算學小叢書

理想數論初步

E. Landau 著
樊 畿 譯

商務印書館發行

算學小叢書

理想數論初步

E. Landau 著
樊 墀 譯

印書館發行

中華民國二十六年五月初版

算學小叢書

理想數論初步一冊

(5145)

Einführung in die elementare Theorie der algebraischen Zahlen und der Ideale

周 翥

每冊實價國幣叁角
外埠酌加運費匯費

原著者 E. Landau

譯述者 樊 墉 上海河南路

發行人 王 雲 五 上海河南路

印刷所 商務印書館 上海及各埠

發行所 商務印書館

馮序

有理整數分解成素因子時，其結果爲惟一。此卽所謂因子分解之定理是也。凡稍具初等數論之常識者，類能知之.在一般之代數數域中,因子分解之定理不必成立.但十九世紀中葉諸疇人皆疏於此事實，以爲此定理之眞確乃當然之事。

自衆知因子分解之定理不必成立後，此乃成爲代數數論上一大困難。Kummer 氏遂在分圓域 (Kreisteilungskörper) 中引入理想數,使因子分解之定理在此種域中得以成立.此後又有 Richard Dedekind 氏將理想數引入一般之數域中,於是代數數論賴理想數論之發生得以完備。

此書乃德國 Göttingen 大學教授 Edmund Landau 氏原著，乃氏在 Berlin 及 Göttingen 二大學歷年之講稿。Landau 氏爲當世解析學及數論大師，關於數論著作如 Handbuch der Lehre von der Verteilung der Primzahlen, Vorlesungen über Zahlentheorie 以及本書,世皆奉爲圭臬。但前二者皆卷帙浩繁，獨本書篇幅雖少，因取

材恰當，已足使初學者習知理想數論之概要．且論證精密，全書清晰簡潔，此乃 Landau 氏所著書之特點．

我國昔時習算學者多賴英文，而英美算學家以數論鳴者實尠，故至今中文高等算學書籍言數論者缺焉．樊君增性嗜代數學及數論，曾譯解析幾何與代數一書，已傳誦一時，有若干大學採爲教本．今復譯此書以餉世，其裨益於中國算學前途，豈淺鮮哉．

公曆一九三六年七月

馮漢叔序於北京大學

目　次

理想數論初步

§1. 多項式

定義1 本書中所謂多項式 (Polynom) 者，皆言一變數 x 之有理整函數，其係數爲有理數。

定義2 設一多項式不恆等於 0，而作

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots\cdots+a_0$$

($a_n\geqq 0$) 之形式，則 n 稱爲**多項式之次數** (Grad des Polynoms).

定理1 一個 n_1 次之多項式與一個 n_2 次之多項式之乘積爲一個 (n_1+n_2) 次之多項式。

證 顯然。

定義3 設有 $f(x)$, $g(x)$ 二多項式，且 $f(x)$ 不恆等於 0，若 $g(x)$ 等於 $f(x)$ 與另外某一個多項式之乘積，則謂 $g(x)$ 能被 $f(x)$ 除盡 [$g(x)$ durch $f(x)$ teilbar]，而以下之記號表之：

$$f(x)\,|\,g(x).$$

定理2 設 $f(x)|g(x)$, $g(x)|f(x)$, 則必 $f(x)=c\cdot g(x)$, 此處 c 爲一有理數.

證 由定理1可知 $f(x)$ 與 $g(x)$ 之次數相同, 故云.

定理3 設 $f(x)$, $g(x)$ 爲二多項式, 而無一恆等於0, 則必有一多項式 $h(x)$ 存在, 此 $h(x)$ 有下列二性質: 第一,

$$h(x)|f(x),\quad h(x)|g(x). \tag{1}$$

第二, $h(x)$ 必可表作

$$h(x)=F(x)\cdot f(x)+G(x)\cdot g(x), \tag{2}$$

此處 $F(x)$, $G(x)$ 爲二適當之多項式.

證 設 $h(x)$ 爲作 $F(x)\cdot f(x)+G(x)\cdot g(x)$ 形狀之不恆等於 0 的多項式之最低次者之一, 則吾謂 $h(x)$ 能滿足 (1) 式. 何則, 設 $f(x)$ 不能被 $h(x)$ 除盡, 則有

$$f(x)=q(x)\cdot h(x)+r(x),$$

此中 $q(x)$, $r(x)$ 皆爲多項式, 而 $r(x)$ 之次數低於 $h(x)$ 者, 於是

$$\begin{aligned} r(x)&=f(x)-q(x)\cdot h(x)\\ &=f(x)-q(x)\cdot[F(x)\cdot f(x)+G(x)\cdot g(x)]\\ &=F_1(x)\cdot f(x)+G_1(x)\cdot g(x). \end{aligned}$$

此結果與原設矛盾.

