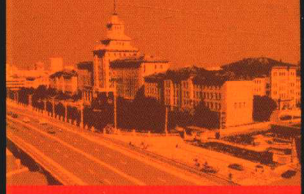

俄罗斯数学精品译丛

“十二五”国家重点图书

Algebraic Function Theory (I)

代数函数论（上）

[苏] 契巴塔廖夫 著　　戴执中 夏定中 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

代数函数论（上）(I)

Algebraic Function Theory (I)

●［苏］契巴塔廖夫 著 ●戴执中 夏定中 译

哈爾濱工業大學出版社

HARBIN INSTITUTE OF TECHNOLOGY PRESS

内容简介

本书是代数函数论的经典著作. 全书共分 5 章:第 1 章介绍了关于体的一般理论;第 2 章至第 5 章叙述了代数函数的算数理论及其基本的应用.

本书可以作为大学生和研究生选修课的教材,或数学研究工作者的参考书.

图书在版编目(CIP)数据

代数函数论. 上/(苏)契巴塔廖夫著;戴执中,夏定中译. —哈尔滨:哈尔滨工业大学出版社,2015.10

ISBN 978-7-5603-5411-8

Ⅰ.①代… Ⅱ.①契… ②戴… ③夏… Ⅲ.①代数函数 Ⅳ.①O174.53

中国版本图书馆 CIP 数据核字(2015)第 117104 号

策划编辑 刘培杰 张永芹
责任编辑 张永芹 刘立娟
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 13.25 字数 253 千字
版 次 2015 年 10 月第 1 版 2015 年 10 月第 1 次印刷
书 号 ISBN 978-7-5603-5411-8
定 价 38.00 元

◎前言

代数函数论的研究对象，是以代数关系式

$$f(x,y)=0 \tag{1}$$

联系着的两个变量 x,y 的有理函数 $\varphi(x,y)$，其中 $f(x,y)$ 是这两个变量 x 与 y 的多项式. 这个理论在历史上是由企图把形如

$$\int\varphi(x,y)\mathrm{d}x \tag{2}$$

的积分用有限的形式积出而产生的. 为了纪念开始研究其理论的伟大的挪威数学家阿贝尔(N. H. Abel，1802—1829)，形如(2)的这一类积分就被称作阿贝尔积分.

关于把这类积分积出成有限形式的问题，关联着如何来适当地选择形如

$$x=\psi_1(u,v),y=\psi_2(u,v) \tag{3}$$

的变换，其中 ψ_1,ψ_2 都是有理函数，而使得经这种变换以后，积分(2)变成对于一个变量的有理函数的积分. 积分(2)可以被积出成有限形式这个性质，并不依赖于对它所作的任意的变换(3). 因此，从如何把积分积出成有限形式这个问题出发，便产生了一个普遍念头，即研究与函数 $\varphi(x,y)$ 有关的对于各种(3)型变换都不变的性质和量. 在特别重要的情形下，即当变换(3)是有理可逆时，这种变换称为双有理变换. 因此，代数函数论可以被表征为研究在双有理变换下的不变量的科学. 这使得我们有理由把它看作是在克莱因(F. Klein)意义下的一种几何学系统. 克莱因曾经规定：几何学是研究在某一种变换群下的不变量的科学(见第 5 章 §1，也见第 2 章 §1).

为了使代数函数论基本问题的提法更加确切与简洁，我们按

照下面的方式来陈述它. 给定两个(1)型的方程式

$$f_1(x,y)=0, f_2(x,y)=0$$

求出一组有限多个量,使它们与这两个方程式中的每一个相关联,并且具有下述性质:要使一个(3)型的变换存在,把其中的一个方程式变换成另一个,其充分且必要的条件是所得到的这组量对于这两个方程式来说是重合的.

被陈述成这种形式的问题,一直到现在还不曾获得解决. 现在已经知道了关系式(1)的一个最重要的不变量——非负整数ρ,称为方程式的(或者按照几何学上的说法,曲线(1)的)亏格数(жанр;geschlecht). 此外,我们也已经知道,当$\rho>1$时,亏格数等于ρ的方程式依赖于$3\rho-3$个不变参数. 黎曼(B. Riemann,1824—1866)称这些参数是曲线(1)的模. 但是,现在还不曾对它们给出什么方便而明了的表示法.

