証明我們也將获得一种方法, 来实际判断,一个已予多項式 $g(x)$ 是否能整除另一多項式 $f(x)$。到現在为止我們还沒有这样一种方法。

定理 設 $f(x)$ 与 $g(x)$ 是 $P[x]$ 的任意兩个多項式, 并且 $g(x)\neq0$。那末在 $P[x]$ 內可以找到多項式 $q(x)$ 与 $r(x)$, 使

$$f(x)=g(x)q(x)+r(x), \tag{3}$$

并且或者 $r(x)=0$, 或者 $r(x)$ 的次數小于 $g(x)$ 的次数。滿足以上条件的多項式 $q(x)$ 与 $r(x)$ 只有一对。

証 先証定理的前一部分。

若是 $f(x)=0$ 或 $f(x)$ 的次数小于 $g(x)$ 的次数,那末可取

$$q(x)=0,\ \ r(x)=f(x).$$

現在假定 $f(x)$ 的次数不小于 $g(x)$ 的次数。我們把 $f(x)$ 与 $g(x)$ 按 x 的降冪寫:

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n,$$

$$g(x)=b_0x^m+b_1x^{m-1}+\cdots+b_{m-1}x+b_m,$$

此处 $a_0 \neq 0$, $b_0 \neq 0$, 并且 $n \geqslant m$。

用初等代数中多项式除多项式的方法，自 $f(x)$ 减去 $g(x)$ 与 $\frac{a_0}{b_0}x^{n-m}$ 的积，那末 $f(x)$ 的最高項被消去，而我們得到 $P[x]$ 的一个多項式 $f_1(x)$:

$$f_1(x)=f(x)-\frac{a_0}{b_0}x^{n-m}g(x),$$

$f_1(x)$ 有以下性質：或者 $f_1(x)=0$ 或者 $f_1(x)$ 的次数小于 $f(x)$ 的次数 n。

若是 $f_1(x)\neq 0$, 并且 $f_1(x)$ 的次数 n_1 仍不小于 $g(x)$ 的次数 m, 那末用同样的步驟我們可以得到 $P[x]$ 的一个多項式 $f_2(x)$:

$$f_2(x)=f_1(x)-\frac{a_{10}}{b_0}x^{n_1-m}g(x),$$

这里 a_{10} 是 $f_1(x)$ 的最高系数。$f_2(x)$ 有以下性質：或者 $f_2(x)=0$ 或者 $f_2(x)$ 的次数小于 $f_1(x)$ 的次数 n_1。

这样作下去，由于多項式 $f_1(x)$, $f_2(x)$, …的次数是遞降的，最后一定达到这样的一个多項式 $f_k(x)$:

$$f_k(x)=f_{k-1}(x)\frac{a_{k-1,0}}{b_0}x^{n_{k-1}-m}g(x),$$

而 $f_k(x)=0$ 或 $f_k(x)$ 的次数小于 m。

总起来，我們得到等式：

$$f(x)-\frac{a_0}{b_0}x^{n-m}g(x)=f_1(x);$$

$$f_1(x)-\frac{a_{10}}{b_0}x^{n_1-m}g(x)=f_2(x);$$

…………………………………………

$$f_{k-1}(x)-\frac{a_{k-1,0}}{b_0}x^{n_{k-1}-m}g(x)=f_k(x).$$

把这些等式加起来，得

$$f(x)=g(x)\left(\frac{a_0}{b_0}x^{n-m}+\frac{a_{10}}{b_0}x^{n_1-m}+\cdots+\frac{a_{k-1,0}}{b_0}x^{n_{k-1}-m}\right)+f_k(x).$$