俄罗斯数学精品译丛

"十二五"国家重点图书

Advanced Algebra (II)

高等代数(下)

[苏]奥库涅夫 著　杨从仁 译

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

俄罗斯数学精品译丛

“十二五”国家重点图书

高等代数（下）

Advanced Algebra (II)

[苏] 奥库涅夫 著

杨从仁 译

HITP

哈尔滨工业大学出版社

HARBIN INSTITUTE OF TECHNOLOGY PRESS

内容简介

本书是根据莫斯科、列宁格勒国营工业及理论书藉出版社出版的奥库涅夫教授所著《高等代数》一出译出的. 本书分上、下两册，下册分为七章. 分别为任意体、有理数体及实数体、复数体上的多项式环、方程式的代数解法、消去法理论、圆规直尺作图法. 本册还包括上册的部分练习及习题答案.

本书适合于大学师生及数学竞赛爱好者阅读参考.

图书在版编目(CIP)数据

高等代数. 下/(苏)奥库涅夫著;杨从仁译. —哈尔滨:哈尔滨工业大学出版社,2016.1

ISBN 978-7-5603-5489-7

Ⅰ. ①高… Ⅱ. ①奥… ②杨… Ⅲ. ①高等代数 Ⅳ. ①O15

中国版本图书馆 CIP 数据核字(2015)第 176709 号

策划编辑 刘培杰 张永芹
责任编辑 张永芹 李 欣
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 哈尔滨市工大节能印刷厂
开 本 787mm×1092mm 1/16 印张 14.25 字数 271 千字
版 次 2016 年 1 月第 1 版 2016 年 1 月第 1 次印刷
书 号 ISBN 978-7-5603-5489-7
定 价 38.00 元

◎ 目录

任意体上的多项式环

第5章

§1　多项式环

未知量 x 的多项式(或者说 x 的有理整函数)的概念是由求解含有一个未知量的一次和高于一次代数方程式的问题而产生. 在远古时期就有人从事于这个问题的研究. 远在公元2000年前,在古巴比伦,就已经能够解决含有二次方程式的问题了. 利用造表的帮助甚至可以解决一些含有三次方程式的问题.

多项式的概念在代数上占着重要的位置,这个教程的以后各章都是集中的在讨论它. 因为我们准备尽可能地从一般的观点来叙述多项式理论,所以我们先讲在任意一个没有零因子和具有单位元素的交换环上的多项式的定义.

设 R 是一个没有零因子和具有单位元素 e 的交换环. 再设 Ω 是 R 的某一个交换扩环①,且 R 的单位元素 e 亦为 Ω 的单位元素. 今在 Ω 中任取一个元素 α,利用加法和乘法的运算作 α 与 R 的元素的乘积与和,就会得出含于 Ω 而形式如下的元素

$$A_1\alpha^{k_1}+A_2\alpha^{k_2}+\cdots+A_s\alpha^{k_s}\quad (s\geqslant 1) \tag{1}$$

式中的 $k_1,\cdots,k_s$ 代表互不相等的非负整数,$A_1,\cdots,A_s$ 代表 R 的元素.

式(1)叫作元素 α 在环 R 上的多项式. 每一个 $A_i\alpha^{k_i}$ 都叫作这个多项式的项,A_i 叫作多项式的系数,k_i 叫作项 $A_i\alpha^{k_i}$ 的次数. 元素

① Ω 可能含零因子,也可能不含零因子.

α 在环 R 上的多项式常用$f(\alpha)$,$g(\alpha)$,$h(\alpha)$等来表示.

由上述多项式的定义可以得出结论:在 R 上的多项式 $f(\alpha)$ 可以看作 Ω 的元素,但两个多项式的相等必须理解为环 Ω 内两个元素相等的意义.

令 $R[\alpha]$ 代表 α 在环 R 上的一切多项式的集合. 这个集合显然是 Ω 的一个部分集合①. 现在我们证明 $R[\alpha]$ 是环 Ω 的一个子环同时是环 R 的一个扩环.

证明 集合 $R[\alpha]$ 内的元素的加法满足交换律是无需证明的,因为交换律既然对 Ω 的元素的加法成立,所以对于 Ω 的一部分 $R[\alpha]$ 当然成立. 同理,集合 $R[\alpha]$ 内的加法和乘法运算满足结合律和分配律. 其次,利用环 Ω 内的元素的加法和乘法运算的一般性质,我们可以证明在 $R[\alpha]$ 中这些运算是闭合的.

