HIT

数论经典著作系列

A Concise Introduction to Transcendental Number Theory

超越数论基础

于秀源 编著

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

超越数论基础

A Concise Introduction to Transcendental Number Theory

于秀源 编著

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

内 容 简 介

在介绍代数数基本知识的基础上，介绍了 Siegel 引理，Liouville 定理及其推广，Lindemann - Weierstrass 定理，A. O. Гельфонд 和 Th. Schneider 对 Hilbert 第七问题中关于数的超越性的证明，关于代数数对数的线形型下界的 Baker 定理，超越性度量，数 e 的超越性度量，数的代数无关性，以及 Mahler 分类.

本书可作为数学专业研究生教材，也可作为数学系高年级大学生选修课教材使用.

图书在版编目(CIP)数据

超越数论基础/于秀源编著. —哈尔滨：哈尔滨工业大学出版社，2011.3

ISBN 978 - 7 - 5603 - 3215 - 4

Ⅰ.①超…　Ⅱ.①于…　Ⅲ.①数论　Ⅳ.①O156

中国版本图书馆 CIP 数据核字(2011)第 038413 号

策划编辑　刘培杰　张永芹
责任编辑　翟新烨
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×1092mm　1/16　印张 7.25　字数 134 千字
版　　次　2011 年 3 月第 1 版　2011 年 3 月第 1 次印刷
书　　号　ISBN 978 - 7 - 5603 - 3215 - 4
定　　价　28.00 元

前言

超越数理论是数学的一个历史悠久的分支,可以追溯到提出“化圆为方”问题的古希腊时代.20 世纪以来,以 A. O. Гельфонд、Th. Schneider、A. Baker 等为代表的杰出数学家的工作使得超越数理论的研究和发展,无论在方法上,还是在研究成果方面,都取得了巨大进展和成就.这些成就对数学的其他分支也产生了深远的影响.

本书的目的,在于介绍超越数的基本理论和重要的研究方法,为读者进行这方面授深入研究提供基础.限于篇幅,本书不可能涉及超越数理论的全部内容和方法而是着重于 Гельфонд 方法、Schneider 方法、Baker 方法,以及与之有关的内容的介绍。毋庸讳言,本书内容会有不妥之处,希望读者指正.

于秀源

2011 年 1 月 31 日

目录

第一章 代数数的基本知识

代数数与超越数构成全体复数. 因此,任何关于代数数或超越数的命题常具有二重性. 例如,对于代数数的必要条件,可以构成对于超越数的充分条件. 所以,作为预备部分,本章主要叙述以后各章内容所涉及的代数数的基本概念和知识,以及有关多项式的几个定理. 对于一些熟知的定理,将证明略去了.

第一节　多项式

下面提到的多项式,都是指系数为有理数的多项式.

定理 1　对于任意的多项式 $f(x)$ 与 $g(x)$, $g(x)\neq 0$,必有多项式 $q(x)$ 与 $r(x)$,使得

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

其中 $r(x)\equiv 0$,或者是一个次数低于 $g(x)$ 的多项式.

两个多项式如果没有非常数的公因式,则称它们是互素的.

定理 2　多项式 $f(x)$ 与 $g(x)$ 互素的充要条件是:存在多项式 $A(x)$ 与 $B(x)$,使得

$$A(x)f(x)+B(x)g(x)=1.$$

多项式 $f(x)$ 如果没有次数比它低的非常数多项式因子,则称它是不可化的.

定理 3　每个 $n(n>0)$ 次多项式 $f(x)$,都可以分解成不可

化多项式的乘积.此外,若不计常数因子的差异及因子的次序,则这种分解式是唯一的.

定理4 设$f(x)$是有理系数的$n(n>0)$次多项式,如果可以分解成两个次数低于n的多项式之积,那么,$f(x)$以两个次数低于n的有理整系数多项式为其因式.