代数函数论在历史上曾经沿着其他的路线发展过,并且是独立地就几个不同的方向发展的,其中的一个方向——函数论的方向——是创自阿贝尔,而由黎曼给出完整形式的,不是在平面上,而是在一种特殊的多层曲面——这种曲面已经获得了黎曼面的名称——来表示多值的复变函数. 这一个天才的观念,就是属于黎曼的. 黎曼曾经在代数函数的最简单情形下研究过这类黎曼面,后来这种曲面成为了在研究广泛的各种普通函数与许多特殊函数(模函数、自守函数、线性微分方程的积分等)时的基本工具.

差不多与黎曼同时,魏尔斯特拉斯(K. Weierstrass,1815—1897)也在相近的方向上发展了代数函数论,他用把多值函数展开成幂级数的方法,研究了多值函数的性质. 后来,在获悉了黎曼的这些结果之后,他修改了自己的讲义,在其中引进了黎曼面的概念.

在19世纪中叶,由于普遍爱好综合几何学的缘故,大批的几何学家用纯粹几何学的方法来从事代数曲线的系统研究,这样就在代数函数论中产生了几何学的方向,也称作代数几何学. 从它的那些创始人中间,我们必须举出普吕克(Plücker)、克莱布施(A. Clebsch)、戈丹(P. Gordan)、布里尔(A. Brill)和诺特(M. Noether). 现在,这个方向为意大利学派的几何学家所继承(卡斯泰尔诺沃(Castelnuovo)、恩里克斯(F. Enriques)、塞韦里(F. Severi),等等),他们把注意力转移到代数曲面上,并且得到了代数曲面的许多有基本意义的结果.

代数函数论的算术方向,它的基础是戴德金所奠定的,他是伊德耶(идеал;gdeal)理论的创始人之一,与韦伯合写了一篇重要的论文. 所有在"绝对的黎曼面"上的某一个位处变成零的$\varphi(x,y)$型的函数集合,构成一个素伊德耶. 从这个事实出发,戴德金与韦伯获得了把函数$\varphi(x,y)$表示成素伊德耶乘积的单值表示法(更确切地说,表示成素伊德耶的乘积的商式的形式).

单变量的有理函数可以被表示成一次因式的乘积的商式,即可以用给出使

它变成0与变成∞的那些值的方法来规定它. 恰和这个相仿,代数函数也可以被表示成素伊德耶的乘积的商式,并且,分子和分母含有相同个数的素因子(都是同一阶数的伊德耶). 二者间的主要区别在于,任意给定有理函数的零点与无限大点(极点)之后,我们总可以求出这个函数,但代数函数的零位与无限大位则不能完全任意地给定. 转到在数论中所得出的同等伊德耶和伊德耶类的概念上去,我们可以说,并非任何有同一阶数的伊德耶都是同等的. 同等的类构成一些线性族,戴德金和韦伯还确定了在阶数与由这个伊德耶所构成的那个类的维数(即在这个类中线性独立的伊德耶的最大数)之间的关系. 他们在引进了与阿贝尔积分密切相关的微分类这一概念后,就以纯粹算术的方法得到了全部理论的核心结果——黎曼 - 诺赫定理. 一般地,算术的代数函数论使我们可以用纯粹算术上的,并且是完全普遍的方法,来导出并表明阿贝尔积分的理论与代数曲线的理论中的大部分结果. 算术的代数函数论与几何的代数函数论比较起来,其基本的优点在于,算术的代数函数论中所得到的那些结果有完全的普遍性,而在几何的代数函数论中,则必须引进曲线(1)所可能有的那些关于异点的特性的限制.

最近,算术的代数函数论的一种新的,并且是十分原则性的优越性已经被阐明了. 现在已经知道可以把它扩充到这样的代数函数上,它们的系数不像在古典理论中所作的那样是任意复数,而是任何一个已知数体中的元素(例如,是有理数,甚至是关于某一个素数的合同类). 研究这种代数函数的重要性,当企图应用代数函数论来求出满足方程式(1)的 x,y 的各组有理值时,即当企图解最普遍形式的丢番图方程式时,就可以看出来. 所说的这个问题,是那些表征代数函数论中现代方向的最突出的问题之一,虽然不是唯一的一个.

◎ 目 录

体的理论

第1章

§1 体与环的概念

所谓体是一个在其上确定了两种运算的若干对象(这些对象我们称作是这个体的元素)的集合. 与在算术中相类似,这两种运算我们称之为加法与乘法,并且,这两种运算应当服从下面的规律:

Ⅰ. 加法. 确立一种规律,使得体内的任意两个元素 a,b 都有第三个元素同它们对应,这第三个元素称为元素 a 与 b 的和,记作 $a+b$,并且,加法是可以结合的

$$(a+b)+c=a+(b+c) \tag{1}$$

可以交换的

$$a+b=b+a \tag{2}$$

以及是单值可逆的. 最后这句话是说,对于任意的元素 a,b,总可以找到体内的一个元素,而且也仅仅只有一个元素 x,使得

$$a+x=b \tag{3}$$

特别地,有这样的一个元素 y 存在,使得

$$a+y=a \tag{4}$$

现在来证明这个元素 y 是与元素 a 的选择无关的. 为此,我们只需在等式(4)的两端都加上一个由式(3)所规定的元素 x. 于是根据(1)与(2),便有

$$b+y=b$$

这里的 b 是体内任意的一个元素. 这样所规定的元素 y,叫作零元素,记作 0.

由等式(3)所规定的那个元素 x,叫作元素 b 与 a 的差,记作 $b-a$. 特别地,差 $0-a$ 叫作 a 的负元素,简记作 $-a$.

由此容易导出对于带括号的运算的通常规律,对于减法的结合律,等等.

Ⅱ. 乘法. 确立另外一种使得对于体中任意两个元素 a,b 总有第三个元素与之对应的规律,这第三个元素称作元素 a 与 b 的积,记作 $a\cdot b$,并且,乘法是可以结合的

$$(ab)c=a(bc) \tag{5}$$

可以交换的

$$ab=ba \tag{6}$$

加法与乘法服从分配律

$$(a+b)c=ac+bc \tag{7}$$

我们要注意,右端的表达式可能会引起误会,因为其中并没有指明应当先进行哪种运算. 鉴于此,通常约定在运算的顺序不曾用括号来指明时,应当先进行乘法的运算,然后再进行加法与减法的运算.

不难证明,分配律也可以推广到减法

$$(a-b)c=ac-bc \tag{8}$$

从分配律可以导出对零元素的乘法的规律

$$a\cdot 0=a(b-b)=ab-ab=0 \tag{9}$$

满足这些规律的元素的集合称为一个环. 一般地,在环内并不假定能作乘法的单值逆运算,或者,如我们将要说的,并不一定可以施行除法. 下面这些集合可以作为环的例子:

(1)全部整数——正整数、负整数及零——的集合;

(2)全部整复数,即形如 $a+b\mathrm{i}$ 的数的集合,其中 $\mathrm{i}=\sqrt{-1}$,a 与 b 取所有的整数;

(3)变量 x 的所有多项式的集合(也可以是几个独立变量 $x_1,x_2,\cdots,x_n$ 的所有多项式的集合).

较环狭一些的概念是体. 要使上面所说的元素集合形成一个体,还应当满足:

Ⅲ. 乘法的单值可逆性. 这就是说,对于任意两个已知的元素 a,b 总有一个元素 x 存在,使得

$$ax=b \tag{10}$$

成立,并且,这个元素 x 是唯一的. 这个元素通常记作 $b:a$,或者 $\frac{b}{a}$(b 被 a 除,或者,以 a 除 b 的商,或者,具有分子 b,分母 a 的分式).

这时我们必须把 $a=0$ 的情形除外. 事实上,既然对任何一个 x 都有 $0\cdot x=0$,所以方程式 $0\cdot x=b$ 当 $b\neq 0$ 时是不可能有解的.

特别地,方程式

$$ay = a$$

的解是与 a 的选择无关的. 这个解称为单位元素,记作 1. 在某些情况下,当这个记号可能会引起误会时,通常用字母 e 来记单位元素(见本章 §2).

在前面所举作为环的例子的那些集合中,没有一个是体. 以下是体的例子:

(1)全部(正的与负的)有理分数,即形如 $\frac{b}{a}$ 的数的集合,其中 a,b 都是整数,并且,$a \neq 0$;

(2)形如 $a+bi$ 的数的集合,其中 $i=\sqrt{-1}$,a,b 可取任何的有理分数;

(3)全部有理函数,即分子、分母都是一个变量 x 的(或几个变量的)多项式的那些分式的集合.

从这三个例子我们可以看出,根据一个已知的环,常可以用如下的方式来作成一个体:就形式上取已知环的元素的商来作为这个体的元素,并用下述规律来规定体中元素的运算

$$\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}, \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \frac{a}{b} : \frac{c}{d} = \frac{ad}{bc}$$

不难验证,就这样的元素来说,用来规定体的那些定律都是正确的,并且,当

$$ad = bc$$

时,而且只在此时,才有

$$\frac{a}{b} = \frac{c}{d}$$

为了要证明在这样的定义中等式的可传性,还必须要有下述环的性质:

Ⅳ. 无零因子. 如果 $ab=0$,那么,或者 $a=0$,或者 $b=0$,二者必居其一.

对于环来说,这个性质是需要予以假定的,而对于体来说,则它是可以证明的. 事实上,从 $ab=0$,并由于有元素 $\frac{1}{b}$ 存在(设 $b \neq 0$),我们得到

$$ab \cdot \frac{1}{b} = a = 0$$

因此,如果 $b \neq 0$,则必定 $a=0$.

另一方面,也有些环并不具备条件Ⅳ. 对于这样的环,自然不能用刚才所描述的方法来作成一个体. 由环用这种方法所作成的体叫作商体.

§2 子体、素体、示性数

如果一个体 K 的一部分元素，本身也形成一个体 k，那么 k 就叫作体 K 的子体，我们也说，k 包含在 K 内，并记作

$$k \subset K$$

体 K 有时也称为体 k 的包含体.

例 如果 K 是变量 $x_1, x_2, \cdots, x_n$ 的所有有理函数所形成的体，那么变量

$$x_1, x_2, \cdots, x_k \quad (k = 1, 2, \cdots, n-1)$$

的有理函数所形成的体，就可以作为它的子体的例子.

如果 $k \subset K$，并且 k 与 K 不是相同的，那么 k 称作是 K 的真子体. 不包含真子体的体叫作素体.

每一个体 K 都含有唯一的一个素体作为它的子体. 要找出这个素体，我们取体 K 的单位元素 e（它应当是包含在所有的子体内的），并构成如下的元素

$$e+e=2e, 2e+e=3e, \cdots, 0, -e, -2e, -3e, \cdots \tag{1}$$

它们组成一个环，这个环显然是包含在体 K 的每一个子体内的. 这里我们应该分两种情形来讨论：

（1）所有式（1）中的元素都是不相同的. 这时它们所形成的环，与整有理数环仅相差一个因子 e，而由于 $e^2 = e$ 的缘故，这个因子是不起任何作用的. 在这种情形下，我们可以置 $e = 1$. 把所得的整有理数环扩充成它们的比值的体，即扩充成有理数体，这个体包含在体 K 的所有子体内，所以是一个素体. 这时我们说，K 是一个示性数为零的体.

（2）可能会遇到，并非所有式（1）中的元素都是互异的. 设

$$me = ne \quad (m \neq n)$$

于是

$$(m-n)e = 0$$

设 p 是所有使

$$pe = 0$$

成立的正整数中最小的那一个. p 应当是一个素数，否则，从

$$p = qr \quad (q < p, r < p)$$

我们就有

$$qe \neq 0, re \neq 0, qe \cdot re = 0$$

这与条件Ⅳ相矛盾.

素数 p 称为体 K 的示性数. 我们所选出的环 R_p，是由 p 个不同的元素

$$0,e,2e,\cdots,(p-1)e \tag{2}$$

所构成的. 对于加法与乘法两个运算,这些元素显得像模于 p 的那些剩余一样. 环 R_p 也构成一个体,所以不需要再扩充成商体. 事实上,如果把整个数列(2)都乘以同一个如(2)型的元素,例如,都乘以 $ae(0<a<p)$,那么数列

$$0,ae,2ae,\cdots,(p-1)ae \tag{3}$$

是由 p 个不同的元素所构成的(从 $ake=ale$,即 $a(k-l)e=0$. 由于 $ae\neq 0$ 及性质Ⅳ,便可以得出 $ke=le$),所以它与数列(2)仅是顺序不同而已. 由此便可推知,方程式

$$ae\cdot xe=be$$

当 $0<a<p$ 时总有解 xe,并且这个解是唯一的. 所以除法总是可以施行的.

体 R_p 是一个素体. 因此:

每一个体都或者包含有理数体 R,或者包含模于素数 p 的有限的剩余类体 R_p,以作为它的素子体.

我们将引进两个体的同构性这一概念.

如果在体 K 的元素 $A,B,C,\cdots$ 与体 k 的元素 $a,b,c,\cdots$ 之间,可以建立起这样的一种一一对应关系

$$A\longleftrightarrow a,B\longleftrightarrow b,C\longleftrightarrow c,\cdots$$

使得同时还保有

$$A+B\longleftrightarrow a+b,A\cdot B\longleftrightarrow a\cdot b,\cdots$$

则这两个体 K 与 k 就称为是同构的.

于是刚才所得到的结果可以叙述如下:

每一个体都含有一个唯一的素子体,这个素子体或者与有理数体 R 同构,或者与关于素数 p 的剩余类体 R_p 同构.

对以上这两种情形中的第二种,我们称体 K 是有示性数 p 的体.

§3 体的扩张、超越扩张

设已知一个体 k 和任意一个元素 x,x 不包含在体 k 内,但是可以把它与体 k 中的元素放在一起来确定服从条件Ⅰ~Ⅳ的运算规律. 包含体 k 与 x 的最小的体,是由系数在体 k 中的含 x 的有理函数所形成的(两个多项式相除的商,我们称之为有理函数). 这个体叫作由添加元素 x 而得出的体 k 的扩张,记作 $k(x)$. 再借助一个新元素 y 来扩张体 $k(x)$,我们便得到借助两个元素 x,y 而得的体 k 的扩张 $k(x,y)$. 用这样的方法可以借助任何多个元素来扩张体 k.

现在来讨论体 $k(x)$. 我们将区分开两种类型的扩张. 属于第一种类型的是

当 x 满足一个关系式

$$f(x)=A_0x^n+A_1x^{n-1}+\cdots+A_{n-1}x+A_n=0 \tag{1}$$

时的这种体 $k(x)$，其中 $A_0,A_1,\cdots,A_{n-1},A_n$ 都是 k 的元素，不同时为零. 这种形态的扩张叫作代数扩张，而当形如(1)的关系式不存在时，扩张 $k(x)$ 就称为超越扩张.

超越扩张 $k(x)$ 是形如

$$\frac{\varphi(x)}{\psi(x)}$$

的有理函数的集合，其中 $\varphi(x)$ 与 $\psi(x)$ 都是具有 k 中系数的 x 的多项式. 为了要完全确定这个体，我们必须确定应当把其中怎样一些元素看作是相等的. 先来讨论由具有 k 中系数的 x 的多项式所形成的环的元素，这些元素构成体 $k(x)$ 的一个子环. 两个多项式

$$\varphi(x)=a_0+a_1x+\cdots+a_mx^m$$

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

当它们的次数相等，$m=n$，并且，x 的同次幂的系数也都相等，即

$$a_k=b_k \quad (k=0,1,2,\cdots,m)$$

时，而且只有在此时，才是彼此相等的. 事实上，如果在不满足这些条件时，有

$$\varphi(x)=\psi(x) \tag{2}$$

成立，那么等式(2)就要导致一个(1)型的非恒等关系式. 这是和已知条件相矛盾的.

现在回到体 $k(x)$ 的一般形式的元素上来. 设

$$\frac{\varphi(x)}{\psi(x)}=\frac{\varphi_1(x)}{\psi_1(x)} \tag{3}$$

上式两边分别乘以多项式 $\psi(x)\psi_1(x)$，我们便得到等式

$$\varphi(x)\psi_1(x)=\varphi_1(x)\psi(x) \tag{4}$$

这个关于多项式的等式，应当遵循上面所规定的意义. 为了要使(3)成立，它是充分的，这只要把式(4)两边同除以 $\psi(x)\psi_1(x)$ 便可以证实.

当式(3)成立时，不一定要使这个等式左右两端的分子、分母都彼此相等. 这很容易证实，只要把任意一个分式的分子、分母乘以同一个多项式，就可以看出来. 但是，我们将证明每一个分式都可以化成正规的(既约的)形式，两个正规的分式，只有在它们的分子、分母各自相等时，才会彼此相等.

如果两个多项式 $f(x)$ 与 $g(x)$ 的商也是一个多项式，我们就说 $f(x)$ 被 $g(x)$ 所除尽. 显然：

Ⅰ. 如果 $f_1(x)$ 与 $f_2(x)$ 都被 $g(x)$ 所除尽，那么 $f_1(x)\pm f_2(x)$ 也被 $g(x)$ 所除尽.

Ⅱ. 如果$f(x)$被$g(x)$所除尽,而$g(x)$又被$h(x)$所除尽,那么$f(x)$也被$h(x)$除尽.

要得出关于可除性的另外一些并不这样显然的定理,我们将引进欧氏法式. 首先要注意,如果多项式$f(x)$与$g(x)$的次数各等于m与n,那么总可以(利用除法)唯一地确定出一个多项式$q(x)$(商)与一个次数小于n的多项式$r(x)$(余式),使它们满足下面的恒等式

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

多项式$q(x)$与$r(x)$的系数也都在k内.

利用这样的方法,我们可以逐步求得多项式序列

$$f,g,r,r_1,r_2,\cdots$$

中每两个相邻的多项式的余式,其间的相互关系是

$$\begin{aligned} f&=g\cdot q+r\\ g&=r\cdot q_1+r_1\\ r&=r_1\cdot q_2+r_2\\ &\vdots \end{aligned} \tag{5}$$

这些多项式的次数是逐渐减小的,所以这个过程必然在有限次的运算之后终止. 最后的那个除式r_k(r_{k-1}被它所除尽)是多项式$f(x)$与$g(x)$的最大公因式. 这是不难证实的. 此外,从恒等式(5)中消去那些中间的余式$r,r_1,\cdots,r_{k-1}$,我们便得到一个关系式

$$f\cdot X+g\cdot Y=r_k \tag{6}$$

其中X,Y是系数在体k中的某两个多项式.

如果$r_k=\text{const}$,那么这两个多项式f与g就称作是互素的. 利用关系式(6),不难证明下面这些关于可除性的定理:

Ⅲ. 如果乘积$f\cdot g$被h所除尽,并且f与h是互素的,那么g必被h所除尽.

Ⅳ. 如果多项式f_1,f_2中的每一个都是与g互素的,那么它们的积$f_1\cdot f_2$也必与g互素.

这个定理很容易推广到任意多个因式的情形.

Ⅴ. 如果多项式f被多项式g,h中的每一个所除尽,并且g,h是互素的,那么f也必被乘积$g\cdot h$所除尽.

从这些定理中,可以很容易地导出把多项式分解成素因式的单一性. 所谓在体k内不可约的多项式(素多项式),我们理解为系数在k中的多项式,它除了自身与常数外无其他具有k中系数的因式. 由这个定义可以推知[①]:

① 以后,在"多项式"这个名词下,我们总理解为具有k中系数的多项式.

任何一个多项式,或者是被不可约的多项式所除尽,或者是与它互素.

就特别的情形来说:

两个不同的(即彼此不仅相差一个常数因子的)不可约多项式,必然是互素的.

现在我们假设一个多项式可以用两种不同的方法分解成不可约的因式

$$f=f_1\cdot f_2\cdot\cdots\cdot f_s=g_1\cdot g_2\cdot\cdots\cdot g_t \tag{7}$$

假定 f_1 与多项式 $g_1,g_2,\cdots,g_t$ 中的任何一个都不相同,那么根据刚才所证明的,可知 f_1 与 $g_1,g_2,\cdots,g_t$ 是互素的. 再由Ⅳ,f_1 与 $g_1g_2\cdots g_t$ 也必定是互素的,即也与 f 互素. 但这是不可能的. 因此,f_1 必定与 $g_1,g_2,\cdots,g_t$ 中的一个相同. 把它从式(7)中约掉,然后再继续同样的推理,最后我们便得到定理:

Ⅵ. 每一个多项式都能单一地分解成素因式的乘积.

设给定一个分式

$$\frac{f(x)}{g(x)}$$

其中 $f(x)$ 与 $g(x)$ 都是多项式. 化简这个分式,即把 $f(x)$ 与 $g(x)$ 同除以它们的最高公因式,我们得到

$$\frac{f(x)}{g(x)}=\frac{f_1(x)}{g_1(x)}$$

其中 $f_1(x)$ 与 $g_1(x)$ 是两个互素的多项式. 我们就说,这时体 $k(x)$ 的元素 $\dfrac{f(x)}{g(x)}$ 已经被化成正规形式了. 如果

$$\frac{f_1(x)}{g_1(x)}=\frac{f_2(x)}{g_2(x)}$$

其中 $f_1(x)$ 与 $g_1(x)$,$f_2(x)$ 与 $g_2(x)$ 都是互素的,那么 $f_1(x)$ 与 $f_2(x)$,$g_1(x)$ 与 $g_2(x)$ 就都只相差一个常数因子. 事实上,我们有

$$f_1(x)g_2(x)=g_1(x)f_2(x)$$

但是,由于 $f_1(x)$ 与 $g_1(x)$ 是互素的,所以由Ⅲ,$g_2(x)$ 必被 $g_1(x)$ 所除尽,而 $f_2(x)$ 也必被 $f_1(x)$ 所除尽. 同理,由于 $f_2(x)$ 与 $g_2(x)$ 是互素的,多项式 $g_1(x)$ 可被 $g_2(x)$ 所除尽,而 $f_1(x)$ 可被 $f_2(x)$ 所除尽. 因此,元素

$$\frac{g_2(x)}{g_1(x)},\frac{f_2(x)}{f_1(x)}$$

都是多项式,并且它们的(对于乘法的)逆元素也都是多项式. 由此可以推知,这两个元素都是常数. 事实上,如果 $\varphi(x)$ 与 $\psi(x)$ 都是多项式,并且

$$\varphi(x)\cdot\psi(x)=1$$

那么,由于 $\varphi(x)\cdot\psi(x)$ 的次数等于 $\varphi(x)$ 与 $\psi(x)$ 的次数的和,并且 $\varphi(x)$ 与 $\psi(x)$ 的次数都不是负的,即可推知 $\varphi(x)$ 与 $\psi(x)$ 的次数都等于零.

在式(6)中所表达的结果,从另外一个观点来看也是重要的:从这个结果可推知,未定方程式

$$aX + bY = c \tag{8}$$

其中 a,b,c 都是 x 的多项式,当 c 可以被多项式 a 与 b 的最高公因式所除尽时,而且只有此时,才有多项式的解. 就特例来说,如果 a 与 b 是两个互素的多项式,c 是任意的一个多项式,那么方程式(8)总有多项式的解.

在实用上,解方程式(8)用下述方法最为方便. 设 a 的次数大于(或等于)b 的次数,并且

$$a = bq + r, c = bq + r_1$$

其中 r 与 r_1 的次数都比 b 的次数低. 把这两个式子代入(8),我们便得到

$$rX + bZ = r_1 \tag{9}$$

其中

$$Z = qX + Y - q_1$$

显然,如果 X,Y 都是多项式,那么 X,Z 也都是多项式,并且反过来说也是对的. 因此,我们已经把问题化为解未定方程式(9),它的系数的次数比(8)的低. 继续这个运算,最终我们可以得到一个方程式,在它的那两个作为系数的未知函数中,有一个是常数. 这样的方程式可以用初等的方法来求解.

§4 体的代数扩张

如果一个不属于体 k 的元素 α 满足方程式

$$f(x) = A_0x^n + A_1x^{n-1} + \cdots + A_{n-1}x + A_n = 0 \tag{1}$$

其中系数 $A_0,A_1,\cdots,A_{n-1},A_n$ 都在体 k 内,那么体 k 的扩张 $k(\alpha)$,即由所有系数取自 k,而且分母与 $f(x)$ 互素的那些 x 的有理函数的集合,形成一个体,我们称它是体 k 的单纯代数扩张.

我们假定多项式 $f(x)$ 在体 k 内是不可约的,否则,从体 $k(\alpha)$ 不含零因子的假设(见本章 §1,Ⅳ),我们由

$$f(\alpha) = \varphi(\alpha) \cdot \psi(\alpha) = 0$$

便可以推断出或者 $\varphi(\alpha) = 0$,或者 $\psi(\alpha) = 0$,二者必居其一. 于是就可以取这两个因式中的一个来作为 $f(x)$. 具有这种性质的多项式,除了属于 k 中的因子不计外,可以被唯一地确定.

定理 1 设 $k(\alpha)$ 的每一个元素都可以唯一地表作含 α 的多项式,且其次数小于 n.

证 设