设

$$f(\alpha)=A_1\alpha^{k_1}+\cdots+A_s\alpha^{k_s}$$
$$g(\alpha)=B_1\alpha^{l_1}+\cdots+B_t\alpha^{l_t}$$

是元素 α 在环 R 上的任意两个多项式. 由此

$$f(\alpha)+g(\alpha)=A_1\alpha^{k_1}+\cdots+A_s\alpha^{k_s}+B_1\alpha^{l_1}+\cdots+B_t\alpha^{l_t}$$

集合同类项得

$$f(\alpha)+g(\alpha)=C_1\alpha^{m_1}+\cdots+C_q\alpha^{m_q}$$

式中的 $C_1,\cdots,C_q$ 代表 R 的元素. 换句话说,我们同样得出元素 α 在环 R 上的一个多项式.

要计算乘积$f(\alpha)g(\alpha)$,必须利用和与和相乘的规则

$$(a_1+a_2+\cdots+a_s)(b_1+b_2+\cdots+b_t)=a_1b_1+\cdots+a_1b_t+\cdots+a_sb_t$$

这个规则对每一个环都成立. 由于这个规则,要求$f(\alpha)$和 $g(\alpha)$的乘积,必须先使多项式$f(\alpha)$的每一项 $A_i\alpha^{k_i}$和多项式 $g(\alpha)$的每一项 $B_j\alpha^{l_j}$相乘,然后再利用乘法的交换律和结合律把这个乘积$(A_i\alpha^{k_i})(B_j\alpha^{l_j})$变成

$$A_iB_j\alpha^{k_i+l_j}$$

最后再集合同类项. 经过这样的运算所得的结果显然也是 α 在环 R 上的一个多项式.

现在我们证明,在 $R[\alpha]$ 内有零元素和加法逆元素存在.

在集合 $R[\alpha]$的元素中,必须含有 0,因为 0 也可以看作是 α 的一个多项式,不过这个多项式的所有系数都等于零而已.

$R[\alpha]$内每一个多项式

$$f(\alpha)=A_1\alpha^{k_1}+\cdots+A_s\alpha^{k_s}$$

的加法逆元素同样是含于 $R[\alpha]$的多项式

$$h(\alpha)=(-A_1)\alpha^{k_1}+\cdots+(-A_s)\alpha^{k_s}$$

---

① $R[\alpha]$也可能和 Ω 一致.

因为

$$
\begin{aligned}
f(\alpha)+h(\alpha)=&A_1\alpha^{k_1}+\cdots+A_s\alpha^{k_s}+(-A_1)\alpha^{k_1}+\cdots+(-A_s)\alpha^{k_s}=\\
&[A_1\alpha^{k_1}+(-A_1)\alpha^{k_1}]+\cdots+[A_s\alpha^{k_s}+(-A_s)\alpha^{k_s}]=\\
&[A_1+(-A_1)]\alpha^{k_1}+\cdots+[A_s+(-A_s)]\alpha^{k_s}=\\
&0\cdot\alpha^{k_1}+\cdots+0\cdot\alpha^{k_s}=0
\end{aligned}
$$

我们以后常用 $-f(\alpha)$ 代表 $h(\alpha)$，并把它叫作多项式 $f(\alpha)$ 的加法逆多项式.

由上述我们可以看出，对于 Ω 内定义的加法和乘法，集合 $R[\alpha]$ 构成一个环，换句话说，$R[\alpha]$ 是 Ω 的一个子环.

最后，我们还需要证明 $R[\alpha]$ 是 R 的扩环. 为了这个目的，我们必须证明 R 所有的元素都含于 $R[\alpha]$.

0 含于 $R[\alpha]$ 已经证明. 次在 R 内任取一个非零元素 c. c 可以看作元素 α 在环 R 上的多项式，因为我们可以把它写成 $c=c\alpha^0$. 因此元素 c 也必须含于 $R[\alpha]$.

我们常把 R 的扩环 $R[\alpha]$ 叫作元素 α 在 R 上的多项式环.

我们还要再一次指出：因为 $R[\alpha]$ 是交换环 Ω 的一个子环，所以 $R[\alpha]$ 也是一个交换环. 由于 $R[\alpha]$ 是 Ω 的部分集合和含有 α，所以在 $R[\alpha]$ 内可能有零因子存在，这一点是依赖于环 Ω 和所取的元素 α.

现在我们举一个例子解释某一个元素的多项式这一概念.

例 1 设 Ω 是实数体 D，R 是整数环 C. 在 D 中取元素 $\alpha=\sqrt{2}$，我们试研究环 $C[\sqrt{2}]$.