定理5 设$f(x)$与$g(x)$是多项式,而且$f(x)$是不可化的.若$f(x)=0$与$g(x)=0$有公共根,则$f(x)\mid g(x)$.

由此定理可知,若$f(x)$是有理系数的不可化多项式,则它的零点各不相同.

以下,讨论任意复系数多项式.

设多项式

$$f(x)=a_0x^m+\cdots+a_m\quad(m>0)$$

与

$$g(x)=b_0x^n+\cdots+b_n\quad(n>0)$$

的全部零点分别为$\alpha_1,\cdots,\alpha_m$与$\beta_1,\cdots,\beta_n$,称$m+n$阶行列式

$$Res(f,g)=\begin{array}{|llll|l}
a_0a_1\cdots a_m & & & & \\
 & a_0a_1\cdots a_m & & & \\
 & \ddots & \ddots & & \\
 & & a_0a_1\cdots a_m & & \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\}n \\
b_0b_1\cdots b_n & & & & \\
 & b_0b_1\cdots b_n & & & \\
 & \ddots & \ddots & & \\
 & & b_0b_1\cdots b_n & & \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\}m
\end{array}$$

为$f(x)$和$g(x)$的结式.

定理6 $Res(f,g)=a_0^n\prod\limits_{i=1}^{m}g(\alpha_1)=(-1)^{mn}b_0^m\prod\limits_{i=1}^{n}f(\beta_1)$.

此外,$f(x)$与$f'(x)$有公共零点的充要条件是

$$D(f)=a_0^{2n-2}\prod_{i>1}(\alpha_i-\alpha_j)^2=0$$

其中$D(f)$称为$f(x)$的判别式.

设$f(x_1,\cdots,x_n)$是n元多项式.如果对于n个变量$x_1,\cdots,x_n$的下标集$(1,2,\cdots,n)$进行任意一个置换后,$f(x_1,\cdots,x_n)$都不改变,则称$f(x_1,\cdots,x_n)$是n元对称多项式.

称

$$\sigma_1 = x_1 + x_2 + \cdots + x_n,$$
$$\sigma_2 = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n,$$
$$\vdots$$
$$\sigma_{n-1} = x_1x_2\cdots x_{n-1} + x_1x_2\cdots x_{n-2}x_n + \cdots + x_2x_3\cdots x_n$$
$$\sigma_0 = x_1x_2\cdots x_n$$

为 $x_1,\cdots,x_n$ 的初等对称多项式.

定理7 任何的系数在数环 R 中的 n 元对称多项式都可以唯一地表示为初等对称多项式 $\sigma_1,\cdots,\sigma_n$ 的多项式,而且它的系数也在 R 中.

第二节 代数数

在本书中,将以 $\mathbf{C},\mathbf{R},\mathbf{Q}$ 分别表示复数域,实数域和有理数域,以 $\mathbf{Z}$ 表示整数集合,以 $\mathbf{N}$ 表示全体自然数的集合. 此外,对于数集 K,以 $K[t]$ 表示形如

$$a_0t^m + a_1t^{m-1} + \cdots + a_m$$

的多项式的集合,其中 $a_i \in K \quad (0 \leqslant i \leqslant m)$.

定义1 设

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbf{Z}[x], (a_0 \neq 0). \tag{1}$$

若数 α 是 $f(x) = 0$ 的根,则称 α 是代数数.

若 $f(x)$ 是不可化多项式(即不存在非常数的 $g(x) \in \mathbf{Z}[x]$ 与 $h(x) \in \mathbf{Z}[x]$,使 $f(x) = g(x)h(x)$),而且 $a_0,\cdots,a_n$ 互素,

$$(a_0,a_1,\cdots,a_n) = 1,$$

则称 $f(x)$ 是 α 的最小多项式,α 是 n 次代数数,并称

$$h(\alpha) = \max_{0\leqslant i\leqslant m} |\alpha_i|$$

是 α 的高.

例如,i 是二次代数数,x^2+1 是它的最小多项式,$h(i) = 1$.