定理4 設 $f(x), g(x)$ 爲二多項式，而無一恆等於0，則必有一個且僅有一個多項式 $d(x)$ 存在，此 $d(x)$ 有下列三性質：第一，

(3) $$d(x)|f(x), \quad d(x)|g(x).$$

第二，凡一多項式 $k(x)$ 若能使

(4) $$k(x)|f(x), \quad k(x)|g(x)$$

二者成立，則必

(5) $$k(x)|d(x).$$

第三，$d(x)$ 之最高次項係數爲1.

證 1. 能滿足定理3所述性質之諸 $h(x)$ 中必有一多項式 $d(x)$，其最高次項係數爲1. 蓋 $h(x)$ 若能滿足定理3之性質，則不論 $c \geqq 0$ 爲任何有理數，$c \cdot h(x)$ 自亦能滿足定理3之性質也. 如此之 $d(x)$ 當然能適合條件(3)，又因

(6) $$d(x) = F_2(x) \cdot f(x) + G_2(x) \cdot g(x),$$

故從(4)可知條件(5)亦能滿足.

2. 設 $d_1(x), d_2(x)$ 二多項式皆能滿足定理4中所述之三性質，則因 $d_1(x)|d_2(x), d_2(x)|d_1(x)$，由定理2，$d_1(x)$ 與 $d_2(x)$ 二者必僅有一常數因子之別，然此常數必爲1，蓋已知 $d_1(x), d_2(x)$ 之最高次項係數皆爲1故也.

定義4 定理 4 中之 $d(x)$ 稱爲 $f(x)$ 與 $g(x)$ 之**最高公因式** (der grösste gemeinsame Teiler).

定義5 設若定理4中之 $d(x)=1$, 於是 $f(x)$ 與 $g(x)$ 之每一公因式皆爲常數,此時謂 $f(x)$ 與 $g(x)$ **互素** (teilerfremd).

定理5 一個零次多項式與每個不恆等於 0 之多項式爲互素.

證 顯然.

定理6 設 $f(x)$, $g(x)$ 爲二多項式,無一恆等於 0. 則當 $f(x)$ 與 $g(x)$ 互素時,方程式 $f(x)=0$ 與 $g(x)=0$ 無公根;且僅當 $f(x)$ 與 $g(x)$ 互素時,此二方程式始無公根.

證 1. 若有 $f(\xi)=0$ 與 $g(\xi)=0$, 則自 (6) 式, $d(\xi)=0$, 於是 $d(x)$ 不爲常數 1.

2. 設 $d(x)$ 不爲常數 1, 則其次數爲正, 於是根據代數之基本定理, 方程式 $d(x)=0$ 必有一根 ξ, 而由 (3) 式, ξ 亦爲 $f(x)=0$, $g(x)=0$ 之根.

定義6 一個不恆等於 0 之多項式 $f(x)$ 稱爲**可約** (reduzibel) 或**不可約** (irreduzibel), 全視其能否分解成

$$f(x)=f_1(x)\cdot f_2(x), \tag{7}$$

但此中 $f_1(x), f_2(x)$ 之次數須同爲正.

定理 7 凡 0 次或 1 次之多項式皆爲不可約.

證 應用定理 1.

定理 8 若 $c \neq 0$ 爲有理數,則當 $f(x)$ 爲不可約時, $c \cdot f(x)$ 亦爲不可約.

證 設若 $c \cdot f(x) = f_1(x) \cdot f_2(x)$, 則 $f(x) = \frac{1}{c} \cdot f_1(x) \cdot f_2(x)$, 於是 $f(x) = f_3(x) \cdot f_2(x)$, 此中 f_1, f_2, f_3 之次數皆爲正.

定理 9 設 $f(x)$ 爲不可約多項式, $g(x)$ 爲任意一多項式,而方程式

$$f(x) = 0 \tag{8}$$

之一根 ξ 能使

$$g(\xi) = 0 \tag{9}$$

滿足,則必

$$f(x) \mid g(x), \tag{10}$$

於是 (8) 式之任一根 η 皆能使

$$g(\eta) = 0.$$

證 1. 若 $g(x)$ 恆等於 0, 則 (10) 當然成立.

2. 若 $g(x)$ 不恆等於 0, 可設 $d(x)$ 爲 $f(x)$ 與 $g(x)$ 之最高公因式, 則因 $d(x) \mid f(x)$, 而 $f(x)$ 又爲不可約, 故或則

$d(x)=1$, 或則 $d(x)=c\cdot f(x)$. 但 $d(x)=1$ 爲不可能之事, 此乃由 (9) 與定理 6 可見者也. 故 $d(x)=c\cdot f(x)$, 而 $c\cdot f(x)\mid g(x), f(x)\mid g(x)$.

定理 10 一個不可約多項式 $f(x)$ 之次數若高於一個任意多項式 $g(x)$ 之次數時, 則 $f(x)=0$ 與 $g(x)=0$ 決無公根.

證 由定理 9, 若 $f(x)=0$ 與 $g(x)=0$ 有一公根, 則 $f(x)\mid g(x)$, 此與定理 1 相抵觸.

定理 11 $f(x)$ 若爲一個不可約多項式, 則 $f(x)=0$ 無重根.

證 若 $f(x)=0$ 有重根時, 則 $f(x)$ 之次數至少爲 2, 而 $f(x)=0$ 與 $f'(x)=0$ 有公根, 但 $f'(x)$ 之次數低於 $f(x)$ 者, 此與定理 10 相抵觸.

§2. 代數數

定義 7 對於一個複數 ϑ 若有一個不恆等於 0 之多項式 $f(x)$ 存在，能使

$$f(\vartheta)=0,$$

則 ϑ 稱爲代數數 (algebraische Zahl).

定理 12 每個代數數 ϑ 必能滿足一個方程式

$$g(\vartheta)=0,$$

此處 $g(x)$ 爲一個不恆等於 0 之整係數多項式.

證 定義 7 中之 $f(x)$ 之各項係數若不全爲整數，而各分數係數之分母之最小公倍數爲 r, 則令 $r\cdot f(x)=g(x)$ 即可.

定理 13 凡有理數皆爲代數數.

證 設 a 爲一有理數,則取 $f(x)=x-a$ 可也.

定理 14 每一代數數 ϑ 至少能滿足一個方程式 $f(x)=0$, 此處 $f(x)$ 爲不可約多項式.

證 在以 $x=\vartheta$ 爲根之一切多項式中，設 $f(x)$ 爲次數最

低者之一，則 $f(x)$ 必爲不可約；何則，設 $f(x)$ 爲可約，則由 (7)，$f_1(x)$ 與 $f_2(x)$ 之次數皆低於 $f(x)$ 者，但既有 $f(\vartheta)=0$，故必或則 $f_1(\vartheta)=0$，或則 $f_2(\vartheta)=0$. 此與原設矛盾.

定理 15 每一代數數 ϑ 能滿足一個且僅一個方程式 $f(x)=0$，此中 $f(x)$ 爲不可約多項式，且其最高次項係數爲 1.

證 從定理 14 與定理 8 可知如此之 $f(x)$ 至少有一個存在. 今設 $f(x)$ 與 $F(x)$ 皆有此性質，則由定理 9 吾人有 $f(x)|F(x)$, $F(x)|f(x)$, 故 $f(x)=F(x)$.

定義 8 設 ϑ 爲一代數數，$f(x)$ 爲定理 15 中所述之多項式，其次數爲 n，則稱 ϑ 爲 ***n* 次代數數** (algebraische Zahl n-ten Grades). 根據定理 11，方程式 $f(x)=0$ 之 n 個根 $\vartheta_1, \vartheta_2, \cdots\cdots, \vartheta_n$ (此中有一數爲 ϑ) 皆相異，此 n 個數稱爲與 ϑ **共軛之代數數** (die zu ϑ konjugierten algebraischen Zahlen).

定理 16 與一個 n 次代數數共軛之代數數亦爲 n 次代數數.

證 顯然 (定理 10).

定理 17 設 ϑ 爲一代數數，$\vartheta_1, \vartheta_2, \cdots\cdots, \vartheta_n$ 爲與 ϑ 共軛

之代數數，又 $g(x)$ 爲一多項式且 $g(\vartheta)=0$，則 $g(\vartheta_1)=0$，$g(\vartheta_2)=0,\cdots\cdots,\ g(\vartheta_n)=0$.

證 此由定理 9 自明.