解 依照定义，这个环必须包含 $\sqrt{2}$ 在整数环上的所有多项式，换句话说，必须包括形式如

$$A_1(\sqrt{2})^{k_1}+\cdots+A_s(\sqrt{2})^{k_s}\quad(s\geqslant 1)\tag{2}$$

的一切元素. 式中的 $k_1,\cdots,k_s$ 代表不同的非负整数，$A_1,\cdots,A_s$ 代表整数. 例如取 $s=3,k_1=3,k_2=2,k_3=0,A_1=3,A_2=5,A_3=7$，我们就得出 $C[\sqrt{2}]$ 的一个元素

$$3(\sqrt{2})^3-5(\sqrt{2})^2+7(\sqrt{2})^0$$

由于 $(\sqrt{2})^2=2$，所以这个元素可以写成

$$6\sqrt{2}-3$$

一般说来，根据等式 $(\sqrt{2})^2=2$，我们可以把 $C[\sqrt{2}]$ 的每一个元素写成一个二项式 $a+b\sqrt{2}$，式中的 a,b 代表整数. 我们从这里可以看出，用 $\alpha=\sqrt{2}$ 去表示 $C[\sqrt{2}]$ 的每一个元素的方法就不是唯一的：$C[\sqrt{2}]$ 的同一个元素既可以表示成含 $\sqrt{2}$ 的高于一次幂的形式(2)，又可以表示成只含 $\sqrt{2}$ 的一次幂的二项式

$a+b\sqrt{2}$. 这一个现象是由于 $\alpha=\sqrt{2}$ 满足等式 $\alpha^2-2=0$ 而起，这个等式的左端是 α 在整数环上系数不为零的多项式 α^2-2.

根据这个观察的结果，我们就得出两个非常重要的概念，就是所谓的代数元素和超越元素.

假若 Ω 的元素 α 满足等式

$$A_1\alpha^{k_1}+\cdots+A_s\alpha^{k_s}=0$$

等式的左端是 α 在环 R 上的一个系数 A_i 不为零的多项式，我们就说 α 是对于环 R 的一个代数元素.

反之，假若 α 在 R 上的多项式限于且仅限于所有的系数 $A_1,\cdots,A_s$ 为零时始终有上述等式成立，我们就说 α 是对于环 R 的一个超越元素.

因此 $\sqrt{2}$ 是关于整数环的一个代数元素.

在历史上，第一个超越元素的例子就是所谓的超越数，换句话说，就是对于整数环是超越元素的复数. 超越数的存在首先由刘维尔在 1851 年证明，之后，在 1873 年埃尔米堤发现自然对数底 e 的超越性. 利用埃尔米堤的思维方法，林得曼证明了 π——圆周长和直径的比——也是一个超越数. 要算苏联学者亚·俄·格尔冯德在 1929~1936 年的工作，使超越数理论的发展向前迈进了极为重要的一步. 格尔冯德证明了一个重要类型的数的超越性，由他的结果就可以断定 $2^{\sqrt{2}}$, $3^{\sqrt{5}}$（一般总的来说 $m^{\sqrt{n}}$，式中 $m>1$, n 代表一个整数，但 $\sqrt{n}$ 是无理数），e^{π}, $2^{i\sqrt{2}}$ 等的超越性.

以后我们常用最后几个拉丁字母 $x,y,z,\cdots$ 代表未知量. 从现在开始我们就专门来讨论含未知量的多项式，这种类型的多项式在代数上占着非常重要的位置.

我们容易证明，用 x 代表多项式环 $R[x]$ 的每一个元素的方法是唯一确定的，换句话说，多项式相等的条件可叙述如下：$R[x]$ 的多项式 $f(x)$ 和 $g(x)$，除去系数为零的项外，限于且仅限于两个所含的项完全一致时相等. [①]

设在多项式 $f(x)$ 和 $g(x)$ 中，除去系数等于零的项外，两者所含的项完全一致. 由多项式 $f(x)$ 减去多项式 $g(x)$，则所有不为零的项都相互消去，结果得 $f(x)-g(x)=0$，换句话说 $f(x)=g(x)$.

又设 $f(x)=g(x)$. 假若所给的条件不满足，$f(x)$ 必有系数不为零的某一项而不含于多项式 $g(x)$ 中，由此 $f(x)-g(x)$ 至少含有系数不为零的一项，但是 $f(x)-g(x)$ 同时又等于零，所以

$$f(x)-g(x)=C_1x^{k_1}+\cdots+C_qx^{k_q}=0 \quad (C_1\neq 0)$$

---

① 读者应当注意，这个性质是含未知量的多项式的特性. 从上面所举的例子我们可以知道，代数元素的多项式就不具备这个性质.

这个等式和 x 在 R 上的超越性相违反.

现在我们导入含未知量的多项式的次数的概念. 设

$$f(x)=A_1x^{k_1}+\cdots+A_sx^{k_s}$$

是 $R[x]$的任意一个多项式,并设 $f(x)$ 至少有一个系数不是零. 由于 x 的超越性,这样的一个多项式显然不等于零. 所谓这个多项式的次数是指系数不为零的各项的最高次数.