代数数也可定义为"系数为有理数的代数方程的根".

由定理5,代数数的最小多项式是唯一的.

定理8 若 α,β 是代数数,则 $\alpha\pm\beta,\alpha\beta$ 以及 $\dfrac{\alpha}{\beta}(\beta\neq 0)$ 都是代数数.

证明 以 $\alpha\beta$ 为例. 设 $\alpha = \alpha_1,\cdots,\alpha_m$ 与 $\beta = \beta_1,\cdots,\beta_n$ 分别是 α 与 β 的最小多项式的全部零点,而且这两个多项式的最高幂项系数分别为 $a_0(a_0\neq 0)$ 与 $b_0(b_0\neq 0)$,则 $\alpha\beta$ 满足方程

$$h(x) = (a_0b_0)^{mn}\prod_{i=1}^{m}\prod_{j=1}^{n}(x-\alpha_i\beta_j) = 0.$$

由多项式系数与零点的关系以及定理 7，可知 $h(x)$ 是有理整系数多项式，所以，$\alpha\beta$ 是代数数. 证毕.

由定理 8，全体代数数构成一个数域.

定义 2 若代数数 α 的最小多项式的最高幂项的系数为 1，则称它为代数整数.

定理 9 代数整数若是有理数，则必是有理整数. 代数整数的和、差、积仍是代数整数.

定理 10 设 α 是方程

$$Q(x) = \beta_0 x^n + \beta_1 x^{n-1} + \cdots + \beta_n = 0$$

的根，其中 $\beta_i(0 \leqslant i \leqslant n)$ 是代数整数，则 $\beta_0\alpha$ 是代数整数.

证明 由 $Q(\alpha) = 0$ 可知 $\beta_0\alpha$ 满足方程

$$\begin{aligned}\widetilde{Q}(x) &= x^n + \beta_1(\beta_0 x)^{n-1} + \cdots + \beta_n\beta_0{}^{n-1} \\ &= x^n + \gamma_1 x^{n-1} + \cdots + \gamma_n = 0.\end{aligned}$$

由定理 8，上式中的 $\gamma_i(1 \leqslant i \leqslant n)$ 是代数整数，设 $\gamma_i(1 \leqslant i \leqslant n)$ 的最小多项式的全部零点为

$$\gamma_i = \gamma_i^{(1)}, \gamma_i^{(2)} \cdots, \gamma_i^{(d_i)},$$

其中 d_i 是 γ_i 的次数，则由对称函数的性质，知

$$Q^*(x) = \prod_{i_1=1}^{d_1} \cdots \prod_{i_n=1}^{d_n} (x^n + \gamma_1^{i_1} x^{n-1} + \cdots + \gamma_n^{i_n})$$

是系数为有理整数的多项式，其首项系数为 1. 显然 $Q^*(\beta_0\alpha) = 0$，因此 $\beta_0\alpha$ 是代数整数. 证毕.

定理 11 设 $f(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_d = a_0(x - \alpha_1)\cdots(x - \alpha_d)$，其中 $a_i \in \mathbf{Z}(0 \leqslant i \leqslant d)$，则对于 $\{1,2,\cdots,d\}$ 的任一子集 $\{i_1,\cdots,i_k\}$，$a_0\alpha_{i_1}\cdots\alpha_{i_k}$ 是代数整数.

证明 首先，我们指出，如果

$$P(x) = \lambda_0 x^m + \lambda_1 x^{m-1} + \cdots + \lambda_m$$

是以代数整数为系数的多项式，$P(\alpha) = 0$，则 $\dfrac{P(x)}{x - \alpha}$ 也是以代数整数为系数的多项式.

