クンマーの理想数論とは何だったか

付値論的解釈とその応用

足立恒雄[1]

ΕΙΣ ΤΑΣ ΑΝΑΜΝΗΣΕΙΣ

ΤΗΣ ΝΕΟΤΗΤΟΣ ΜΟΥ

クンマーの理想数はとても複雑で奇妙な技法であったのだが，デデキントがイデアルの概念を導入することによって理想数論を簡明に解釈し直した，と一般に信じられている（と思われる）．しかし実際には，理想数は決して複雑で奇妙な概念ではない．現今の可換代数の言葉で言えば，それは因子論であり，とくに体拡大に伴う因子の延長の理論である．本講演では，付値の延長をクンマーの方法で展開することによって，理想数の本質を明らかにする．

さらに，その考え方を一般的な加法付値の理論に生かせないかを考える．

目次

§1. クンマーの考えた道　p.2 - p.5

§2. 離散付値の延長　p.5 - p.11

§3. 加法付値の延長　p.11 - p.19

[1]q.n.adachi@gmail.com

1　クンマーの考えた道

1.1　素元分解の具体例

ℓ を固定された素数，そして有理数体 $\mathbb{Q}$ に 1 の ℓ 乗根を添加した体を K とし，その整数環を $\mathbb{O}$ とする：

$$K = \mathbb{Q}(\zeta),\quad \mathbb{O} = \mathbb{Z}[\zeta],\quad \zeta = \exp 2\pi i/\ell$$

p を

$$p \equiv 1 \pmod{\ell}$$

を満たす素数とする．p を K で素元分解することを考える．p が K で素元分解できるとすれば，素元 π が存在して

$$p = \mathrm{N_K}\pi = \pi\pi' \cdots \pi^{(\ell-2)}$$

となるはずである．ここに $\mathrm{N_K}$ は K からのノルムである．そこで仮に K に p 上の素元があるとして π とする．$\mathbb{O}/\mathbb{O}\pi = \mathbb{Z}/\mathbb{Z}p$ なので，

$$\zeta \equiv k \pmod{\pi}$$

を満たす有理整数 k が存在する．つまり $\zeta - k$ は π で割り切れる．したがって素因数を見つけるには $\zeta - k$ の約数から探せばよい．ここに k は，$\zeta^\ell = 1$ だから，次を満たす：

$$k^\ell \equiv 1\ (p),\quad k \not\equiv 1\ (p)$$

例　$\ell = 7,\ p = 29$ の場合

$$k^6 \equiv 1 \pmod{29}$$

の原始根として

$$k \equiv -4 \pmod{29}$$

を採る．π を p を割り切る（仮想的な）素元とすると

$$\zeta \equiv -4 \pmod{\pi}$$

としてよい．今 $N_K(\zeta + 4)$ を計算してみると

$$\mathrm{N_K}(\zeta + 4) = 29 \cdot 113$$

を得る．

$$f(\zeta) = \zeta^4 - \zeta^3 - 1$$

と置けば，

$$f(-4) = (-4)^4 - (-4)^3 - 1 \equiv -5 + 6 - 1 \equiv 0\ (29)$$

である．したがって $f(\zeta) \equiv 0\ (\pi)$ が成り立つ．計算してみると

$$N_K f(\zeta) = 29$$

が成り立つ．したがって $\pi = f(\zeta) = \zeta^4 - \zeta^3 - 1$ が $p = 29$ の素因数であって，

$$29 = \pi_1 \cdots \pi_6$$

が成り立っている．ここに $\pi_1 = \pi$ で，π_j は π_1 の共役である．

クンマーは ℓ が $\ell \leq 19$ なる素数である場合に，

$$p < 1000, \quad p \equiv 1\ (\ell)$$

を満たす全ての素数 p に対して $\mathbb{Q}(\zeta_\ell)$ における素元分解を具体的に与えた（1847）．

しかし $p = 23$ になると，この計算は破綻する：

命題 $\ell = 23$ のとき，$p = 47$ は $\mathbb{Q}(\zeta_\ell)$ で素元分解ができない．あるいはまた，言い換えれば既約元分解は一意的でない．

証明 $F = \mathbb{Q}(\sqrt{-23}) \subset \mathbb{Q}(\zeta_{23})$ であり，F の整数基は $[1, \omega], \omega = (1 + \sqrt{-23})/2$ である．

$$\mathrm{N}_F(a + b\omega) = a^2 + ab + 6b^2$$

だが，この 2 次形式は 47 を表せない．したがって，47 は $\mathbb{Q}(\zeta_{23})$ からのノルムにもならない．

4 が $k^{23} \equiv 1\ (47)$ の原始根であり，$1 - 4 + 4^{21} \equiv 0$ が成り立つことから，$1 - \zeta + \zeta^{21}$ を選んで計算すると，

$$\mathrm{N}_K(1 - \zeta + \zeta^{21}) = 47 \cdot 139$$

これによって，$1 - \zeta + \zeta^{21}$ が既約元であることがわかる．クンマーはもう一つの既約元分解を与えているが，それは省略する． O.E.Δ.

クンマーは $p < 1000$ の範囲で $p \equiv 1 \pmod{23}$ を満たす 8 個の素数 p のうち，3 個について素元分解を与え，5 個については素元分解ができないことを示している．

この研究に続いて，クンマーは理想数の導入に至る前に $p \not\equiv 1\ (\ell)$ なる場合の研究をしている（1846）．

1.2 理想数の導入

再度 $\ell = 23$ の場合を考え，

$$\varphi(\zeta) = 1 - \zeta + \zeta^{21}$$

と置く．$\varphi(\zeta)$ を始めとするノルムが 47 で割り切れる ζ の多項式には 47 の仮想的な因子が含まれていると考える．その仮想因子（つまり，クンマーの言う理想数）を P とすると P が持っている性質は次で特徴づけられる：

$$f(\zeta) \text{ is divisible by } P \Leftrightarrow\ f(\zeta)\Psi(\zeta) \equiv 0 \pmod{47}$$

ここに $\Psi(\zeta) = \mathrm{N_K}\varphi(\zeta)/\varphi(\zeta)$ であり，$\Psi(\zeta)$ は P 以外の 47 の約因子は全て備えている．