例如

$$f(x)=x^8+7x^5-0\cdot x^8+2x-1$$

就是在整数环上的一个五次多项式.

显然,我们可以把环 R 的每一个元素 $a\neq0$ 看作含未知量 x 的零次多项式,因为 $a=ax^0$. 至于 R 的零元素,我们可以把它看作没有次数的多项式,或者叫它是零多项式.

根据我们已经证明的多项式相等的条件,知道两个次数不同的含未知量的多项式决不会相等.

我们还应当注意,x 虽然是 Ω 的元素,但不是 R 的元素. 不仅如此,我们还可以证明,在 $R[x]$的多项式$f(x)$中,没有次数大于零的多项式能够等于环 R 的元素. 假若不然,设 $f(x)=a$,a 代表环 R 的一个元素. 结果,等式的左端是次数大于零的多项式,等式的右端是零次多项式或零多项式($a=0$). 这个等式显然和未知量的多项式的相等条件相抵触.

把 $R[x]$的多项式 $f(x)$的项依照未知量 x 的降幂排列,我们得出所谓的多项式的标准形式为

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n \tag{3}$$

式中的 n 代表一个非负整数,$a_0,a_1,\cdots,a_n$ 代表 R 的元素. 我们以后在实际的利用上,往往把多项式写成这个形式.

a_0x^n 叫作多项式的最高项,a_n 叫作多项式的绝对项. 最高项的系数 a_0 叫作多项式的最高系数.

显然,多项式(3)的次数限于且仅限于最高系数 a_0 不为零时始终等于 n. 至于其余的系数 $a_1,\cdots,a_n$ 可以部分为零或甚至于全为零.

为了方便,有时并不把项依照 x 的降幂排列,相反的,可以把项依照 x 的升幂排列即

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

和上面一样,$f(x)$的次数限于且仅限于 $a_n\neq0$ 时等于 n.

要研究未知量 x 的多项式环 $R[x]$的更多性质,我们先求这些多项式的加法和乘法规则. 为了这个目的把多项式的项按照升幂排列.

设

$$f(x)=a_0+a_1x+\cdots+a_nx^n$$
$$g(x)=b_0+b_1x+\cdots+b_mx^m$$
是 $R[x]$ 的任意两个多项式. 为了更确定起见,不妨设 $n\geqslant m$. 使这两个多项式相加得

$$f(x)+g(x)=(a_0+a_1x+\cdots+a_nx^n)+(b_0+b_1x+\cdots+b_mx^m)$$

先去括弧再集同类项,提出同类项的公因子(因为我们讨论的是环 Ω 的元素,所以这个运算是完全合理的)后得

$$f(x)+g(x)=c_0+c_1x+\cdots+c_nx^n \tag{4}$$

式中的 $c_i=a_i+b_i(i=0,1,\cdots,n)$,但 $n>m$ 时,我们必须假设 $b_{m+1}=\cdots=b_n=0$.

根据上面的结果,我们得到了一个非常简单的多项式加法规则:把 $f(x)$ 和 $g(x)$ 的同次幂的系数相加就得出这两个多项式的和的系数 c_i.

由等式(4),我们知道两个多项式的和的次数不超过这两个多项式次数较高的一个的次数.

利用和与和相乘的规则,容易求出多项式的乘积 $f(x)\cdot g(x)$. 集合同类项后再提出公因子得

$$f(x)g(x)=a_0b_0+(a_0b_1+a_1b_0)x+\cdots+a_nb_mx^{n+m} \tag{5}$$

根据等式(5),可以得出含未知量 x 的多项式环 $R[x]$ 的一个重要性质. 就是说,$R[x]$ 是一个不含零因子的环. 事实上,如果 $f(x)\neq 0$ 和 $g(x)\neq 0$,那么这两个多项式的每一个都具有一个完全确定了的次数. 设 $f(x)$ 的次数是 n,$g(x)$ 的次数是 m,于是便有 $a_n\neq 0$ 和 $b_m\neq 0$. 由此乘积 a_nb_m 不等于零,因为 R 不含零因子,从这里,我们再去研究一下式(5),便可以看出,如果 $a_n\neq 0$,$b_m\neq 0$,所以由 $a_nb_m\neq 0$ 和 x 的超越性,乘积 $f(x)g(x)$ 也不等于零.

不仅如此,由等式(5)我们还可以看出:$R[x]$ 的两个多项式的乘积的次数等于这两个多项式的次数的和.

我们还要附带提一下,规则(4)和(5)不仅对于含未知量的多项式成立,对于任意一个元素 α 的多项式也同样成立,因为这些规则仅仅根据环 Ω 的元素的加法和乘法运算的一般性质而得来. 但是,在 α 是代数元素的时候,$R[\alpha]$ 可能含有零因子. 这是不足为奇的,因为未知量的多项式环不含零因子,主要是由 x 的超越性而起. 现在我们举一个例子以资说明.