事实上，当 $m = 1$ 时，结论是显然的. 假定结论对于 m 成立，那么，对于 $m + 1$ 次多项式.

$$P(x) = \lambda_0 x^{m+1} + \lambda_1 x^m + \cdots + \lambda_{m+1} \tag{1}$$

($\lambda_0 \cdots \lambda_{m+1}$ 是代数整数)，$P(\alpha) = 0$，由假定可知 $Q(x) = P(x) - (x - \alpha)\lambda_0 x^m$ 是一个以代数整数为系数的 m 次多项式，而且 $Q(\alpha) = 0$，因此

$$\frac{Q(x)}{x - \alpha} = \frac{P(x)}{x - \alpha} - \lambda_0 x^m \tag{2}$$

是一个以代数整数为系数的多项式，因而$\frac{P(x)}{x-\alpha}$也是以代数整数为系数的多项式．这样，由归纳法得到上面提到的结论．

现在证明定理结论．依次应用已经证得的结论，可知

$$P(x)\prod_{\substack{1\leqslant i\leqslant d, i\neq i_j\\ 1\leqslant j\leqslant k}}\frac{1}{x-\alpha_i}=a_0\prod_{j=1}^{k}(x-\alpha_{ij})$$

是以代数整数为系数的多项式，它的常数项

$$(-1)^k a_0 a_{i_1}\cdots a_{i_k}$$

当然是代数整数，由此证得定理．证毕．

定义 3　若 α 与$\frac{1}{\alpha}$都是代数整数，则称 α 为单位数．

定理 12　α 是单位数的充要条件是：α 满足一个首项系数为 1，而且末项系数为 ± 1 的有理整系数方程．

证明　由定义可推出．

第三节　有理数域的扩张

设 α 是 n 次代数数，记

$$E=\{a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1};a_1\in\mathbf{Q},0\leqslant i\leqslant n-1\}.$$

定理 13　E 是一个数域．此外，若

$$(a_0,a_1,\cdots,a_{n-1})\neq(b_0,b_1,\cdots,b_{n-1}),$$

其中 $a_i\in\mathbf{Q},b_j\in\mathbf{Q}(0\leqslant i,j\leqslant n-1)$，则

$$a_0=a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}\neq b_0+b_1\alpha+\cdots+b_{n-1}\alpha^{n-1}.$$

证明　设 α 的最小多项式为$f(x)$．又设

$$\lambda=a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}=a(\alpha)\in E,$$

$$\mu=b_0+b_1\alpha+\cdots+b_{n-1}\alpha^{n-1}=b(\alpha)\in E,$$

则 $\lambda\pm\mu\in E$ 是显然的．下面证明 $\lambda\mu$ 以及$\frac{1}{\mu}(\mu\neq 0)$ 也都 在 E 内，从而 E 是一个域．以 $\deg P(x)$ 表示多项式 $P(x)$ 的次数．

由定理 1 可知，存在有理系数多项式 $g(x)$ 与 $r(x)$，使得

$$a(x)b(x)=g(x)f(x)+r(x),\deg r(x)<\deg f(x)=n,$$

因此，由$f(\alpha)=0$ 得到

$$\lambda\mu=a(\alpha)b(\alpha)=g(\alpha)f(\alpha)+r(\alpha)=r(\alpha)\in E.$$

当 $\mu\neq 0$ 时，由于$f(x)$ 是不可化多项式，所以 $b(x)$ 与$f(x)$ 互素，从而存在

有理系数多项式 $p(x)$ 与 $s(x)$，使得

$$p(x)b(x)+s(x)f(x)=1, \deg p(x)<\deg f(x)=n,$$

因此

$$p(\alpha)\mu=p(\alpha)b(\alpha)+s(\alpha)f(\alpha)=1,$$
$$\mu^{-1}=p(\alpha)\in E.$$

最后，如果 $(a_0,a_1,\cdots,a_{n-1})\neq(b_0,b_1,\cdots,b_{n-1})$，但是

$$a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}=b_0+b_1\alpha+\cdots+b_{n-1}\alpha^{n-1},$$

那么 α 满足一个次数小于等于 $n-1$ 的代数方程，从而是一个次数小于等于 $n-1$ 的代数数，这与假设矛盾．所以定理的最后一个结论得证．证毕．

定义 4　设 α 是 n 次代数数，则数域

$$\mathbf{Q}(\alpha)=\{a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1};a_i\in\mathbf{Q},0\leqslant i\leqslant n-1\}$$

称为有理数域 $\mathbf{Q}$ 添加 α 所得到的单扩张，并称为 n 次代数数域，记 $n=[\mathbf{Q}(\alpha):\mathbf{Q}]$.