定義 9 設 ϑ 爲一代數數，若有一多項式

$$g(x)=x^m+b_{m-1}x^{m-1}+\cdots\cdots+b_0$$

存在，其最高次項係數爲 1，其餘諸係數皆爲有理整數，而

$$g(\vartheta)=0,$$

則 ϑ 稱爲**代數整數** (ganze algebraische Zahl).

定理 18 凡有理整數皆爲代數整數，且凡有理數之爲代數整數者皆爲有理整數.

證 1. 設 a 爲一有理整數，則彼爲方程式

$$g(x)=x-a=0$$

之根.

2. 設一個不爲 0 之有理數 $\frac{q}{r}$ 爲代數整數 (q, r 爲互素之二有理整數)，則必

$$\left(\frac{q}{r}\right)^m+b_{m-1}\left(\frac{q}{r}\right)^{m-1}+\cdots\cdots+b_0=0,$$

此中諸 b 皆爲有理整數. 於是

$$q^m+b_{m-1}rq^{m-1}+\cdots\cdots+b_0r^m=0,$$

如是 r 爲 q^m 之約數，但 q 與 r 二者互素，故 $r=\pm 1$，而 $\frac{q}{r}$ 爲有理整數。

定義 10 以後本書中凡言整數者，意卽言代數整數。而言有理整數者，意卽言普通之 $0, \pm 1, \pm 2, \cdots\cdots$.

定理 19 與一整數共軛之數亦爲整數。

證 若整數 ϑ 能滿足方程式

$$g(x)=x^m+b_{m-1}x^{m-1}+\cdots\cdots+b_0=0,$$

(諸 b 皆爲有理整數)，則根據定理 17，與 ϑ 共軛之數亦能滿足方程式 $g(x)=0$.

定理 20 若 ϑ 爲一代數數，則必有一正有理整數 r 存在，能使 $r\vartheta$ 爲整數。

證 自定理 12，吾人可取 $m, c_m, \cdots\cdots, c_0$ 使

$$c_m\cdot\vartheta^m+\cdots\cdots+c_0=0,$$

此中諸 c 爲有理整數而 $c_m\geqq 0$. 於是

$$(c_m\vartheta)^m+c_{m-1}(c_m\vartheta)^{m-1}+c_{m-2}\cdot c_m\cdot(c_m\vartheta)^{m-2}+\cdots\cdots$$

$$+\cdots\cdots+c_0{c_m}^{m-1}=0,$$

卽 $$(|c_m|\vartheta)^m\pm c_{m-1}(|c_m|\vartheta)^{m-1}+\cdots\cdots\pm c_0{c_m}^{m-1}=0,$$

故 $|c_m|\cdot\vartheta$ 爲整數。

定理 21 1. 設 ϑ 爲一複數，且有 k 個不全爲 0 之複數

$\xi_1, \xi_2, \cdots\cdots, \xi_k$ 存在 $(k \geqq 1)$, 能使

$$(11)\qquad \begin{cases} \vartheta\xi_1 = a_{11}\xi_1 + \cdots\cdots + a_{1k}\xi_k, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \vartheta\xi_k = a_{k1}\xi_1 + \cdots\cdots + a_{kk}\xi_k \end{cases}$$

成立,而此中諸係數 a 皆爲有理數,則 ϑ 爲代數數,且其次數至多爲 k.

2. 若諸係數 a 不僅爲有理數而全爲有理整數,則 ϑ 爲整數。

證 自 (11) 式, k 個一次齊次方程式

$$\begin{cases} (\vartheta - a_{11})x_1 - a_{12}x_2 - \cdots\cdots - a_{1k}x_k = 0, \\ -a_{21}x_1 + (\vartheta - a_{22})x_2 - \cdots\cdots - a_{2k}x_k = 0, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ -a_{k1}x_1 - a_{k2}x_2 - \cdots\cdots + (\vartheta - a_{kk})x_k = 0 \end{cases}$$

有一組不全爲 0 之根 $\xi_1, \xi_2, \cdots\cdots, \xi_k$; 故

$$0 = \begin{vmatrix} \vartheta - a_{11}, & -a_{12}, \cdots, & -a_{1k} \\ \cdots\cdots\cdots\cdots\cdots\cdots & & \\ -a_{k1}, & -a_{k2}, \cdots, & \vartheta - a_{kk} \end{vmatrix} = \vartheta^k + c_{k-1}\vartheta^{k-1} + \cdots + c_0.$$

若諸 a 爲有理數,則上式中之諸 c 亦爲有理數;若諸 a 爲有理整數,則諸 c 亦爲有理整數。