例 2 我们来研究形式如

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

的二阶矩阵的集合 M,式中 a,b 代表任意的整数. 读者容易证明,关于矩阵的乘法和加法,集合 M 构成一个交换环. M 含有单位元素,因为二阶单位矩阵

$$\boldsymbol{e}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

显然就是 M 的单位元素. 我们还要指出,二阶零矩阵

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

就是 M 的零元素. 现在我们把 M 当成 Ω 看待. 其次,不难看出,所有形式如

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

的二阶矩阵(a 代表任意的整数)的集合 N 可以看作是 M 的一个子环. N 含有单位元素,但不含零因子.

今由 M 中取出矩阵

$$\boldsymbol{\alpha} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

因为单位元素 $\boldsymbol{e}$ 含于 N 和 $\boldsymbol{\alpha}^2 = \boldsymbol{e}$,所以 $\boldsymbol{\alpha}$ 是关于环 N 的一个代数元素.

现在我们证明 $\boldsymbol{\alpha}$ 的多项式环 $N[\boldsymbol{\alpha}]$ 含有零因子. 为了这个目的取 $\boldsymbol{\alpha}$ 在环 N 上的两个多项式

$$f(\boldsymbol{\alpha}) = \boldsymbol{\alpha} - \boldsymbol{e}, \quad g(\boldsymbol{\alpha}) = \boldsymbol{\alpha} + \boldsymbol{e}$$

因为

$$\boldsymbol{\alpha} - \boldsymbol{e} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & -2 \end{pmatrix} \neq \boldsymbol{0}$$

$$\boldsymbol{\alpha} + \boldsymbol{e} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \neq \boldsymbol{0}$$

所以 $f(\boldsymbol{\alpha})$ 和 $g(\boldsymbol{\alpha})$ 都不等于零,但是 $f(\boldsymbol{\alpha})$ 和 $g(\boldsymbol{\alpha})$ 的乘积却等于零

$$\begin{aligned}(\boldsymbol{\alpha} - \boldsymbol{e})(\boldsymbol{\alpha} + \boldsymbol{e}) = {} & \boldsymbol{\alpha}^2 + \boldsymbol{\alpha}\boldsymbol{e} - \boldsymbol{e}\boldsymbol{\alpha} - \boldsymbol{e}^2 = \\ & \boldsymbol{\alpha}^2 + \boldsymbol{\alpha} - \boldsymbol{\alpha} - \boldsymbol{e}^2 = \\ & \boldsymbol{e} - \boldsymbol{e}^2 = \boldsymbol{e} - \boldsymbol{e} = 0\end{aligned}$$

最后这个结果,自然还可以直接证明为

$$(\boldsymbol{\alpha} - \boldsymbol{e})(\boldsymbol{\alpha} + \boldsymbol{e}) = \begin{pmatrix} 0 & 0 \\ 0 & -2 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \boldsymbol{0}$$

现在再回来研究含未知量 x 的多项式环. 我们现在来看一下除法. 发现,纵使 R 是一个体,在 $R[x]$ 内除法是不一定可以施行的,换句话说,设 $f(x)$ 和 $g(x) \neq 0$ 是 $R[x]$ 的两个已知多项式,$R[x]$ 内不一定有第三个多项式 $h(x)$ 存在而满足

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

例如,如果 $f(x) = x + a$,$g(x) = x^2 + a$(a 代表 R 的某一个不为零的元素),那么就不可能在 $R[x]$ 求出一个多项式 $h(x)$ 满足等式 $x + a = (x^2 + a)h(x)$,因为 $(x^2 + a) \cdot h(x)$ 的次数高于 $x + a$ 的次数.

根据上述结果，$R[x]$是一个不含零因子的交换环，但不是一个体.

设在 Ω 中或在环 R 的另外一个扩环 Ω' 中另取一个未知量 y①. 我们现在证明 y 在 R 上的多项式环和原来的环 $R[x]$（严格地说，除去一一同构不计外）是相同的. 换句话说，有下述定理成立：

含未知量的多项式环的唯一性定理 设 x, y 是含于环 R 的相同或不相同的扩环 Ω 和 Ω' 的两个未知量，则 x 在 R 上的多项式环和 y 在 R 上的多项式环一一同构.