定理 14　若代数数 $\alpha\neq0$，则 $\mathbf{Q}(\alpha)$ 即是 α 经过加、减、乘、除（除数不为零）运算所得到的最大数集．

证明略．

定义 5　由有限个代数数 $\alpha_1,\cdots,\alpha_k$ 经加、减、乘、除（除数不为零）运算后所得到的数域，称为 $\mathbf{Q}$ 上的有限扩张，记为 $\mathbf{Q}(\alpha_1,\cdots,\alpha_k)$.

定理 15　对于任何 $\mathbf{Q}$ 上的有限扩张 $\mathbf{Q}(\alpha,\beta,\cdots,\gamma)$，总存在代数数 λ，使得

$$\mathbf{Q}(\lambda)=\mathbf{Q}(\alpha,\beta,\cdots,\gamma).$$

证明　仅就 $k=2$ 的情形证明．对于 $k>2$，可由归纳法及此处的方法给出证明．

设 α 与 β 的最小多项式的全部零点分别为

$$\alpha=\alpha_1,\alpha_2,\cdots,\alpha_n \text{ 与 } \beta=\beta_1,\beta_2\cdots,\beta_m,$$

取有理数 h，使得

$$h\neq\frac{\beta_i-\beta_j}{\alpha_k-\alpha_l}(1\leqslant k,l\leqslant n,1\leqslant i,j\leqslant m),$$

于是 mn 个数 $h\alpha_j+\beta_k(1\leqslant j\leqslant n,1\leqslant k\leqslant m)$ 各不相同．

记

$$\lambda=h\alpha+\beta,$$

则 λ 是代数数，且满足方程

$$F(x)=\prod_{f=1}^{n}\prod_{k=1}^{m}(x-(h\alpha_j+\beta_k))=0.$$

令

$$H(x)=F(x)\sum_{f=1}^{n}\sum_{k=1}^{m}\frac{\alpha_j}{x-(h\alpha_j+\beta_k)}, \tag{3}$$

则由对称函数的性质可知,$F(x)$ 与 $H(x)$ 都是有理系数的多项式,而且,式(3)导出

$$H(\lambda) = F'(\lambda)\alpha.$$

但是 $F(x)$ 没有重零点,$F'(\lambda) \neq 0$,从而

$$\alpha = \frac{H(\lambda)}{F'(\lambda)},$$

即 $\alpha \in \mathbf{Q}(\lambda)$,因此

$$\beta = \lambda - h(\alpha) \in \mathbf{Q}(\alpha).$$

于是

$$\mathbf{Q}(\alpha,\beta) \subseteq \mathbf{Q}(\lambda).$$

由此及显然的关系式

$$\mathbf{Q}(\lambda) \subseteq \mathbf{Q}(\alpha,\beta)$$

即可得出 $\mathbf{Q}(\lambda) = \mathbf{Q}(\alpha,\beta)$. 证毕.

由定理 15,$\mathbf{Q}$ 上的有限扩张总可归结为 $\mathbf{Q}$ 上的单扩张,因此,可以只讨论单扩张以替代对有限扩张的研究.

定义 6 设 $\alpha_1,\cdots,\alpha_k$ 与 λ 是代数数,λ 的次数是 d. 若

$$\mathbf{Q}(\alpha_1,\cdots,\alpha_k) = \mathbf{Q}(\lambda),$$

则记

$$d = [\mathbf{Q}(\alpha_1,\cdots,\alpha_k) : \mathbf{Q}].$$

第四节 基 底

设 λ 是 n 次代数数,$\lambda = \lambda_1,\lambda_2,\cdots,\lambda_n$ 是 λ 的最小多项式的全部零点.

