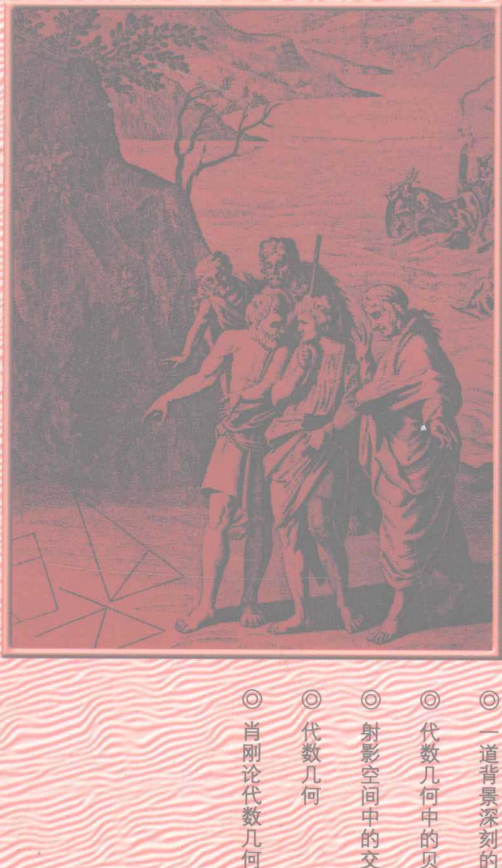
《数学中的小问题大定理》丛书（第一辑）

代数几何中的贝祖定理

——从一道IMO试题的解法谈起



刘培杰 编著

◎一道背景深刻的IMO试题

◎代数几何中的贝祖定理的简单情形

◎射影空间中的交

◎代数几何

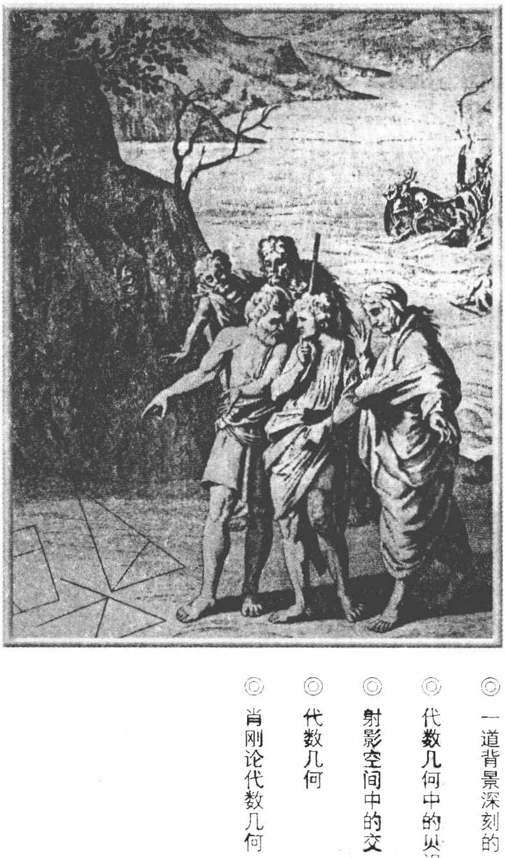
◎肖刚论代数几何

《数学中的小问题大定理》丛书（第一辑）

代数几何中的贝祖定理

——从一道IMO试题的解法谈起

刘培杰 编著



◎一道背景深刻的IMO试题

◎代数几何中的贝祖定理的简单情形

◎射影空间中的交

◎代数几何

◎肖刚论代数几何

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

内容简介

代数几何是数学中的一个重要分支，国内外很多著名的数学家都从事过对它的研究。本书从一道IMO试题的解法谈起，详细介绍了代数几何中的贝祖定理。全书共分五章，分别为：一道背景深刻的IMO试题、多项式的简单预备知识、代数几何中的贝祖定理的简单情形、射影空间中的交、代数几何、肖刚论代数几何。

本书可供从事这一数学分支或相关学科的数学工作者、大学生以及数学爱好者研读。

图书在版编目(CIP)数据

代数几何中的贝祖定理：从一道IMO试题的解法谈起/《代数几何中的贝祖定理：从一道IMO试题的解法谈起》刘培杰编著. —哈尔滨：哈尔滨工业大学出版社，2012.7

ISBN 978-7-5603-3640-4

Ⅰ.①代… Ⅱ.①代… Ⅲ.①代数几何 Ⅳ.①O187

中国版本图书馆CIP数据核字(2012)第149739号

策划编辑　张永芹　李子江
责任编辑　王　慧　张　佳
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×960mm　1/16　印张5.75　字数55千字
版　　次　2012年7月第1版　2012年7月第1次印刷
书　　号　ISBN 978-7-5603-3640-4
定　　价　18.00元