证明 令 $R[x]$ 的每一个多项式和 $R[y]$ 中具有相同系数的多项式成对应，即

$$f(x)=a_0+a_1x+\cdots+a_nx^n \to f(y)=a_0+a_1y+\cdots+a_ny^n \tag{6}$$

首先我们证明：这个对应(6)不仅是唯一的，而且是一个一一对应. 为了这个目的，在 $R[x]$ 中另取一个多项式

$$g(x)=b_0+b_1x+\cdots+b_mx^m$$

根据所给的对应关系，$g(x)$ 必须对应 $g(y)$，即

$$g(x)=b_0+b_1x+\cdots+b_mx^m \to g(y)=b_0+b_1y+\cdots+b_my^m$$

设 $f(x)=g(y)$. 于是，根据含未知量的多项式的相等条件，$f(y)$ 和 $g(y)$ 的差仅仅是系数等于零的项. 由此得出，$f(y)$ 和 $g(y)$ 的同次幂的项的系数必须相等，换句话说，$b_0=a_0, b_1=a_1$ 等等. 由于系数的一致，所以 $f(x)$ 等于 $g(x)$. 这样，我们就证明了 $R[x]$ 内不相等的多项式必须对应 $R[y]$ 内不相等的多项式，换句话说，对应(6)是一个一一对应.

现在我们再看和 $f(x)+g(x)$，$f(x)g(x)$ 对应的多项式是什么.

根据多项式的加法规则，在 $n \geqslant m$ 时有

$$f(x)+g(x)=h(x)=c_0+c_1x+\cdots+c_nx^n$$

式中 $c_i=a_i+b_i(i=0,1,\cdots,n)$，但 $n>m$ 时，必须令 $b_{m+1}=0,\cdots,b_n=0$. $h(x)$ 应当和具有相同系数的 $h(y)$ 成对应，即

$$h(x)=c_0+c_1x+\cdots+c_nx^n \to h(y)=c_0+c_1y+\cdots+c_ny^n$$

但是在环 $R(y)$ 里，显然有同样的加法规则(4)成立. 因而

$$f(y)+g(y)=c_0+c_1y+\cdots+c_ny^n=h(y)$$

所以

$$f(x)+g(x) \to f(y)+g(y)$$

同理，根据多项式的乘法规则(5)，我们得出这样的结论：乘积 $f(x)g(x)$ 必须和 $f(y)g(y)$ 成对应.

综合上述，我们就证明了对应(6)是环 $R[x]$ 和环 $R[y]$ 的一个一一同构，

---

① 和 Ω 一样，我们自然也假设 Ω' 是一个交换环. R 的单位元素亦为 Ω' 的单位元素.

定理也就得到了证明.

有时为了简单,我们需要把未知量 x 代入式

$$y=c_0x^n+c_1x^{n-1}+\cdots+c_n \quad (c_0\neq 0)$$

等式的右端是 $R[x]$ 的某一个次数不小于 $1(n\geqslant 1)$ 的多项式,等式左端的 y 被看作是新的未知量.

例如,在二次多项式

$$x^2+2a_1x+a_2$$

中,令 $x=y-a_1$ 则得出一个更简的含未知量 y 的多项式

$$y^2+b$$

式中 $b=a_2-a_1^2$. 这个多项式的形式较原多项式简单,因为 y 的一次项的系数是零.

根据下述的事实,这种置换是完全合理的:$R[x]$ 的每一个 $n\geqslant 1$ 次多项式都是关于 R 的一个超越元素.

证明 假若不然,设

$$y=c_0x^n+c_1x^{n-1}+\cdots+c_n \quad (c_0\neq 0,n\geqslant 1)$$

是关于 R 的一个代数元素. 这就是说,我们可以选择一个非负整数 k 和选择环 R 的元素 $a_0\neq 0,a_1,\cdots,a_k$ 而使 y 满足等式

$$a_0y^k+a_1y^{k-1}+\cdots+a_k=0 \tag{7}$$

显然,$k\neq 0$,因为 $k=0$ 时,等式(7)的左端只剩下一个 a_0,但 a_0 是假设不为零的.

根据上述可令 $k\geqslant 1$. 把 y 的值代入等式(7)得

$$a_0(c_0x^n+\cdots+c_n)^k+a_1(c_0x^n+\cdots+c_n)^{k-1}+\cdots+a_k=0$$

除去括弧后再集合同类项则有

$$a_0c_0^kx^{kn}+\cdots+(a_0c_n^k+a_1c_n^{k-1}+\cdots+a_k)=0 \tag{8}$$

因为 x 是关于 R 的超越元素,所以等式(8)所有的系数都必须是零,特别 $a_0c_0^k=0$. 由于 R 不含有零因子,所以从最后这个等式得 $a_0=0$ 或 $c_0=0$,无论是哪一个情形都和 $a_0\neq 0,c_0\neq 0$ 的假设相冲突①.

对于超越元素(未知量)的概念我们已经谈得够多了. 现在发生这样一个问题,就是关于任意一个环 R 这种元素是否存在. 这个问题的完全回答将在第 8 章讲述;在那里我们可以证明:对于每一个不含零因子和具有单位元素的交换环 R 都有一个交换扩环 Ω 存在,在 Ω 中含有无限多关于 R 的超越元素.