定义 7 设 $\alpha_1 = \alpha \in \mathbf{Q}(\lambda)$,

$$\alpha = a(\lambda) = a_0\lambda^{n-1} + a_1\lambda^{n-2} + \cdots + a_{n-1}, a_i \in \mathbf{Q}(0 \leqslant i \leqslant n-1),$$

称

$$a_k = a(\lambda_k) \quad (k = 2,3,\cdots,n) \tag{4}$$

是 α 在 $\mathbf{Q}(\lambda)$ 上的共轭数,$\lambda_2,\cdots,\lambda_n$ 则称为 λ 的共轭数.

定理 16 设 $\alpha \in \mathbf{Q}(\lambda)$ 是 d 次代数数,其最小多项式为 $f(x)$,

$$f(x) = a_0x^d + \cdots + a_j, a_i \in \mathbf{Z}(0 \leqslant i \leqslant d).$$

又设

$$g(x) = \prod_{k=1}^{n}(x - \alpha_k),$$

其中 α_k 由式(4)确定,则 $g(x) \in \mathbf{Q}[x]$,而且

$$g(x)=c(f(x))^l,$$

其中 $l\in\mathbf{N},l\mid n,c\in\mathbf{Q}$.

证明 由定理 5 可以推出．证毕．

由定理 16，以 $\alpha=\alpha^{(1)},\alpha^{(2)},\cdots,\alpha^{(d)}$ 表示 α 的最小多项式的全部零点，则 α 在 $\mathbf{Q}(\lambda)$（λ 是 n 次代数数）上的全部共轭数恰好是 $\alpha^{(1)},\cdots,\alpha^{(d)}$ 的 $\frac{n}{d}$ 次重复．

定义 8 若在 $\mathbf{Q}(\lambda)$ 中存在一组数 $\alpha_1,\cdots,\alpha_m$，使得对于任意的 $x\in\mathbf{Q}(\lambda)$，都有唯一的表示式

$$x=a_1\alpha_1+\cdots+a_m\alpha_m,a_i\in\mathbf{Q}(1\leqslant i\leqslant m),$$

则称 $\alpha_1,\cdots,\alpha_m$ 是 $\mathbf{Q}(\lambda)$ 的一组基底．

例如，若 λ 是 n 次代数数，则 $1,\lambda,\cdots,\lambda^{n-1}$ 构成 $\mathbf{Q}(\lambda)$ 的一组基底．

定理 17 $\mathbf{Q}(\lambda)$ 中的任一组基底所含元素的个数相同．

证明略．

定义 9 设 $\alpha_1,\cdots,\alpha_n$ 是 $\mathbf{Q}(\lambda)$ 中的任意 n 个数，$n=[\mathbf{Q}(\lambda):\mathbf{Q}]$，称

$$\Delta(\alpha_1,\cdots,\alpha_n)=\begin{vmatrix}\alpha_1^{(1)}\cdots\alpha_n^{(1)}\\ \vdots\qquad\vdots\\ \alpha_1^{(n)}\cdots\alpha_n^{(n)}\end{vmatrix}^2$$

为 $\alpha_1,\cdots,\alpha_n$ 的判别式，其中 $\alpha_i=\alpha_i^{(1)},\alpha_i^{(2)},\cdots,\alpha_i^{(n)}$，是 α_i 在 $\mathbf{Q}(\lambda)$ 上的共轭数．