わかり易くするために現代的な記号と考え方で形式化する．

定義（理想数の現代風定義） K を円分体 $\mathbb{Q}(\zeta_\ell)$ とし，p を素数とする．K の整数 Ψ が次の 2 条件を満たすとき対 (p, Ψ) は p の理想数を定めると言う：

1. $\Psi \not\equiv 0 \pmod{p}$
2. K の整数 α, β に対して $\alpha\beta\Psi \equiv 0 \pmod{p}$ ならば

$$\alpha\Psi \equiv 0 \pmod{p}, \text{または } \beta\Psi \equiv 0 \pmod{p}$$

次に (p, Ψ_1) と (p, Ψ_2) が同じ理想数を定めるとは

$$\alpha\Psi_1 \equiv 0 \pmod{p} \iff \alpha\Psi_2 \equiv 0 \pmod{p}$$

が成り立つこととする．この関係は明らかに同値関係である．そこで (p, Ψ) で定まる同値類を p の**理想数**と呼ぶ．

定義 α が P で割り切れること（記号：$\alpha \equiv 0 \pmod{P}$）を

$$\alpha \equiv 0 \pmod{P} \iff \alpha\Psi \equiv 0 \pmod{p}$$

によって定義する．さらに

$$\alpha \equiv \beta \pmod{P} \iff \alpha - \beta \equiv 0 \pmod{P}$$

と定義する．

また α が P^μ で割り切れることを

$$\alpha \equiv 0 \pmod{P^\mu} \Longleftrightarrow \alpha\Psi^\mu \equiv 0 \pmod{p^\mu}$$

によって定義する．

以上のように定義されたあらゆる素数 p 上の理想数 P の全体の集合を生成系とする自由加群を考る．以後因子類群に進み，その有限性を証明して，フェルマーの大定理が正則素数の場合には正しいことを証明するに至るのだが，こうしたク

ンマーの業績については [2]，第 4 章「クンマーの金字塔」を参照．シャファレビッチ [4] は因子論を使って整数論を展開した珍しい本である．ちなみに言えば，Hasse はイデアル論が大嫌いで，類体論を有名にした “Berichte” を例外として，イデアルという概念を可能な限り避けていた（cf. Hasse, History of Class Field Thery in Cassels-Frölich [7]）.

2　離散付値の延長

2.1　基礎事項

本節は私が昔書いた論文 [1] の紹介である．クンマーの理想数論は実は因子論であることが Edwards[3] で詳細に解説されているが，一般化して付値の延長理論と捉えるとさらに自然なものとして理解できること，ならびに付値の延長に関する基本的ないくつかの定理が現今知られた方法（たとえば，シャファレヴィッチ [4]，永田 [5] 等）よりも容易に証明できることを話す.

まず予備知識として一般的な加法付値について基礎事項を記しておく.

K を体とし，Γ を（他のどの元よりも大きい元 ∞ が添付されているという意味で拡張された）全順序加群とする．写像 $v : K \to \Gamma$ が次の 3 条件を満たすとき，K の**加法付値**、略して単に**付値**であると言われる：

1. $v(x) = \infty \Leftrightarrow x = 0$
2. $v(xy) = v(x) + v(y) \quad (\forall x,\ \forall y \in K)$
3. $v(x; y) \geq \mathrm{Min}\{v(x), v(y)\}$

K を体とし，v を K の付値とするとき

$$A = \{x\ (\in K) \mid v(x) \geq 0\}, \quad \mathfrak{p} = \{x\ (\in K) \mid v(x) > 0\}$$

と置いて，A を v の**付値環**，$\mathfrak{p}$ を**付値イデアル**)，また $A/\mathfrak{p}$ を**剰余体**と呼ぶ．A は K において整閉であり，局所環（すなわち唯一の極大イデアルを持つ環）である.

L/K を有限次拡大とする（かならずしも分離拡大とは限らない)。V を L の付値とする。v の値群 Γ_v が V の値群 Γ_V に埋蔵できて、V が K 上では v と一致するとき、V は v の L への**延長**であると言われる。

2.2　離散付値の場合

特に $\Gamma_v = \mathbb{Z} \cup \{\infty\}$ のとき，v は K の**離散付値**と言われる．さらに v が全射であるとき正規化された離散付値と呼ばれる．この場合は，$v(\pi) = 1$ を満たす元が

存在するので，それを v の**一意化元**（uniformizer）と呼ぶ．$\mathfrak{p} = A\pi$ である．

補題 1　v を体 K の離散付値とする．上の設定の下に，L/K を（分離的とは限らない）有限次拡大とし，B を A の L における整閉包 (integral closure) とする．B の元 ψ が次の二つの性質を持つならば，

$$V(\pi) = V(\psi) + 1 \tag{1}$$

を満たす v の L への延長となる離散付値 V が存在する：

1. $\psi \not\equiv 0 \pmod{\pi}$
2. $\alpha, \beta \in B$ に対して

$$\alpha\beta\psi \equiv 0 \pmod{\pi} \Rightarrow \alpha\psi \equiv 0 \pmod{\pi} \ \vee \ \beta\psi \equiv 0 \pmod{\pi}$$

逆に V を v の L への延長となる離散付値とすると（1）ならびに条件 1.,2. が成り立つような $\psi \in B$ が存在する．

証明　$\xi(\neq 0) \in B$ に対して $\xi(\psi/\pi)^n \in B$ だが，$\xi(\psi/\pi)^{n+1} \notin B$ を満たす負でない整数 n を取る．B は完全整閉[2]であるから，こうした n の存在が証明される．そしてその n は一意的に定まるので，これを $V(\xi)$ と記す．また $V(0) = \infty$ とする．この V を L から $\mathbb{Z} \cup \{\infty\}$ への写像に持ち上げる．このとき V が付値の条件を満たすことが容易に証明される．

また $V(\pi/\psi) = 1$ は V の定義から明らかなので (1) が成り立つが，同時にこれは V が $\mathbb{Z}$ の上への写像であることも示している．

さらに u が A の単数であれば $V(u) = 0$, また $V(\pi^m) = mV(\pi)$ であるから，V は v の延長である．$V(\psi) + 1 = e$ と置けば，$V(K^\times) = e\mathbb{Z}$ となっていることに注意．

逆に V を v の L への延長となる離散付値とする．$V(\Pi) = 1$ を満たす $\Pi \in B$ を取る．$V(\pi) = e$ を満たす $e \geq 1$ が存在する．このとき $\alpha \in B$ に対して

$$\alpha \equiv 0 \pmod{\pi} \iff \alpha \equiv 0 \pmod{\Pi^e}$$

が成り立つ．そこで $\psi = \Pi^{e-1}$ と置けば，条件 1.,2. が成り立つことは明らかである．　O. E. Δ.