◎ 目录

第 1 章 一道背景深刻的 IMO[①] 试题

设 n 是一个正整数,考虑 $S=\{(x,y,z)\mid x,y,z=0,1,2,\cdots,n,x+y+z>0\}$ 这样一个三维空间中具有 $(n+1)^3-1$ 个点的集合.问最少要多少个平面,它们的并集才能包含 S 但不包含 $(0,0,0)$.

(这是一道 48 届 IMO 试题.其解答颇费周折)

分析 二维的情况比较简单,方法如下:

我们可以考虑最外一圈的 $4n-1$ 个点.如果没有直线 $x=n$ 或 $y=n$,那么每条直线最多过这 $4n-1$ 个点中的两个.故至少需要 $2n$ 条直线.如果有直线 $x=n$ 或 $y=n$,那么将此直线和其上的点去除,再考虑最外一圈,只不过点数变成了 $4n-3$ 个,需要至少 $2n-1$ 条直线,再加上去掉的那条正好 $2n$ 条.如果需要多次去除直线,以至于比如 $x=1,x=2,\cdots,x=n$ 这

① 国际数学奥林匹克(International Mathematical Olympiad)的英文缩写为 IMO.——编者注

所有 n 条直线全部被去除了,那么剩下$(0,1),(0,2),\cdots,(0,n)$至少还需要 n 条直线去覆盖,$2n$ 条亦是必须的. $2n$ 条显然是可以做到的,所以二维的最终结果就是 $2n$.

但是将这种方法推向三维的时候,会出现困难,因为现在用来覆盖的不是直线而是平面,平面等于有了三个自由变量,而且不容易选取标志点来进行考察. 当然,我们要坚信一个事实,那就是答案一定是 $3n$,否则题目是没有办法解决的. 在这个前提下,通过转化,将这个看起来是一道组合计数的题目变成一道代数题.

解法 1　首先第一步,我们就要将每个平面表示成一个三元一次多项式的形式. 比如平面 $x+y+z=1$ 就表示成 $x+y+z-1$,将所有这些平面均表述成如此形式后,我们将这些多项式都乘起来. 下面我们需要证明的只有一点,就是乘出来的多项式,至少具有 $3n$ 次($3n$ 个平面是显然可以做到的,只要证明这点,$3n$ 就是最佳答案了).

这个乘出来的多项式具有什么特点呢? 它在 x,y,z 均等于 0 时不等于 0,在 x,y,z 取其他 $0\sim n$ 之间的数值时,其值均为 0. 我们发现,当多项式中某一项上具有某个字母的至少 $n+1$ 次时,我们可以将其降低为较低的次数. 我们用的方法就是,利用仅仅讨论 x,y,z 在取 $0,1,2,\cdots,n$ 这些值时多项式的取值这一事实,在原多项式里可以减去形如 $x(x-1)(x-2)\cdots(x-n)$ 或者此式子的任何倍数的式子. 从而,如果多项式中某一项的某个字母次数超过 n,可以用此法将其变成小于或等于 n.

我们假设用此法变换后剩余的多项式是 F,显然

F 的次数不大于原乘积多项式的次数. 我们下面需要证明的,就是 F 中 $x^n y^n z^n$ 这一项系数非零(F 中只有这一项次数是 $3n$). 要想证明这样的问题,我们需要证明二维即两个未知数时的两个引理.

引理 1　一个关于 x 和 y 的实系数多项式,x 和 y 的次数均不超过 n. 如果此多项式在 $x=y=0$ 时非零,在 $x=p,y=q(p,q=0,1,2,\cdots,n$ 且 p,q 不全为 $0)$ 时为零,那么此多项式中 $x^n y^n$ 的系数必然不是零.

证明　假设 $x^n y^n$ 的系数是 0,我们知道,当假设 $y=1,2,3,\cdots,n$ 中任意一值时,将 y 代入多项式,所得的多项式必须都是零多项式. 这是由于当 y 取这些值时,此多项式为关于 x 的不超过 n 次的多项式,却有 $n+1$ 个零点,所以假设 y 是常数,按 x 的次数来整理该多项式,x^n 的次数是一个关于 y 的不超过 $n-1$ 次的多项式,但是却有 n 个零点,故为零多项式. 因此,当按照 x 的次数来整理多项式时,x 的最高次最多是 $n-1$ 次. 现令 $y=0$ 代入多项式,转化为关于 x 的多项式,最多 $n-1$ 次,但是有 n 个零点$(1,2,\cdots,n)$. 因此,这个多项式应当是零多项式,但是这与此多项式在 $x=y=0$ 时非零矛盾.