定理 18 判别式具有以下性质：

（ⅰ）$\Delta(\alpha_1,\cdots,\alpha_n)\in\mathbf{Q}$. 特别地，若 $\alpha_1,\cdots,\alpha_n$ 是代数整数，则

$$\Delta(\alpha_1,\cdots,\alpha_n)\in\mathbf{Z}.$$

（ⅱ）若 $\alpha_1,\cdots,\alpha_n$ 与 $\beta_1,\cdots,\beta_n$ 是 $\mathrm{Q}(\lambda)$ 的两组基底，则

$$\Delta(\alpha_1,\cdots,\alpha_n)\Delta(\beta_1,\cdots,\beta_n)>0.$$

（ⅲ）$\alpha_1,\cdots,\alpha_n$ 是 $\mathbf{Q}(\lambda)$ 的一组基底的充要条件，是 $\Delta(\alpha_1,\cdots,\alpha_n)\neq 0$.

证明 （ⅰ）由对称多项式的性质即可得证．

（ⅱ）设

$$\alpha_j=\sum_{k=1}^{n}a_{jk}\cdot\beta_k(1\leqslant j\leqslant n),$$

其中 $a_{jk}\in\mathbf{Q}(1\leqslant j,k\leqslant n)$，则显然有

$$\alpha_j^{(l)}=\sum_{k=1}^{n}a_{jk}\cdot\beta_k^{(l)}(1\leqslant l,j\leqslant n),$$

因此

$$\Delta(\alpha_1,\cdots,\alpha_n) = \begin{vmatrix} \alpha_1^{(1)}\cdots\alpha_n^{(1)} \\ \vdots \qquad \vdots \\ \alpha_1^{(n)}\cdots\alpha_n^{(n)} \end{vmatrix}^2 =$$

$$|a_{ij}|^2 \cdot \begin{vmatrix} \beta_1^{(1)}\cdots\beta_n^{(1)} \\ \vdots \qquad \vdots \\ \beta_1^{(n)}\cdots\beta_n^{(n)} \end{vmatrix}^2 =$$

$$|a_{ij}|^2 \cdot \Delta(\beta_1,\cdots,\beta_n), \tag{5}$$

其中 $|a_{ij}|$ 表示以 a_{ij},为其第 i 行、第 j 列元素的行列式.

由式(5)可得到结论(ii).

(iii)对于基底 $1,\lambda,\cdots,\lambda^{n-1}$,有

$$\Delta(1,\lambda,\cdots,\lambda^{n-1}) = \begin{vmatrix} 1 & \lambda\cdots\lambda^{n-1} \\ 1 & \lambda_2\cdots\lambda_2^{n-1} \\ & \vdots \\ 1 & \lambda_n\cdots\lambda_n^{n-1} \end{vmatrix}^2 =$$

$$\prod_{1\leqslant j<k\leqslant n}(\lambda_j-\lambda_k)^2 \neq 0,$$

由此及结论(ii),可知当 $1,\alpha,\cdots,\alpha_n$ 是一组基底时,

$$\Delta(\alpha_1,\cdots,\alpha_n) \neq 0.$$

另一方面,若 $\Delta(\alpha_1,\cdots,\alpha_n) \neq 0$. 令

$$\alpha_j = \sum_{k=1}^{n} b_{jk}\lambda^{k-1} \quad (1 \leqslant j \leqslant n),$$

则由

$$\Delta(\alpha_1,\cdots,\alpha_n) = |b_{jk}|^2\Delta(1,\cdots,\lambda^{n-1}),$$

可知行列式 $|b_{jk}| \neq 0$. 因此,$1,\lambda,\cdots,\lambda^{n-1}$ 可以由 $\alpha_1,\cdots,\alpha_n$ 线性表出,所以 $\alpha_1,\cdots,\alpha_n$ 是 $\mathbf{Q}(\lambda)$ 的一组基底. 证毕.

定义 10 设 $\omega_1,\cdots,\omega_m$ 是 $\mathbf{Q}(\lambda)$ 中的代数整数. 若 $\mathbf{Q}(\lambda)$ 中的任一代数整数都可唯一地表示为

$$a_1\omega_1+\cdots+a_m\omega_m \quad (a_i \in \mathbf{Z}, 1 \leqslant i \leqslant m),$$

则称 $\omega_1,\cdots,\omega_m$ 是 $\mathbf{Q}(\lambda)$ 的一组整底.