補題 2　$\psi \in B$ に対して

$$\overline{B\psi} = B\psi/B\pi = \{x\psi \bmod \mathrm{B}\pi \ ; \ x \in B\}$$

[2] $\xi \in L$ とする．ある $\alpha(\neq 0)$ があって，$\alpha\xi^n \in B$ $(\forall n \geq 0)$ ならば $\xi \in B$ が成り立つとき，B は完全整閉と呼ばれる．一般に，A が完全整閉な整域であれば商体 K の任意の拡大 L の整閉包 B は完全整閉である（ブルバキ [6]，第 V 章，演習問題 §1, no. 14.）

と書く．このとき ψ が補題 1 の 2 条件を満たすためには，$\overline{B\psi}$ が環 $\overline{B} = B/B\pi$ で極小イデアルを成すことが必要十分である．

証明　$\overline{B\psi}$ が $\overline{B}$ における極小イデアルとする．このとき ψ は条件 1.,2. を満足する．$\because\ \alpha\beta\psi \equiv 0 \pmod{\pi}$ とし，$\alpha\psi \not\equiv 0 \pmod{\pi}$ とする．$\overline{B\psi}$ の極小性により $\overline{B\alpha\psi} = \overline{B\psi}$ である．従って，$\psi \equiv \gamma\alpha\psi \pmod{\pi}$ を満たす $\gamma \in B$ が存在する．ゆえに，

$$\beta\psi \equiv \beta(\gamma\alpha)\psi \equiv \gamma(\alpha\beta\psi) \equiv 0 \pmod{\pi}$$

を得る．

逆に，$\psi \in B$ が条件 1.，2. を満たすとする．$\overline{B\alpha\psi} \subsetneq \overline{B\psi}$ となる $\alpha \in B$ が存在すると仮定する．$\overline{B\psi}$ から $\overline{B\alpha\psi}$ への全射を $x\psi \to x\alpha\psi$ から誘導する．$\dim_{\overline{A}}\overline{B\alpha\psi} < \dim_{\overline{A}}\overline{B\psi}$ であるから，この全射は単射ではない．すなわち $\overline{\beta\alpha\psi} = \overline{0}$ なる $\beta\psi(\not\equiv 0 \pmod{\pi})$ が存在する．つまり $\alpha\beta\psi \equiv 0 \pmod{\pi}$ だが，$\beta\psi \not\equiv 0 \pmod{\pi}$ なので $\alpha\psi \equiv 0 \pmod{\pi}$ である．従って $\overline{\alpha\psi} = \overline{0}$ が成り立つ．　O. E. Δ.

分析

1. 補題 1 の条件 1., 2. は次と同値である：

   $\overline{B\psi}$ に和と積を

   $$\overline{x\psi} + \overline{y\psi} = \overline{(x+y)\psi}, \quad \overline{x\psi} \cdot \overline{y\psi} = \overline{xy\psi}$$

   によって定義すれば，$\overline{B\psi}$ は体を成す．

2. $\varphi : B \to \overline{B\psi}$ を $\varphi(x) = \overline{x\psi}$ によって定義すれば，上に定義した $\overline{B\psi}$ の演算の下で φ は準同型全射になる．像が体なのだから $P = \mathrm{Ker}\ \varphi$ は B の極大イデアルである．

命題 1　体 K の離散付値は任意の有限次拡大体 L の付値に延長できる．$[L : K] = n$ ならば，K の付値は L へ高々 n 個の延長を有する．しかも延長付値はすべて離散的である。$V_j\ (j = 1, \ldots, g)$ を K の付値 v の L への延長付値のすべてとし，$B_j\ (j = 1, \ldots, g)$ をその付値環とすれば

$$B = \bigcap_{j=1}^{g} B_j$$

が成り立つ．ここに B は v の付値環 A の L における整閉包である．

証明　次の順に証明する：

1. 極小イデアルに対応する延長付値が少なくも一つ，しかし高々 n 個存在することを示す．

2. 極小イデアルに対応する延長付値の全体を $V_1, \ldots, V_g$ とすると，定理に述べた等式が成り立つことを示す.

3. 付値の（必ずしも離散付値と限らない）延長は極小イデアルからもたらされること，従って離散付値であることを示す.

第1段　$\overline{B} = B/B\pi$, $\overline{A} = A/A\pi$ と置く．$\{\overline{x}_j\}$ を $\overline{A}$ 上独立な元の系とすると，$\{x_j\}$ は K 上1次独立である．従って $\dim_{\overline{A}}\overline{B} \leq n = [L:K]$ が成り立つ.

$\{\overline{M}_j\}$ を $\overline{B}$ の極小イデアルの系とすると，$\sum_j \overline{M}_j$ は必然的に直和であり，$\overline{M}_j$ は $\overline{A}$ 上のベクトル空間だから，$\sum_j \overline{M}_j$ の次元も n を超えることはできない．従って，極小イデアルの数は n 以下である.

第2段　$V_1, \ldots, V_g$ を極小イデアルに対応して得られるような，v のすべての延長とし，$B_1, \cdots, B_g$ をそれぞれの付値環とする．$B \subseteq \cap_j B_j$ は自明だから，逆の包含関係を示す．$\alpha \notin B$ と仮定すると，$V_j(\alpha) < 0$ となる j が存在することを言えばよい．$\alpha = \beta/a$, $\beta \in B$, $a \in A$, $v(a) > 0$ と表すことができる．$\alpha \notin B$ であるから，$v(a) > 0$ である．これによって $\beta \not\equiv 0 \pmod{\pi}$ と仮定してよい．補題の結果から $V_j(\beta) < V_j(\pi)$ なる V_j が存在する（$\overline{B\beta}$ に含まれる極小イデアルを $\overline{B\psi}$ とすれば，これから作られる V_j が当該の性質を持つ）．したがって $V_j(\alpha) = V_j(\beta) - V_j(a) < V_j(\pi) - V_j(a) \leq 0$ である．これは $\alpha \notin B_j$ を意味し，逆の包含関係が示された.

第3段　延長は極小イデアルから得られる $V_1, \ldots, Vg$ に限ることを示そう．V をそれ以外の延長（必ずしも離散付値とは限らない）とする．付値の独立性から $V_j(\xi) \geq 0$ $(j = 1, 2, \ldots, g)$ で，$V(\xi) < 0$ なる $\xi \in L$ が存在するが，前者から $\xi \in B$，後者から $\xi \notin B$ が得られて矛盾を生じる．　O. E. Δ.

2.3　分岐分解定理

定義　V を（離散付値とは限らぬ）付値 v の L への延長とし，B を V の付値環，P をその付値イデアルとする．V の拡大 L/K における V の**分岐指数** e，ならびに V の**相対次数** f を次のように定義する：

1. $e = (V(L) \colon V(K))$

2. $f = [B/P : A/\mathfrak{p}]$

命題2 (分岐分解定理)　$V_1, \ldots, V_g$ を離散付値 v の L へのすべての延長とし，e_j, f_j をそれぞれの分岐指数，相対次数とすると，

$$\sum_{j=1}^{g} e_j f_j = [B/B\mathfrak{p} : A/\mathfrak{p}] \leq [L:K] \tag{2}$$

まず次の命題から始める：

命題３　K の離散付値 v の L への延長のすべてを $V_1, \ldots, V_g$ とし，それらの付値イデアルを $P_1, \ldots, P_g$ とすれば，

$$B\pi = \bigcap_j P_j^{e_j}$$

証明　$\alpha \in \bigcap_j \mathfrak{p}_j^{e_j}$ とすると $V_j(\alpha) \geq e_j$ が各 j に対して成り立つ．$V_j(\pi) = e_j$ だから $V_j(\alpha/\pi) \geq 0$ $(\forall j)$ となり，定理１から $\alpha \in B\pi = B\mathfrak{p}$ を得る．　O.E.Δ.

これまでに述べた命題１，命題２は離散付値ではなく，一般の加法付値でも成り立つ．しかし加法付値の場合は証明が難しくなる．離散付値の場合，付値環がネーター環で，しかも PID であることが証明を易しくする理由である．

命題２の証明　V_j の付値イデアルを P_j とし，$\mathfrak{p}_j = P_j \cap B$ とすると，

$$B/\bigcap_j \mathfrak{p}_j^{e_j} \cong B/\mathfrak{p}_1^{e_1} \oplus \cdots \oplus B/\mathfrak{p}_g^{e_g}$$

なぜなら $\mathfrak{p}_i$ と $\mathfrak{p}_j$ は $i \neq j$ のとき互いに素，つまり $\mathfrak{p}_i + \mathfrak{p}_j = (1)$ だからである．

さらにまた $B/\mathfrak{p}_j^{e_j} \cong B_j/P_j^{e_j}$ だから, 上の系と合わせて，

$$B/B\pi \cong B_1/P_1^{e_1} \oplus \cdots \oplus B_g/P_g^{e_g}$$

である．$\overline{A}$ 上のベクトル空間の列

$$B_j/P_j^{e_j} \supsetneq P_j/P_j^{e_j} \supsetneq \cdots \supsetneq P_j^{e_j-1}/P_j^{e_j}$$

を考える．$\overline{A}$ 上のベクトル空間として

$$(P_j^{k-1}/P_j^{e_j})/(P_j^k/P_j^{e_j}) \cong P_j^{k-1}/P_j^k \cong B_j/P_j$$

であるから，

$$\dim_{\overline{A}} P_j^{k-1}/P_j^{e_j} - \dim_{\overline{A}} P_j^{k-1}/P_j^{e_j} = \dim_{\overline{A}} B_j/P_j = f_j$$

従って

$$\dim_{\overline{A}} B_j/P_j^{e_j} = e_j f_j$$

である．従って $\dim_{\overline{A}} \overline{B} = \sum_j e_j f_j$ が得られた．一方では定理 1 の証明中に示した通り $\dim_{\overline{A}} \overline{B} \leq n$ が成り立つ．　O. E. Δ.

命題４　L/K を離散付値 v を持つ体 K の有限次拡大とする。次の場合は (2) において等号が成り立つ．すなわち

$$\sum_{j=1}^{g} e_j f_j = [B/B\mathfrak{p} : A/\mathfrak{p}] = [L : K]$$

が成り立つ：

1. L/K が分離拡大である．
2. K が v に関して完備である．
3. A がある体上有限生成である．

証明　(1) L/K が分離拡大の場合，$L = K(\theta),\ \theta \in B$ とし，$f(x)$ を θ の満たすモニック既約多項式とすれば，

$$f'(\theta) \neq 0,\ \text{かつ}\ \mathrm{f'(\theta)B} \subseteq \mathrm{A}[1, \theta, \ldots, \theta^{\mathrm{n}-1}]$$

がわかる．A は PID なので B も A 上階数 n ($= [L : K]$) の自由加群である．これより容易に $[B/B\mathfrak{p} : A/\mathfrak{p}] = [L : K]$ が従う．
(2) K が完備であるとする．$B/B\pi = \overline{A}[\overline{\xi_1}, \ldots, \overline{\xi_m}]$ とすると，$\alpha \in B$ に対し，

$$\alpha = a_1\xi_1 + \cdots + a_m\xi_m + \pi\alpha_1, \quad \alpha_1 \in B$$

と表せる．α_1 に同じ操作を行い，これを続ければ，A が完備であることから，$\alpha \in A[\xi_1, \ldots, \xi_m]$ がわかる．従って $m = n$ でなければならない．故に B は A 上階数 n の自由加群である．
(3) A がある体上有限生成のとき B が有限生成 A 加群となることは永田 [5] にある（定理 3.9.5）．　O. E. Δ.