引理 2　一个关于 x 和 y 的实系数多项式,x 和 y 的次数均不超过 n. 如果此多项式在 $x=p,y=q(p,q=0,1,2,\cdots,n)$ 时均为 0,则此多项式为零多项式.

证明　对于任意的 $y=0,1,2,\cdots,n$ 代入原多项式,变成关于 x 的不超过 n 次的多项式,这个新多项式必然是零多项式,否则它不可能有 $n+1$ 个零点,所以按 x 的次数来整理原多项式,对于任意的 $k=0,1,2,\cdots,n$,x^k 项的系数 $C_k(y)$ 都是一个关于 y 的不超过

n 次的多项式,但是却有 $n+1$ 个零点,故所有的系数都为零.

回到原题. 假设 F 中 $x^n y^n z^n$ 这一项系数为 0,那么设 z 为常数,考虑按 x 和 y 的次数来整理多项式 F. F 中,$x^n y^n$ 项的系数是一个关于 z 的,不超过 $n-1$ 次的多项式. 但是由引理 2,这个多项式却拥有 $1,2,\cdots,n$ 共 n 个零点,故它是零多项式. 现在我们令 $z=0$,化归成关于 x 和 y 的多项式. 此时,$x^n y^n$ 项的系数已经是 0,但是我们却发现,这个多项式恰恰在 $x=y=0$ 时非零,在 $x=p,y=q(p,q=0,1,2,\cdots,n$ 且 p,q 不全为 0) 时为零,这与刚才的引理 1 矛盾.

综上,我们证明了多项式 F 中 $x^n y^n z^n$ 这一项系数非零,即原乘积多项式至少有 $3n$ 次,即至少需要 $3n$ 个平面,才能覆盖题目中要求的所有点而不过原点. 故原题的答案为 $3n$.

评论 这是一道很难的题目,最关键的一点就是将这个看似组合计数的题目,转化成纯代数问题. 尤其是在有二维背景的前提下,在考试规定的时间内,更是很少有人能跳出思维的局限. 这或许就是为什么全世界顶尖的高中生只有区区 4 人做出此题的原因吧!

解法 2 很容易发现 $3n$ 个平面能满足要求,例如平面 $x=i,y=i$ 和 $z=i(i=1,2,\cdots,n)$,易见这 $3n$ 个平面的并集包含 S 但不含原点. 另外的例子是平面集

$$x+y+z=k \quad (k=1,2,\cdots,3n)$$

我们证明 $3n$ 是最少可能数,下面的引理是关键的.

引理 3 考虑 k 个变量的非零多项式 $P(x_1,\cdots,x_k)$. 若所有满足 $x_1,\cdots,x_k\in\{0,1,\cdots,n\}$ 且 $x_1+\cdots+x_k>0$,点 $(x_1,\cdots,x_k)$ 都是 $P(x_1,\cdots,x_k)$ 的零点,且 $P(0,$

$0,\cdots,0)\neq 0$,则 $\deg P\geqslant kn$.

证明　我们对 k 用归纳法:当 $k=0$ 时,由 $P\neq 0$ 知结论成立.现假设结论对 $k-1$ 成立,下证结论对 k 成立.

令 $y=x_k$,设 $R(x_1,\cdots,x_{k-1},y)$ 是 P 被 $Q(y)=y(y-1)\cdots(y-n)$除的余式.

因为多项式 $Q(y)$ 以 $y=0,1,\cdots,n$ 为 $n+1$ 个零点,所以 $P(x_1,\cdots,x_{k-1},y)=R(x_1,\cdots,x_{k-1},y)$ 对所有 $x_1,\cdots,x_{k-1},y\in\{0,1,\cdots,n\}$ 成立.

因此,R 也满足引理的条件.

进一步有 $\deg_y R\leqslant n$,又明显地 $\deg R\leqslant\deg P$,所以只要证明 $\deg R\geqslant nk$ 即可.

现在,将多项式 R 写成 y 的降幂形式

$$\begin{aligned}R(x_1,\cdots,x_{k-1},y)=&R_n(x_1,\cdots,x_{k-1})y^n+\\&R_{n-1}(x_1,\cdots,x_{k-1})y^{n-1}+\cdots+\\&R_0(x_1,\cdots,x_{k-1})\end{aligned}$$

下面我们证明 $R_n(x_1,\cdots,x_{k-1})$满足归纳假设条件.

事实上,考虑多项式

$$T(y)=R(0,\cdots,0,y)$$

易见 $\deg T(y)\leqslant n$,这个多项式有 n 个根,$y=1,\cdots,n$;另一方面,由 $T(0)\neq 0$ 知 $T(y)\neq 0$,因此 $\deg T=n$,且它的首项系数是 $R_n(0,\cdots,0)\neq 0$(特别地,在$k=l$的情况下,我们得到系数 R_n 是非零的).

类似地,取任意 $a_1,\cdots,a_{k-1}\in\{0,1,\cdots,n\}$ 且 $a_1+\cdots+a_{k-1}>0$.

在多项式 $R(x_1,\cdots,x_{k-1},y)$ 中令 $x_i=a_i$,我们得到 y 的多项式 $R(a_1,\cdots,a_{k-1},y)$ 以 $y=0,\cdots,n$ 为根且 $\deg R\leqslant n$,因此它是一个零多项式.

所以 $R_i(a_i,\cdots,a_{k-1})=0(i=0,1,\cdots,n)$，特别有 $R_n(a_1,\cdots,a_{k-1})=0$.

这样我们就证明了多项式 $R_n(x_1,\cdots,x_{k-1})$ 满足归纳假设的条件，所以 $\deg R_n\geqslant(k-1)n$.

故 $\deg R\geqslant\deg R_n+n\geqslant kn$. 引理得证.

回到原题. 假设 N 个平面的并集包含 S 但不包含原点. 设它们的方程是

$$a_ix+b_iy+e_iz+d_i=0$$

考虑多项式

$$P(x,y,z)=\prod_{i=1}^{N}(a_ix+b_iy+c_iz+d_i)$$

它的阶为 N. 对任何 $(x_0,y_0,z_0)\in S$，这个多项式有性质 $P(x_0,y_0,z_0)=0$ 但 $P(0,0,0)\neq0$，因此，由引理我们得到 $N=\deg P\geqslant3n$.

（此解法属于朱华伟和付云皓）

我们知道：两条直线交于一点；直线与圆锥曲线交于两点；两条圆锥曲线交于四点. 将其引申下去就得到代数几何的开卷定理.

定理 1（Bézout[①] 定理） 次数分别为 M 和 N 的两条代数曲线，如果没有公共分支，则恰好交于 MN 个点（要恰当地计数）.

这个定理首先被马克劳林（Maclaurin）于 1720 年所断言. 欧拉（Euler）于 1748 年，克莱姆（Cramer）于 1750 年都分别讨论过它，但是，是贝祖（Bézout）于 1770 年把它叙述得更完整.

而这仅限于代数曲线而不能推广到超越情形. 陈

① 贝祖（Bézout），法国人，1739—1783. ——编者注

省身的学生希夫曼(Bernard Shiffman)1972 年在耶鲁大学(Yale University)当助理教授时与科纳尔巴(Cornalba)合作写了一篇论文“A counterexample to the ‘transcend ental Bézout problem’”(Ann of Math. 2, 1972,402-406)中给出了一个反例,说明古典代数几何中著名的贝祖定理在超越的情况下是失效的.

多项式的简单预备知识

第2章

在这一章里,我们首先研究多项式的代数性质,而不管多项式也是函数. 换句话说,我们先研究加法、乘法和形式求导的运算.

定义 1(在一个整环 A 上具有一个未定元的多项式) 设 A 是一个整西环,也就是说一个无零因子而有单位元素(乘法的中性元素)的环. 在以后,我们取为 A 的,或者是复数域 **C**,或者是实数域 **R**,或者是有理数域 **Q**(在研究具有多个未定元的多项式时,可以得到 A 是多项式环).

考虑 A 的元素的这样一个序列,使得从某个序标起,序列的所有以后的元素都等于 A 的 0 元素,这里 0 是 A 里加法的中性元素. 于是,得到一序列

$$a=(\alpha_0,\alpha_1,\cdots,\alpha_n,0,0,\cdots)$$

这里 $\alpha_i\in A$;这样的序列叫做 A 上具有一个未定元的多项式.

使 $\alpha_n\neq 0$ 的最大的序标叫做多项式 a 的次数.

元素 α_i 叫做多项式的系数;系数 α_0 叫做常数项.

如果所有的系数都等于 0,则对应的多项式用 0 来表示,且约定:它是没有次数的,我们偶尔也约定给它象征性的次数,记为 $-\infty$,这个符号按照约定满足不等式 $-\infty < n$,这里 n 是任意整数.

2.1　多项式矢量空间

设有两个多项式

$$a=(\alpha_0,\cdots,\alpha_n,0,0,\cdots)$$

和

$$b=(\beta_0,\cdots,\beta_m,0,0,\cdots)$$

如果有恒等关系,也就是说,如果 $n=m$(次数相同),又如果对一切 $i=0,1,2,\cdots,n,\alpha_i=\beta_i$,则令 $a=b$.

定义 2(加法)　我们在多项式的集上定义一个内运算,记为加法,即

$$a+b=(\alpha_0+\beta_0,\alpha_1+\beta_1,\cdots)$$

我们看到,这个运算是可结合的和可交换的.

它有一个中性元素:这是记为 $0=(0,0,\cdots)$ 的多项式,它的所有系数都是零.

最后,每一多项式具有一个对称元素或相反元素,记为

$$-a=(-\alpha_0,\cdots,-\alpha_n,0,0,\cdots)$$

这是其系数都与 a 的系数反号的多项式.

于是对于这个规律,多项式的集构成一可交换的群.

要指出,如果两个多项式的次数不等,则 $a+b$ 的次数等于两个次数中较大的一个;如果两个次数相等,

则 $a+b$ 的次数可能变小，于是总有 $(a+b)$ 的次数 $\leqslant \max\{a$ 的次数，b 的次数$\}$，以后记为 $\deg(a+b) \leqslant \max\{\deg a, \deg b\}$①. 零多项式的次数是不定的，$-a$ 的次数与 a 的次数相同.

定义 3（乘以 A 的元素的乘法） 设 $\lambda \in A$，令

$$\lambda a = (\lambda\alpha_0, \lambda\alpha_1, \cdots, \lambda\alpha_n, 0, 0, \cdots)$$

λa 是一多项式，它的系数是 a 的系数乘以 λ 的积.

如果 $\lambda \in A$ 且 $\mu \in A$，则有下列规则

$$\lambda(a+b) = \lambda a + \lambda b$$

$$(\lambda+\mu)a = \lambda a + \mu a$$

$$\lambda(\mu a) = (\lambda\mu)a$$

$$1 \cdot a = a$$

如果 $\lambda \neq 0$，则可看到 $\deg(\lambda a) = \deg a$.

在 A 是域 K 的情况下，这些运算将多项式集作成系数域 K 上的一矢量空间.

现在来考虑多项式 $u_n = (0, \cdots, 0, 1, 0, \cdots)$，它的系数除序标为 n 的一项以外都是零. 序标为 n 的一项的系数为 1，即 A 的单位元素；这样，u_n 仍是一 n 次多项式. 每一多项式 $a = (\alpha_0, \alpha_1, \cdots, \alpha_n, 0, 0, \cdots)$ 以唯一的方法写成下式

$$a = \alpha_0 u_0 + \alpha_1 u_1 + \cdots + \alpha_n u_n$$

在 A 为域 K 的场合，将 a 用唯一的方法表示为有限个元素 u_n 的线性组合，u_n 的系数为 K 的元素. 我们说，元素 u_n 形成多项式矢量空间的一个基. 基的元素的个数叫做矢量空间的维数. 这样，多项式矢量空间是

① degré 是法文“次数”的意思，本书中以 deg a 表示多项式 a 的次数. ——编者注

无限维的.

通常的记法　为了后面要出现的理由,我们用记号 x^n 以代替 u_n. 重要的是指出下面一点:现时 x 不表示什么东西,而 x^n 是一个符号,其中 n 与 x 是不能分离的,n 起到序标的作用. 最后,作为一个约定,我们写 $u_0=x^0=1$.

我们通常还写为

$$a=\alpha_0+\alpha_1x+\cdots+\alpha_nx^n$$

或

$$a=\alpha_nx^n+\alpha_{n-1}x^{n-1}+\cdots+\alpha_1x+\alpha_0$$

在第一种写法中,我们说 a 是按 x 的升幂排列的;在第二种写法中,a 是按 x 的降幂排列的.

在环 A 上多项式集记为 $A[x]$,x 叫做未定元或变量. 变量这一术语主要在我们把多项式看做函数时使用.

2.2　多项式环

多项式乘法　我们引入多项式集上的第二个组合规律,一种可结合的同时对于多项式加法可分配的规律.

根据可分配性,只要对 $\alpha_ix^i(\alpha_i\in A)$ 这种形式的多项式,定义第二个规律就行了.

对于 $\alpha_i\in A,\beta_i\in A$,我们令

$$(\alpha_ix^i)(\beta_jx^j)=\alpha_i\beta_jx^{i+j}$$

换句话说,未定元的相乘,其序标像幂指数那样处理.

如果

$$a=\alpha_0+\alpha_1x+\cdots+\alpha_nx^n,b=\beta_0+\beta_1x+\cdots+\beta_mx^m$$

则根据分配律,可以看出

$$\begin{aligned}a\cdot b=&\alpha_0\beta_0+(\alpha_0\beta_1+\alpha_1\beta_0)x+\cdots+\\&(\alpha_0\beta_i+\alpha_1\beta_{i-1}+\cdots+\alpha_i\beta_0)x^i+\cdots+\\&\alpha_n\beta_mx^{n+m}\end{aligned}$$

这个运算是可换的,对于加法是可分配的.我们可用一稍长但不甚困难的计算验证,它是可结合的.

我们要指出下面的重要性质

$$\deg(a\cdot b)=\deg a+\deg b$$

如果 $b=0$,在约定对不论怎样的 n,总有 $-\infty=n+(-\infty)$ 时,上式仍保持为真.

集 $A[x]$ 是可交换环.设多项式

$$u=\eta_0+\eta_1x+\cdots+\eta_lx^l$$

如果对任意多项式 a 有 $u\cdot a=a$,u 就是对于乘法的中性元素.特别应该有 $ux^n=x^n$,于是

$$\eta_0x^n+\eta_1x^{n+1}+\cdots+\eta_lx^{n+l}=x^n$$

这就要求

$$\eta_0=1,\eta_1=0,\eta_2=0,\cdots,\eta_l=0$$

这样就有 $u=x^0=1$;这就是将多项式 x^0 与数 1 等同的理由.于是环 $A[x]$ 是酉环.另一方面,多项式 x 可以与未定元等同,这是从下面意义来说的,用符号 x^i 表示的多项式是多项式 x 的 i 次幂,而后者又是按照刚刚定义的乘法来作成的.

我们来探求 $A[x]$ 有无零因子.设 a 和 b 是 $A[x]$ 的两个多项式,且 $a\neq0$;于是在 a 中至少存在一个系数 $\alpha_h\neq0$;假设 h 是具有如下性质的最小序标,它使得如果存在整数 i:$0\leqslant i<h$,则有 $\alpha_i=0$.如果 b 的系数是

$\beta_0, \beta_1, \cdots$，由等式 $ab=0$ 得

$$\alpha_h\beta_0=0, \alpha_h\beta_1+\alpha_{h+1}\beta_0=0, \cdots$$

因 $\alpha_k \neq 0$，我们陆续推出 $\beta_0=0, \beta_1=0, \cdots$，于是就有 $b=0$. 于是环 $A[x]$ 是一个整环.

推论 1　由等式 $ab=ac$ 导致：如果 $a\neq 0$，则 $b=c$.

实际上，等式 $ab=ac$ 也写为 $a(b-c)=0$；然而 $a\neq 0$，于是 $b-c=0$，从而 $b=c$.

每个多项式 $a\neq 0$ 对乘法是正则的.

2.3　按降幂排列的除法

在这一部分，我们假设 A 是一个域 K，这里 K 或是 $\mathbf{C}$，或是 $\mathbf{R}$，或是 $\mathbf{Q}$.

2.3.1　除法的等式

设已给两个多项式 a 和 b，并不总是存在多项式 q，使 $a=bq$. 如果存在这样的多项式 q，就说 a 能被 b 整除，或 b 整除 a，或 a 是 b 的倍式.

这样，多项式 0 是任一多项式的倍式.

为了使 a 能被 b 整除，必须 a 属于 b 的倍式的集 I，也就是 cb 这样形式的多项式的集，这里 c 是一任意的多项式. 可以立刻验证：I 是 $K[x]$ 的子环；而且 I 还是这个环的一个理想，因为 b 的一个倍式被一任意的多项式来乘，其积仍是 b 的倍式.

I 的每一非零多项式的次数至少等于 b 的次数，因而 b 是 I 的一个非零多项式，它有可能最小的次数.

如果 a 的次数严格小于 b 的次数，则 a 不能被 b 整除，除非 $a=0$.