---

① 至于零次多项式或零多项式,它们已经是关于 R 的代数元素了. 事实上,若 $y=0$ 是 R 的某一个元素,我们就可以选择 k 和系数 $a_0\neq 0,a_1,\cdots,a_k$ 而使 $a_0c^k+a_1c^{k-1}+\cdots+a_k=0$. 因为令 $k=1,a_0=e$, $a_1=-c$(e 代表 R 的单位元素),就有 $c-c=0$. 在此,我们有理由令 $a_1=-c$,因为 $-c$ 是 R 的元素.

在结束这节前，我们再引入多项式的值这一概念. 这个概念在将来要遇到. 设

$$f(x)=a_0+a_1x+\cdots+a_nx^n \quad (a_n\neq 0)$$

是 $R[x]$ 的任意一个多项式. 假若用 R 的任意一个元素 c 去代替未知量 x，我们就得出一个含于 R 的元素

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

元素 d 叫作多项式 $f(x)$ 在未知量的值 $x=c$ 的时候的值. 因为 $a_0+a_1c+\cdots+a_nc^n$ 正是元素 c 的多项式，所以我们可以用 $f(c)$ 代表 d. 我们强调指出，所谓未知量 x 的值，就是指环 R 的元素.

显然，假若 $f(x)=g(x)$，对于 R 的任意元素 c，则有 $f(c)=g(c)$. 反之，不一定成立：$f(x)$ 和 $g(x)$ 仅可以不相等，但是对于 R 的任意元素 c 可能有 $f(c)$ 等于 $g(c)$，为了说明，举例如下.

例 3 设 R 是只含有零元素 0 和单位元素 e 的体. 这样一个体我们在前面已经遇见过(参考高等代数(上)的第 3 章 §4). 我们来研究在这个体上的两个多项式

$$f(x)=x^2,g(x)=x$$

$f(x)$ 和 $g(x)$ 不相等，因为 $f(x)$ 和 $g(x)$ 的幂不同. 但是在 $x=0$ 和 $x=e$ 的时候，这两个多项式的值是一样的，即

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

在函数论中，多项式 $f(x)$ 被看作是变数 x 的函数，变数 x 系假定它取某一个已知区域内所有的值(例如，取实数体内所有的值). 从函数论的观点，假若 x 任取已知区域内一个值，函数 $f(x)$ 和 $g(x)$ 的值都相等，我们就可以把 $f(x)$ 和 $g(x)$ 看作相等. 但是由上面这个例子，我们就可以知道这个观点对于任意一个不含零因子和具有单位元素的交换环不能适用，因为在函数论中所讲的多项式的相等和我们这里所谓多项式的相等条件并不一致.

根据上述的理由，所以在研究多项式一般的理论的时候，我们避免用"变数"这一术语，而代以"未知量"这一个名词.

虽然如此，但是以后就会看出，对于任意一个不含零因子和具有单位元素且含有无限多元素的交换环，特别是对于无限环，由函数论的观点看多项式仍然是有效的，在某些情形下(例如实数体和复数体的情形)这个观点甚而占着非常重要的位置.

现在我们再回到多项式的值的问题. 设

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

我们容易证明，把 x 代以环 R 的元素 c 后，这些等式仍然保持成立，换句话说，由上面的等式有

$$f(c)+g(c)=h(c), f(c)g(c)=k(c)$$

§2 多项式环内的可除性

体是一个不含零因子和具有单位元素的交换环的特别情形. 现在我们要研究在某一个体 P 上的多项式是否还具有某些其他的性质. 所谓在某一个体 P 上的多项式就是指系数属于这个体 P 的多项式. 在这一节里,我们不对体 P 加以限制,换句话说,P 可以是任意的一个体. 因此,我们所得的结论就不因为 P 是实数体,或另外的数体,或不是数体而受到影响.

不久我们就会看出,关于加法和乘法的运算,多项式有许多地方和整数相似. 在多项式环 $P[x]$ 中含有除式的除法定则首先成立. 换句话说,有下述定理成立.

定理 1(含有余式的除法定则) 设 $f(x)$ 和 $g(x)\neq 0$ 是 $P[x]$ 的任意两个多项式,那么在 $P[x]$ 内可以选出两个多项式 $q(x)$ 和 $r(x)$ 满足

$$f(x)=g(x)q(x)+r(x) \tag{1}$$

且 $r(x)$ 的次数小于 $g(x)$ 的次数. 不仅如此,满足这个等式的 $q(x)$ 和 $r(x)$ 还是唯一的.

证明 设

$$f(x)=a_0+a_1x+\cdots+a_nx^n \quad (a_n\neq 0)$$

$$g(x)=b_0+b_1x+\cdots+b_mx^m \quad (b_m\neq 0)$$

关于这两个多项式的次数有两个可能性:$n<m$ 或 $n\geqslant m$.

在第一个情形下,不妨设 $q(x)=0, r(x)=f(x)$,这样,等式(1)是显然成立的. 在第二个情形下可由 $f(x)$ 减去乘以 $a_nb_m^{-1}x^{n-m}g(x)$,有

$$f(x)-a_nb_m^{-1}x^{n-m}g(x)=h(x)$$

由此 $f(x)$ 的最高项 a_nx^n 就被消去,$f(x)$ 的次数也随之降低

$$h(x)=a_0'+a_1'x+\cdots+a_{n_1}'x^{n_1} \quad (a_{n_1}'\neq 0)$$

式中 $n_1<n$. 假若 $h(x)$ 的次数远大于或等于 $g(x)$ 的次数,我们就可以重复上述方法把 $h(x)$ 的次数降低,换句话说,作下面的差就可以消去 $h(x)$ 的最高项 $a_{n_1}'x^{n_1}$,有

$$h(x)-a_{n_1}'b_m^{-1}x^{n_1-m}g(x)=k(x)$$

继续施行上述方法,最后一定得到一个次数较 $g(x)$ 的次数低的多项式 $r(x)$,因为非负整数 $n, n_1, \cdots$ 是不能无限制减小的. 根据上述得

$$
\begin{cases}
f(x)-a_nb_m^{-1}x^{n-m}g(x)=h(x)\\
h(x)-a'_{n_1}b_m^{-1}x^{n_1-m}g(x)=k(x)\\
\qquad\vdots\\
p(x)-a_{n_s}^{(s)}b_m^{-1}x^{n_s-m}g(x)=r(x)
\end{cases}
\tag{2}
$$

使等式(2)的两端分别相加后再简化,则有

$$f(x)-g(x)q(x)=r(x)$$

或

$$f(x)=g(x)q(x)+r(x)$$

式中

$$q(x)=a_nb_m^{-1}x^{n-m}+a'_{n_1}b_m^{-1}x^{n_1-m}+\cdots+a_{n_s}^{(s)}b_m^{-1}x^{n_s-m}$$

实际说来,我们在这里不过是重复了初等代数上有名的多项式除多项式的方法.

我们不难看出,$q(x)$和$r(x)$都是$P[x]$的多项式.因为根据上述方法,$q(x)$和$r(x)$可由体P的元素施以减法、乘法和除法的运算而得来,但是经过这些运算后所得的元素同样的也含于体P.

定理的第一部分得到了证明.我们现在来证明,$q(x)$和$r(x)$是唯一确定的.设在$P[x]$内还有另外两个多项式$q_1(x)$和$r_1(x)$,满足

$$f(x)=g(x)q_1(x)+r_1(x) \tag{3}$$

式中$r_1(x)$的次数低于$g(x)$的次数.由式(1)减去式(3),则有

$$[q(x)-q_1(x)]g(x)=r_1(x)-r(x) \tag{4}$$

其次设$r_1(x)\neq r(x)$.由$r_1(x)-r(x)\neq 0$得$q(x)-q_1(x)\neq 0$,否则由等式(4)就有$r_1(x)-r(x)=0$.式(4)右端的多项式$r_1(x)-r(x)$是一个次数较$g(x)$次数低的多项式,式(4)左端是一个次数等于或高于$g(x)$的次数的多项式.由此就得出一个不合理的结论,因为这和多项式相等的条件是矛盾的.因而,必须有$r_1(x)-r(x)=0$和$q(x)-q_1(x)=0$,换句话说$r_1(x)=r(x)$,$q_1(x)=q(x)$.由此就完全证明了所要的定理.

$q(x)$叫作$f(x)$除以$g(x)$所得的商,$r(x)$叫作$f(x)$除以$g(x)$所得的除式.

设想给定了$P[x]$的两个多项式$f(x)$和$g(x)$,假若在环$P[x]$内存在一个多项式$h(x)$满足$f(x)=g(x)h(x)$,我们就说多项式$f(x)$可以被$g(x)$整除.$g(x)$叫作$f(x)$的除式.

根据含有除式的除法定则可以判断一个多项式$f(x)$是否可以被另外一个多项式$g(x)$所整除.多项式$f(x)$可以被$g(x)$整除的充分必要条件是$f(x)$除以$g(x)$所得的余式等于零.

事实上,若余式$r(x)$等于零,等式(1)就可以写成$f(x)=g(x)q(x)$,这就是说$f(x)$可以被$g(x)$所整除.反之,若$f(x)$可以被$g(x)$所整除,我们就可以在