命題 4 の３．は一般の加法付値でも成り立つが，１.，２．の証明には離散付値という条件が使われる．分離拡大でなければ，等号が成り立たない例がシャファレヴィッチ [4] にある（第３章 §4. 問題９）．一般的な加法付値で L/K が分離拡大の場合にどうなるかは現在検討中である．

3　加法付値の延長

3.1　極大イデアルと極小イデアル

v を体 K の加法付値とする．A を v の付値環，$\mathfrak{p}$ を付値イデアルとする．
L/K を分離的とは限らない有限次拡大とする．K の L における整閉包を B とする．さらに，$\overline{B} = B/B\mathfrak{p},\ \overline{A} = A/\mathfrak{p}$ と記す．

以下の話は次の二つのステップからなる．

1. $\overline{B} = B/B\mathfrak{p}$ の極小イデアルと B の極大イデアルの間の 1 対 1 対応を与える．

2. B の極大イデアルと L の延長付値の間の 1 対 1 対応を与える．

命題 1　B の極大イデアルの個数は有限であり，$\overline{B}$ の極小イデアルの個数も有限である．

証明　$\overline{B}$ のすべての極小イデアル（体）の集合を X とする[3]．B のすべての極大イデアルの集合を Y とする．$\overline{B\psi} \in X$ に対して自然な全射 $J : B \to \overline{B\psi}$ の核 P は Y の元である．この $\overline{B\psi}$ に P を対応させる対応を Φ と記そう．

Φ は全射である．なぜなら $P \in Y$ に対して $\overline{P}$ に含まれる極小イデアルを一つ取って $\overline{B\psi}$ とすると，P による局所化 $B_P = S_P^{-1}B$ を考えるとすぐわかるように，$\overline{P\psi} = \overline{0}$ が成り立つ．すなわち $\Psi(P) = \overline{B\psi}$ であるからである．

$\overline{B}$ はベクトル空間として $\overline{A}$ 上有限次元（$\leq n = [L : K]$）[4]であるが，極小イデアルの和は直和であって，ベクトル空間としての次元は n を超えることができない．つまり X は有限集合である．　O.E.Δ.

次に極大イデアル P に L の付値を対応させることを考えよう．

補題 1　整閉整域 B と極大イデアル P の組 (B, P) が次の意味で極大性を持てば B は商体 L の付値環である：

$$B \subseteq B' \subsetneq L, \quad P \subseteq P' \ \Rightarrow B' = B, \ P' = P$$

証明　(B, P) が上に述べた意味で極大であるとする．B が付値環である条件は $x \in L^\times$ に対して $x \notin B$ ならば，$1/x \in B$ が成り立つことである．そこで $x\,(\neq 0) \in L$ に対して $x \notin B$，しかも $1/x \notin B$ である x が存在したとせよ．

$P \subsetneqq P[1/x],\ B \subsetneqq B[1/x]$ なので (B, P) の極大性により，$1 \in P[1/x]$ である．故に

$$1 = a_0 + a_1/x + \cdots + a_n/x^n, \quad a_j \ \in P \ (j = 0, 1, \ldots, a_n)$$

と表せる．従って

$$(1 - a_0)x^n + a_1x^{n-1} + \cdots + a_n = 0$$

$1 - a_0$ は B の単数であるから x は B 上整的である．B は整閉だから $x \in B$ が示されたが，これは仮定に反する．故に B は付値環である．　O. E. Δ.

補題 2　(B, P) を体 L の整閉部分環とその極大イデアルの組とすると，

$$B \subseteq B' \subsetneq L, \quad P \subseteq P'$$

[3]極小イデアルは単項イデアルであることに注意．また $X = \{\overline{B}\}$ という場合も起こり得る．

[4]その証明には A が付値環なので，有限生成のイデアルは単項イデアルであることが使われる．

を満たす付値環 $(B',\ P')$ が存在する．

証明　$B \subseteq B_\lambda \subsetneq L,\ P \subseteq P_\lambda$ を満たす L の部分環 B_λ とその極大イデアル P_λ の対 $(B_\lambda,\ P_\lambda)$ の成す族を $\mathfrak{X}$ としよう．$\mathfrak{X}$ は自明な包含関係によって帰納的順序集合を成すことは明らかので，ツォルンの補題によって極大ペア (B', P') が存在する．(B', P') は前補題によって付値環である．　O.E.Δ.

命題 2　L/K を有限次拡大，v を K の付値，A をその付値環，B を A の L における整閉包，P を B の極大イデアルとする．(B', P') を $B \subseteq B' \subsetneq L,\ P \subseteq P'$ なる付値環とすれば $B' = B_P$（B の P による局所化）である．

証明　$\alpha \in B'$ とする．

$$1/(1+\alpha+\cdots+\alpha^s) \in B, \quad \alpha/(1+\alpha+\cdots+\alpha^s) \in B$$

なる自然数 $s(\geq 2)$ が存在する（永田 [5], 補題 4.8.3.）[5]．従って，

$$1/(1+\alpha+\cdots+\alpha^s) \in B',\ \alpha/((1+\alpha+\cdots+\alpha^s) \in B'$$

$\alpha \in B'$ なので，まず第 1 式から $1+\alpha+\cdots+\alpha^s$ は B' の可逆元であることがわかるから，$(1+\alpha+\cdots+\alpha^s)^{-1} \notin P'$ となる．故に

$$(1+\alpha+\cdots+\alpha^s)^{-1} \in B - P$$

従って

$$\alpha = \alpha(1+\alpha+\cdots+\alpha^s)^{-1}/(1+\alpha+\cdots+\alpha^s)^{-1} \in B_P$$

これにより $B' \subseteq B_P$ が示された．逆の包含は自明である．　$O.E.\Delta$

この命題によって $B/\mathfrak{p}$ の極小イデアルの成す族，B の各極大イデアルの成す族，L の付値環 B_P の成す族の濃度がいずれも等しいことが分かった．

3.2　一般の分岐分解定理

命題 3　K を体，v をその付値，A をその付値環とする．L を K の有限次拡大とし，B を A の L における整閉包とする．v の L へのすべての（同値でない）延長を $V_1, \ldots, V_g$ とし，各 V_j の付値環を B_j とすると次が成り立つ：

$$B = \bigcap_j B_j$$

[5]残念ながらここだけ self-contained でない．加法付値の条件から直接示せる簡単な補題だが，証明は省略する．

さらに I を B のイデアルとすると

$$I = \bigcap_j I_j^*$$

ここに I_j^* は I の P_j に関する充満化，すなわち $I_j^* = I_P \cap B$ とする．

証明　$\subseteq$ は自明なので，逆の包含を示す．$x \in \bigcap_j B_j$ とせよ．B_j の極大イデアル P_j に対して $s_j x \in B$ を満たす $s_j \in B - P_j$ を取る（$B_j = B_{P_j}$ に留意せよ）．$\{s_j\}_j$ の生成するイデアルはどの極大イデアルにも含まれないので B に一致する．従って

$$1 = \sum_{j=1}^{g} a_j s_j, \quad a_j \in B \ (\forall j)$$

と表せる．故に

$$x = \sum_{j=1}^{g} a_j s_j x \in B$$

これで証明が終わった．I に関しても同様である．　O.E. Δ.

定義　G を順序集合とする．G の部分集合 H $(\neq \emptyset)$ が上界集合（major set）であるとは，$x \in H$ かつ $x \leq y$ ならば $y \in H$ が満たされることを言う．

注意

1. $V_j(B_j)$ の上界集合 H は B_j のイデアル I によって

   $$H = \{V_j(x) \mid x \in I\}$$

   と表せる集合として特徴付けられる．

2. $V_j(B_j\mathfrak{p})$ は上界集合だが，$V_j(\mathfrak{p})$ は上界集合ではない．

定義　$V(B_j)$ の上界集合の個数を付値 V_j の（あるいは P_j の）**第一分岐指数**[6]と称し，ϵ_j と記す．ϵ_j は P_j と $B_j\mathfrak{p}$ の間にあるイデアルの数と言い換えることができる．

命題 4　以上の定義と記号の下に次が成り立つ：

1. $[B/B\mathfrak{p} : A/\mathfrak{p}] \leq n$; 従って特に $f_j \leq n = [L : K]$ が成り立つ．
2. $[B_j/B_j\mathfrak{p} : A/\mathfrak{p}] = \epsilon_j f_j$

[6] ブルバキ [6] による．

証明　$\overline{\xi_1},\ldots,\overline{\xi_m}$ が $\overline{B}=B/B\mathfrak{p}$ の $\overline{A}=A\mathfrak{p}$ 上１次独立な系であるとする．$\xi_1,\ldots,\xi_m$ は K 上でも１次独立であることを示せば，これは $m\leq[L:K]$ を意味する．

仮に

$$a_1\xi_1+\cdots+a_m\xi_m=0 \qquad (1)$$

がすべては 0 ではないある $a_1,\ldots,a_m\ (\in K)$ に対して成り立つとすると，分母を払って各 a_j は A の元であるとしてよい．A は付値環なので有限生成のイデアルは単項イデアルである．従って $(a_1,\ldots,a_m)=a$ を満たす $a\in A$ が取れる．両辺を a で割ることにより，少なくとも一つ $a_i\not\equiv 0\pmod{\mathfrak{p}}$ としてよい．(1) 式を $\mathfrak{p}$ を法として考えて，

$$\overline{a_1}\overline{\xi_1}+\cdots+\overline{a_m}\overline{\xi_m}=\overline{0}$$

を得るが，これは $\overline{\xi_1},\ldots,\overline{\xi_m}$ が $\overline{B}$ の $\overline{A}$ 上１次独立な系であるという仮定に反する．すなわち $\xi_1,\ldots,\xi_m$ は K 上１次独立である．

P_j に対応する $\overline{B}$ の極小イデアルを $\overline{B\psi_j}$ とすると $B/P_j\cong\overline{B\psi_j}\subseteq\overline{B}$ であるから，$f_j=\dim_{\overline{A}}B/P_j\leq\dim_{\overline{A}}\overline{B}\leq n$ が成り立つ．

2.　$V_j(B_j)$ の上界集合 $(\supseteq V_j(B_j\mathfrak{p}))$ と B_j のイデアル（$\supseteq B_j\mathfrak{p}$）との１対１対応を考えれば，$\epsilon_j$ は B_j のイデアル（$\supseteq B_j\mathfrak{p}$）の成す組成列の長さに等しい．しかし B_j の組成列の各イデアル間の商加群は B/P_j に同型であって，$\overline{A}$ 上の次元は f_j である．故に $[B_J:B_j/B_j\mathfrak{p}]=\epsilon_jf_j$ が成り立つ．　O.E.Δ.

命題 5　B の極大イデアルを $P_1,\ldots,P_g$ とすると

$$\sum_{j=1}^{g}\epsilon_jf_j=[B/B\mathfrak{p}:A/\mathfrak{p}]$$

証明　$\mathfrak{q}_j$ を $B\mathfrak{p}$ の P_j に関する充満化，すなわち $\mathfrak{q}_j=B_j\mathfrak{p}\cap B$ とすると，§3, 命題 3 によって

$$B/B\mathfrak{p}\cong\bigoplus_{j=1}^{g}B/\mathfrak{q}_j\cong\bigoplus_{j=1}^{g}B_j/B_j\mathfrak{p}$$

が成り立つ．これに上の命題を適用すれば結果が得られる．　O.E.Δ.

命題 6

$$e_jf_j\leq[L:K]$$

証明　V_j,B_j を $V,\ B$, また $e_j,\ f_j$ を $e,\ f$ と添え字 j を略する．$r\leq e$ なる自然数を任意に取る。e の定義により $V(x_i)\not\equiv V(x_j)\pmod{V(K^\times)}\ (i\neq j)$ を満たす B の元 $x_i\ (i=1,...,r)$ が取れる．また f の定義により B の元 $y_j\ (j=1,...,f)$ を P を法として考えた $\overline{y_1},...,\overline{y_f}$ が $\overline{A}$ 上１次独立であるように選ぶことができる．

x_iy_j $(i=1,\dots r; j=1,\dots,f)$ が K 上1次独立であることを示せば，$ef \le [L:K]$ が示されたことになる．

仮に非自明な関係

$$\sum_{i,j} a_{ij}x_iy_j = 0, \quad a_{ij} \in A \ (i=1,..,r; j=1,...,f)$$

があるとする．これを書き換えて

$$\left(\sum_{i=1}^{r} a_{i1}x_i\right) y_1 + \cdots + \left(\sum_{i=1}^{r} a_{if}x_i\right) y_f = 0$$

$i \neq i'$ ならば $V(a_{ij}x_i) \neq V(a_{i'j'}x_{i'})$ である．なぜなら仮に等号が成り立つとすると $V(x_i) - V(x_{i'}) = V(a_{ij}) - V(a_{i'j'}) \in V(K)$ を得て，x_i の選び方に反するからである．そこで $V(a_{i_0j_0}x_{i_0})$ が最小値であるとする．上式の両辺を $a_{i_0j_0}x_{i_0}$ で割ると，$i \neq i_0$ のとき $a_{ij}x_i/a_{i_0j_0}x_{i_0} \equiv 0 \pmod{P}$ だから，

$$(a_{i_01}/a_{i_0j_0})y_1 + \cdots + (a_{i_0f}/a_{i_0j_0})y_f \equiv 0 \pmod{P}$$

しかも y_{j_0} の係数は1だから．これは $\overline{y_1},\dots,\overline{y_f}$ が $\overline{A}$ 上で1次独立という仮定に反する． O.E.Δ.

命題 7 L/K を有限次拡大とする．体 K の指数付値 v の L への延長 V の第一分岐指数を ϵ，また分岐指数を e とする．このとき

1. v の付値イデアル $\mathfrak{p}$ が単項イデアルであることと V の付値イデアル P が単項イデアルであることは同値である．

2. $\mathfrak{p}$ が単項イデアルならば，$\epsilon = e$ である．従って $e < +\infty$ が成り立つ．

3. （ブルバキ [6], 第6章，§6.8, 命題4）$\mathfrak{p}$ が単項イデアルではないならば，$\epsilon = 1$ である．このときまた v の延長付値 V は唯一つである．

証明 V の付値環を B とし，P を付値イデアルとする．
1. $V(P)$ が最小値を持つ場合．その値が $V(\Pi)$ であるとする．$B\Pi^k = P^k$ であり，また $P^e \subseteq B\mathfrak{p}$ が成り立つ．$\overline{B} = B/B\mathfrak{p}$ のイデアルに関する降下列

$$\overline{B} \supsetneq \overline{P} \supsetneq \overline{P^2} \supsetneq \cdots \supsetneq \overline{P^{e-1}} \supsetneq \{\overline{0}\}$$

を考えると，これは組成列である．何故なら，$\overline{P^k} \supsetneq \overline{I} \supsetneq \overline{P^{k+1}}$ なるイデアル I があるとすると，$kV(\Pi) < V(x) < (k+1)V(\Pi)$ なる $x \in I$ が存在することになるが，これは $V(\Pi)$ の最小性に反するからである．従って第一分岐指数の定義により $e = \epsilon$ である．

次に $V(\mathfrak{p})$ にも最小値が存在することを示す．$B\mathfrak{p} = P^{\epsilon}$ であるから $\epsilon V(\Pi) \leq V(x) \leq (\epsilon+1)V(\Pi)$ を満たす $x \in \mathfrak{p}$ が存在するが，$V(\Pi)$ の最小性によって $V(x) = \epsilon V(\Pi)$ あるいは $V(x) = (\epsilon+1)V(\Pi)$ である．もしすべての $x \in \mathfrak{p}$ に対して後者が成り立つなら $V(B\mathfrak{p}) = V(P^{\epsilon+1})$ となるから $V(x) = \epsilon V(\Pi)$ を満たす $x \in \mathfrak{p}$ が存在する．こうした x を一つ取って π とすると $V(\pi) = \epsilon V(\Pi)$ である．

2. $V(P)$ が最小値を持たない場合．$G = V(P),\ H = V(B\mathfrak{p})$ とする．$x \in G$ を任意に取ると，仮定によって $0 < z < x$ なる $z \in G$ が無数に存在する．$(G : H) = \epsilon < +\infty$ だから G の H によるの一つの類に，0 と x の間に収まる複数の元，例えば，z_1, z_2 が存在する．$0 < z_i < x\ (i = 1, 2)$ によって，その差 y は $y \in H$ であって，$0 < y < x$ を満たす．H は上界集合だから $x \in H$ である．従って $H = G$，すなわち $\epsilon = 1$ である．従ってまた $v(\mathfrak{p})$ も最小値を持たない．

V を改めて V_j, P を P_j と置き直す．A の L における整閉包 $\mathrm{Ic}(A; L)$ を B，また $P_J \cap B = P$ とする．上では $P_j = B_j\mathfrak{p}$ を証明したのだが，$V_j(B) = V_j(B_j), V_j(P) = V_j(P_j)$ であることを考えて証明を見直せば，結局 $P = B\mathfrak{p}$ が成り立つことがわかる．これは延長 V_j の取り方に関係なく成り立つのだから，延長付値は唯一であることがわかる．　O.E.Δ.

この命題によって V(P) が最小値を持つときは，$P \supsetneq \mathfrak{q}$ なる素イデアルが存在する（すなわち付値の階数が 2 以上である）としても，$\bigcap_n P^n \supsetneq \mathfrak{q}$ であること，つまり分岐指数は付値群の最小部分にしか関係しないことがわかる．従って次の系が得られる．

系　加法付値 v がいわゆる**準離散付値**，すなわち体 K の付値群 $v(K^{\times})$ が辞書式順序を備えた加群 $\mathbb{Z}^n$ である場合，あるいはさらには付値群が，Γ を任意の全順序加群として，辞書式順序を備えた加群 $\Gamma \times \mathbb{Z}$ という形をしている場合は，有限次拡大体 L/K の任意の延長付値 V に対して分岐指数は第一分岐指数に等しい．

証明　v の L への延長付値を V とする．先の証明に見る通り，$V(P)$ が最小値を有するかどうかは K の付値 v が同じ性質を持っているかどうかによって決まる．命題に挙げた形の全順序加群には最小元が存在するので命題によって $e = \epsilon$ が成り立つ．　O.E.Δ.

命題 8（付値の分岐分解定理）　体 K の加法付値 v の付値環を A，付値イデアルを $\mathfrak{p}$ とする．K の任意の有限次拡大 L における v のすべての（同値でない）延長を $V_1, \ldots, V_g$ とする．このとき次の不等式が成り立つ：

$$\sum_{j=1}^{g} e_j f_j \leq [L : K] \qquad (3.2)$$

証明　**1．** $v(\mathfrak{p})$ が最小値を持たない場合は先の命題 7 により付値の延長は一つしか存在しない．従って命題 6 は定理の主張を意味している．
2． $\mathfrak{p}$ が最小値を持つ場合は，命題 7 の 2. により $e_j = \epsilon_j$ であるから，命題 5 が適用できる．　O.E.Δ.

註

1. $\mathfrak{p}$ が単項イデアルである場合は $\epsilon = e$ が成り立つという事実は簡単ながらも重要な事実だが，ブルバキ [6] は見落としたのではないかと思われる．もちろん，本稿における推論に誤りがなければ，の話である．

2. 知られている命題 3.5 の証明（例えば，ブルバキ [6], 永田 [5]）はかなり厄介であり，また数学的帰納法が使われていて，本質が見えにくい．本稿のようにすれば見通しが良く簡潔であろう．

命題 9　Lk を付値 v を備えた体 K の有限次拡大とするとき、次の 4 条件は同値である：

1. B が A 上有限生成の加群である．

2. B が自由 A 加群である．

3. $[B/B\mathfrak{p} : A/\mathfrak{p}] = [L : K]$

4. $\sum_j e_j f_j = [L : K]$ ，かつ各 j に対して $\epsilon_j = e_j$ が成り立つ．

証明　1. $\Leftrightarrow$ 2. は A の有限生成のイデアルは単項であることから容易に示せる．
2. $\Rightarrow$ 3. も明らか．3. $\Rightarrow$ 2. はあまり容易ではない．$\xi_1, \ldots, \xi_n,\ (n = [L : K])$ を $B/B\mathfrak{p}$ の基底となる B の元とする．$L = A[\xi_1, ..., \xi_n]$ と置く．$\alpha \in B$ を任意に取り，$M = L + A\alpha$ として $M = L$ を証明れば，$L = B$ が示せたことになる．$\dim_{\overline{A}} B/B\mathfrak{p} = n$ であることから自然な準同型写像 $/L\mathfrak{p} \to M/M\mathfrak{p}$ が全射であることがわかる．従って $M = L + M\mathfrak{p}$ が成り立つ．M は有限生成 A 加群なので中山の補題から $M = L$ が従う（証明の詳細はブルバキ [6]，第 VI 章，§8.5. 定理 2 を参照せよ）．
3. $\Leftrightarrow$ 4. の証明：命題 5，および命題 8 によって

$$[B/B\mathfrak{p} : A/\mathfrak{p}] = \sum_j \epsilon_j f_j \leq \sum_j e_j f_j \leq [L : K]$$

が成り立つことから得られる．　O. E. Δ.

命題 10　加法付値 v がいわゆる**準離散付値**，すなわち体 K の値群 $v(K)$ が辞書式順序を備えた加群 $\mathbb{Z}^n$ である場合，あるいはさらには値群が，Γ を任意の全順序加

群として，辞書式順序を備えた加群 $\Gamma \times \mathbb{Z}$ という形をしている場合は，有限次拡大体 L/K の任意の延長付値 V_j に対して分岐指数 e_j は第一分岐指数 ϵ_j に等しい．

証明　v の L への延長付値を V とする．先の証明に見る通り，$V(P)$ が最小値を有するかどうかは K の付値 v が同じ性質を持っているかどうかによって決まる．命題に列挙した全順序加群には最小元が存在するので命題 7 によって $e_j = \epsilon_j$ である．従って特に命題 7 の系が成り立つ．　O.E.Δ.

重要な例　$K = \mathbb{Q}(X, Y)$ とする．

$$v(aX^m Y^n) = m + n\sqrt{2}, \quad a \in \mathbb{Q},\ m, n \in \mathbb{Z}$$

と定義すれば，これから K に付値 v が誘導される．値群は $v(K^\times) = \mathbb{Z} + \mathbb{Z}\sqrt{2}$，付値イデアル $\mathfrak{p}$ はそのうち $m + n\sqrt{2} > 0$ を満たす元の全体である．さらに

$$\{x\ (\in K) \mid v(x) = 0\} = \left\{ a\frac{1+f}{1+g} \mid a \in \mathbb{Q}^\times,\ f, g \in \mathfrak{p} \right\} = \mathbb{Q} + \mathfrak{p}$$

であるから剰余体は $\mathbb{Q}$ に同型である．$v(\mathfrak{p})$ には最小元が存在しないので，$\epsilon = 1$, $\mathfrak{p}^2 = \mathfrak{p}$ が成り立っている．

次に，$L = K(\sqrt{X})$ とする．L/K は分離拡大である．$V(aX^{m/2}Y^n) = m/2 + n\sqrt{2}$ から誘導される v の L への延長 V を考える．$V(L^\times) = \mathbb{Z}/2 + \mathbb{Z}\sqrt{2}$ であり，付値イデアル P はそのうち $m/2 + n\sqrt{2} > 0$ となる元の全体である．また剰余体は K の場合と同様で $\mathbb{Q}$ と同型である．以上から $e = 2$, $\epsilon = 1, f = 1$ が従う．

なお，K の付値環 A は単項イデアル整域ではなく，また A の L における整閉包 B も A 加群として有限生成ではない．

参考文献

[1] Adachi, N., A Valuational Interpretation of Kummer's Theory of Ideal Numbers, Proc. Japan Acad., 61, Ser A (1985) 235-238

[2] 足立恒雄『フェルマーの大定理—整数論の源流』

[3] Edwards, H. M., The Genesis of Ideal Theory, Arch. Hist. Exact Sci., 23 (1980) 321-378

[4] ボレビッチ=シャフハレビッチ『整数論』 第 3 章 整除の理論

[5] 永田雅宜『可換体論』第 I V章 付値

[6] ブルバキ『可換代数』 第 7 章 付値

[7] Cassels=Frölich, Algebraic Number Theory