定理 19 在 $\mathbf{Q}(\lambda)$ 的一切由代数整数所组成的基底 $\{\alpha_1,\cdots,\alpha_n\}$ 中,使 $|\Delta(\alpha_1,\cdots,\alpha_n)|$ 取最小值的一组基底,必是整底.

证明 设 $\omega_1,\cdots,\omega_n$ 使得

$$|\Delta(\omega_1,\cdots,\omega_n)| = \min_{\{\alpha_1,\cdots,\alpha_n\}} |\Delta(\alpha_1,\cdots,\alpha_n)|,$$

其中 min 是对由代数整数组成的基底 $\{\alpha_1,\cdots,\alpha_n\}$ 取的.

若 $\omega_1,\cdots,\omega_n$ 不是整底,则必有代数整数 ω,

$$\omega = a_1\omega_1 + \cdots + a_n\omega_n,$$

其中至少有一个 a_i 不是有理整数．设 $a_1 \notin \mathbf{Z}$,令

$$a_1 = b + c, b \in \mathbf{Z} \quad 0 < c < 1,$$

则

$$\omega_1' = \omega - b\omega_1 = c\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n$$

也是代数整数,而且 $\omega_1',\omega_2,\cdots,\omega_n$ 也是 $\mathbf{Q}(\lambda)$ 的一组由代数整数构成的基底．此时

$$|\Delta(\omega_1',\omega_2,\cdots,\omega_n)| = c^2|\Delta(\omega_1,\cdots,\omega_n)| < |\Delta(\omega_1,\cdots,\omega_n)|,$$

这与 $\omega_1,\cdots,\omega_n$ 的选取矛盾．所以 $\omega_1,\cdots,\omega_n$ 必是一组整底．证毕．

推论　整底必是基底,因而含有 $n = [\mathbf{Q}(\lambda):\mathbf{Q}]$ 个元素．

定理 20　设 $\omega_1,\cdots,\omega_n$ 与 $\omega_1',\cdots,\omega_n'$ 是 $\mathbf{Q}(\lambda)$ 的两组整底,则

$$\Delta(\omega_1,\cdots,\omega_n) = \Delta(\omega_1',\cdots,\omega_n').$$

证明　由于 $\{\omega_i\}$ 与 $\{\omega_i'\}$ 都是整底,所以存在

$$a_{ij} \in \mathbf{Z}, b_{kl} \in \mathbf{Z} \quad (1 \leqslant i,j,k,l \leqslant n),$$

使得

$$\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j', \omega_k' \underset{l=1}{\overset{n}{=}} b_{kl}\omega_l, 1 \leqslant i,k \leqslant n$$

因此,行列式之积

$$|a_{ij}|\cdot|b_{kl}| = 1,$$

所以

$$|a_{ij}|^2 = |b_{kl}|^2 = 1.$$

由此及式(5)得证．

证毕．

第二章 Siegel 引理

这一章主要叙述代数数的一些基本性质,它们在超越数的研究中经常用到.

此外,还介绍利用众所周知的 Dirichlet 原则所得到的 Siegel 引理及其推广形式,这是在研究超越数理论时的一个广泛使用的工具.

最后,简单地介绍数的 Mahler 测度及其基本性质.

第一节　代数数的基本性质

定义 1　对于任意的多项式

$$P(x) = b_0x^r + \cdots + b_r,$$

称

$$L(P) = |b_0| + \cdots + |b_r| \text{ 与 } h(P) = \max_{0\le i\le r} |b_i|$$

分别为 $P(x)$ 的"长度"与"高".

定义 2　设代数数 α 的最小多项式是

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

则定义 $L(P)$ 与 $h(P)$ 分别为 α 的"长度"$L(\alpha)$ 与"高"$h(\alpha)$: