応用代数学特論講義ノート

安藤哲哉

はじめに

応用代数学特論は，付値の話と順序体の話の 2 本建てである．付値は付値体と付値環の両方について説明する．千葉大学での講義ノートであるが，大学院修士 1 年生，または学部 4 年生あたりを対象に書かれている．また，講義 14 回の授業構成を前提に書かれている．

第 I 部 付値

1. 付値体

以下の乗法的付値の定義は，永田雅宜「可換体論」§4.1 の定義と異なっている (同値でもない) が，現在では以下の定義を採用するほうが多い．永田氏の本では (3) をもっと弱い (一般的な) 条件にしているが，結果的に以下の定義を採用した場合と同じことになる．

定義 1.1. K は体とする．写像 $v\colon K \to \mathbb{R}$ が以下の (1), (2), (3) を満たすとき，v は K 上の**乗法的付値**であるという．また，乗法的付値 v を 1 つ固定した体 K を**付値体**といい，付値体 (K, v) などと表す．

(1) (正定値性) 任意の $x \in K$ に対し $v(x) \geqq 0$ である．また，$v(x) = 0 \iff x = 0$ である．

(2) (乗法性) 任意の $x, y \in K$ に対し $v(xy) = v(x)v(y)$ が成り立つ．

(3) (三角不等式) 任意の $x, y \in K$ に対し $v(x+y) \leqq v(x) + v(y)$ が成り立つ．

以下の条件 (4) は (3) より強い条件であるが，$v\colon K \to \mathbb{R}$ が条件 (1), (2), (4) を満たすとき，v は**非アルキメデス付値**であるという．$v\colon K \to \mathbb{R}$ が乗法的付値であって非アルキメデス的付値でないとき，v は**アルキメデス付値**であるという．

(4) 任意の $x, y \in K$ に対し $v(x+y) \leqq \max\{v(x), v(y)\}$ が成り立つ．

例 1.2. (1) K は $\mathbb{C}$ の部分体とする．$v\colon K \to \mathbb{C}$ を $v(x) = |x|$ (x の絶対値. $x \in K$) で定めると，v はアルキメデス的付値である．この付値 v を絶対値と呼ぶ．

(2) $K = \mathbb{Q}$ とし，p を素数とする．$x \in \mathbb{Z}$ が $x = p^n a$ (a は p と互いに素な整数, n は非負整数) と書けるとき，$\operatorname{ord}_p x = n$ と定める．例外的に，$\operatorname{ord}_p 0 = +\infty$ と定める．また，$x \in \mathbb{Q}$ の場合 $x = \dfrac{y}{z}$ (y, $z \in \mathbb{Z}$) と分数で表せるので，$\operatorname{ord}_p x = \operatorname{ord}_p y - \operatorname{ord}_p z$ と定義する．これは x の分数表示に依存しないで一意的に定まる．$x \in \mathbb{Q}$ に対し，$v(x) = p^{-\operatorname{ord}_p x}$ と定める．ただし，$v(0) = p^{-\infty} = 0$ とする．すると，v は非アルキメデス的付値である．この v を v_p などとも書き，p **進付値**という．

(3) K は体とし，$0 \neq x \in K$ に対し $v(x) = 1$ と定め，$v(0) = 0$ と定めると，v は K 上の非アルキメデス的付値になる．この v を**自明な付値**という．

(4) R は UFD(素元分解整域) で，$p \in R$ は素元とする．$0 \neq a \in R$ に対し，$a \in p^n R$ かつ $a \notin p^{n+1}R$ ($n \in \mathbb{N} \cup \{0\}$) のとき $\operatorname{ord}_p a = n$ とし，$\operatorname{ord}_p 0 = -\infty$ と定める．$K = Q(R)$ (R の分数体) とし，$x = a/b$ ($a, b \in R$) に対して，$\operatorname{ord}_p x = \operatorname{ord}_p a - \operatorname{ord}_p b$ が矛盾なく定義できる．そして，$v(x) = 2^{-\operatorname{ord}_p x}$ と定めると，v は K 上の非アルキメデス的付値になる．

UFD でない整域 R や，素元でない p の場合に上の定義を拡張する場合には，$\operatorname{ord}_p x$ や $v(x)$ が矛盾なく定義できていて，所望する性質を満たしているかどうか，よく確認すること．

命題 1.3. K は体，$v\colon K \to \mathbb{R}$ は乗法的付値とする．このとき，以下が成り立つ．

(1) $v(1) = 1$ である．

(2) 任意の $x \in K$ に対し $v(-x) = v(x)$ が成り立つ．

(3) $0 \neq x \in K$ に対し $v\left(\dfrac{1}{x}\right) = \dfrac{1}{v(x)}$ が成り立つ．

(4) v が非アルキメデス的ならば，任意の $n \in \mathbb{N}$ に対し $v(n \cdot 1_K) \leqq 1$ である．ここで 1_K は K の単位元である．

証明. (1) $v(1) = v(1^2) = \big(v(1)\big)^2$ だから $v(1) = 0$ または $v(1) = 1$ である．しかし $v(x) = 0$ となるのは $x = 0$ の場合に限るから $v(1) = 1$ である．

(2) $\big(v(-1)\big)^2 = v((-1)^2) = v(1) = 1$ だから，$v(-1) = \pm 1$ である．$v(-1) \geqq 0$ であったから，$v(-1) = 1$ となる．よって，$v(-x) = v((-1)x) = v(-1)v(x) = 1 \cdot v(x) = v(x)$ である．

(3) $v(x)v(1/x) = v(x \cdot (1/x)) = v(1) = 1$ からわかる．

(4) $n \in \mathbb{N}$ の場合に $v(n \cdot 1_K) \leqq 1$ であることは，$n \geqq 2$ のとき $v(n \cdot 1_K) \leqq \min\big\{v((n-1) \cdot 1_K), v(1_K)\big\}$ より，帰納法ですぐ証明できる．$n < 0$ のときは (2) からわかる． □

定義 1.4. K は体，$v\colon K \to \mathbb{R}$ と $w\colon K \to \mathbb{R}$ は乗法的付値とする．ある正の実数 c が存在して，任意の $x \in K$ に対して $v(x) = \big(w(x)\big)^c$ が成り立つとき，付値 v と w は**同値**であるという．$b = 1/c$ とおく

と $v(x)=\big(w(x)\big)^c$ と $w(x)=\big(v(x)\big)^b$ は同値であるので，付値の同値は同値条件であることがわかる．

定理 1.5. K は体，$v\colon K\to\mathbb{R}$ と $w\colon K\to\mathbb{R}$ は乗法的付値とする．
(1) v と w が同値であるための必要十分条件は，任意の $x\in K$ に対し，$v(x)<1\iff w(x)<1$ が成り立つことである．
(2) v が自明でない付値のときは，任意の $x\in K$ に対し $v(x)<1\Longrightarrow w(x)<1$ が成り立てば，v と w は同値である．

証明. (2) v は自明でないから，$v(x)\neq 1$ となる $0\neq x\in K$ が存在する．$v(x)>1$ ならば $v(1/x)<1$ だから，$v(a)<1$ を満たす $0\neq a\in K$ が存在する．この a を 1 つ固定する．$v(a)=s$, $w(a)=t$ とし，$c=\log_s t$ とおく．$v'(x):=\big(v(x)\big)^c$ $(\forall x\in K)$ で付値 v' を定める．$v'(a)=s^c=t=w(a)<1$ である．
(2-i) $0\neq x\in K$, $v(x)<1$ の場合に $v'(x)=w(x)$ が成り立つことを示す．各 $n\in\mathbb{N}$ に対し

$$\big(v'(a)\big)^{(m(n)+1)/n}<v'(x)\leqq\big(v'(a)\big)^{m(n)/n}$$

を満たす $m(n)\in\mathbb{N}$ が一意的に存在する．$v'(x)=\lim_{n\to\infty}\big(v'(a)\big)^{m(n)/n}=\lim_{n\to\infty}\big(w(a)\big)^{m(n)/n}$ である．他方，

$$v'(x^n)=\big(v'(x)\big)^n<\big(v'(a)\big)^{m(n)}=v'(a^{m(n)})$$

より，$v'(x^n/a^{m(n)})\leqq 1$ だから $w(x^n/a^{m(n)})\leqq 1$ が成り立ち $\big(w(x)\big)^n\leqq\big(w(a)\big)^{m(n)}$ が成り立つ．同様に，$\big(v'(a)\big)^{(m(n)+1)/n}\leqq v'(x)$ から $\big(w(a)\big)^{(m(n)+1)/n}\leqq w(x)$ が導かれる．よって，

$$w(x)=\lim_{n\to\infty}\big(w(a)\big)^{(m(n)+1)/n}=\lim_{n\to\infty}\big(w(a)\big)^{m(n)/n}=v'(x)$$

が成り立つ．
(2-ii) $x\in K$, $v(x)>1$ の場合は，(2-i) より $v'(1/x)=w(1/x)$ が成立するから $v'(x)=w(x)$ が成り立つ．
(2-iii) 最後に $v(x)=1$ の場合は $v(ax)<1$ だから，(2-i) より $v'(ax)=w(ax)$ が成り立ち，$v'(a)=w(a)$ だから $v'(x)=w(x)$ が成り立つ．また，$v(x)=0$ ならば $x=0$ で $v'(x)=0=w(x)$ である．
以上で，$v'(x)=w(x)$ $(\forall x\in K)$ が示され，v と w は同値である．
(1) は (2) からすぐわかる． □

命題 1.6. K は体，$v\colon K\to\mathbb{R}$ は乗法的付値とする．もし，任意の $n\in\mathbb{N}$ に対し $v(n\cdot 1_K)\leqq 1$ ならば，v は非アルキメデス的である．ここで，1_K は K の単位元である．

証明. $x\in K$, $n\in\mathbb{N}$ のとき $v(nx)=v(n\cdot 1_K\cdot x)=v(n\cdot 1_K)v(x)\leqq 1\cdot v(x)=v(x)$ であることに注意する．
$x,y\in K$, $v(x)\geqq v(y)$ と仮定して $v(x+y)\leqq v(x)$ を証明する．$n\in\mathbb{N}$ のとき，$(x+y)^n$ の二項展開を考えると，$0\leqq k\leqq n$ のとき $v(x)^kv(y)^{n-k}\leqq v(x)^n$ だから

$$\begin{aligned}\big(v(x+y)\big)^n=v((x+y)^n)&=v\left(\sum_{k=0}^{n}{}_nC_kx^ky^{n-k}\right)\\&\leqq\sum_{k=0}^{n}v\left({}_nC_kx^ky^{n-k}\right)\leqq\sum_{k=0}^{n}v(x^ky^{n-k})\leqq\sum_{k=0}^{n}v(x)^kv(y)^{n-k}\leqq(n+1)v(x)^n\end{aligned}$$

となる．よって，$v(x+y)\leqq\sqrt[n]{n+1}v(x)$ となる．ここで，$n\to+\infty$ とすると $v(x+y)\leqq v(x)$ を得る．
□

系 1.7. K は標数 p (素数) の体，$v\colon K\to\mathbb{R}$ は乗法的付値とする．
(1) v は非アルキメデス的である．
(2) K が有限体ならば，v は自明である．

証明. (2) K の元の個数を q とすると，$K^\times=K-\{0\}$ は位数 $q-1$ の巡回群だから，任意の $x\in K^\times$ に対して $\big(v(x)\big)^{q-1}=v(x^{q-1})=v(1)=1$ となる．$v(x)>0$ だから $v(x)=1$ で，v は自明な付値である．

(1) v がアルキメデス的だとすると，ある $0 \neq n \in \mathbb{F}_p \subset K$ で $v(n) > 1$ を満たすのものが存在する．しかし，(2) より v は $\mathbb{F}_p$ 上では自明な付値で，$v(n) = 1$ となり矛盾する． □

2. 付値環

定理 2.1. K は体，$v\colon K \to \mathbb{R}$ は非アルキメデス的付値とする．

$$R = \left\{x \in K \;\middle|\; v(x) \leqq 1\right\}, \quad \mathfrak{m} = \left\{x \in K \;\middle|\; v(x) < 1\right\}$$

とおくと，R は $\mathfrak{m}$ を唯一の極大イデアルとする局所環である．また，任意の $x, y \in R$ に対して，$x \in Ry$ または $y \in Rx$ が成り立つ．

この R を (K, v) の**付値環**といい，$\mathfrak{m}$ を**付値イデアル**という．

証明. (1) $(R, \mathfrak{m})$ が局所環であることを示す．

$x, y \in R$ のとき，$v(x+y) \leqq \max\{v(x), v(y)\} \leqq 1$, $v(xy) = v(x)v(y) \leqq 1$ だから R は可換整域になる．同様にして，$\mathfrak{m}$ が R のイデアルであることが証明できる．I は R のイデアルで $I \neq R$ とする．もし $x \in I$ が $v(x) = 1$ を満たせば，$v(1/x) = 1$ だから $1/x \in R$ である．すると，$1 = (1/x)x \in I$ となり $I = R$ となる．よって，$x \in I$ ならば $v(x) < 1$ で $x \in \mathfrak{m}$ となる．したがって，$I \subset \mathfrak{m}$ で，$\mathfrak{m}$ は R の唯一の極大イデアルである．

(2) $x, y \in R$ ならば $x \in Ry$ または $y \in Rx$ を示す．

$v(x) \leqq v(y)$ ならば $v(x/y) \leqq 1$ なので $x/y \in R$ である．よって $x \in Ry$ である．同様に $v(x) \geqq v(y)$ ならば $y \in Rx$ である． □

この定理を念頭において，可換環論の視点から付値環の定義を与え，体の非アルキメデス的付値との関係を順次明らかにしていく．

定義 2.2. R は可換整域とする．「$x, y \in R$ ならば $x \in Ry$ または $y \in Rx$」が成り立つとき，R は**付値環**であるという．

定理 2.3. R は可換整域, $K = Q(R) := \left\{ \dfrac{x}{y} \;\middle|\; x, y \in \mathbb{R}, y \neq 1 \right\}$ は R の分数体とする．このとき，次の (1), (2), (3) は同値である．

(1) R は付値環である．

(2) $x \in K$, $x \notin R$ ならば $1/x \in R$.

(3) R は局所環で，R の任意の有限生成イデアルは単項イデアルである．

証明. (1) $\Longrightarrow$ (2). $x \in K$, $x \notin R$ とする．$x = y/z$ $(y, z \in R)$ と書ける．$y/z \notin R$ だから $y \notin Rz$. R は付値環だから $z \in Ry$. つまり，$1/x = z/y \in R$ である．

(2) $\Longrightarrow$ (1). $x, y \in R$, $x \notin Ry$ とする．$x/y \in K - R$ だから，(2) より $y/x \in R$ となる．つまり $y \in Rx$.

(1) $\Longrightarrow$ (3). $\mathfrak{m} := \left\{x \in R \;\middle|\; 1/x \notin R\right\}$ とおく．$I \neq R$ を I の任意のイデアルとする．$x \in I$, $1/x \in R$ とすると $1 = (1/x)x \in I$ となり $I = R$ となってしまうから，$x \in I$ ならば $1/x \notin R$ である．よって，$I \subset \mathfrak{m}$ である．これは，$\mathfrak{m}$ が R のイデアルであり，しかも唯一の極大イデアルであることを意味する．

さて，イデアル $I = Ra + Rb \subsetneqq R$ を考える．$a \in Rb$ または $b \in Ra$ であるが，前者なら $I = Rb$, 後者なら $I = Ra$ となる．以下，n に関する帰納法で，$I = (a_1, \ldots, a_n) \subsetneqq R$ が有限生成イデアルのとき，ある $1 \leqq k \leqq n$ が存在して $I = Ra_i$ となることが同様にして証明できる．

(3) $\Longrightarrow$ (1). (3) を仮定する．$x, y \in R$ とし $x \in Ry$ または $y \in Rx$ を示す．$x \neq 0$, $y \neq 0$ と仮定してよい．$Rx + Ry$ は単項イデアルだから，$Rx + Ry = Rz$ を満たす $z \in R$ が存在する．$x \in Rz$ だから $x/z \in R$ である．同様に $y/z \in R$. $R \cdot (x/z) + R \cdot (y/z) = R \cdot (z/z) = R$ だから，x/z, y/z の少なくとも一方は $\mathfrak{m} := \left\{x \in R \;\middle|\; 1/x \notin R\right\}$ に属さない．$x/z \notin \mathfrak{m}$ と仮定してよい．すると，$z/x \in R$ だから $Rx = Rz$ で $y \in Rz = Rx$ となる． □

定理 2.4. R は Nother 局所整域で，$\mathfrak{m}$ は R の唯一の極大イデアルとする．(このとき，$(R, \mathfrak{m})$ は Nother 局所整域であるという)．このとき，以下の (1), (2), (3) は同値である．

(1) R は付値環である．
(2) R は PID(単項イデアル整域) である．
(3) $\mathfrak{m}$ は単項イデアルで $\operatorname{Krull\,dim} R = 1$ である．

以上のいずれか (よってすべて) が成り立つとき R は**離散付値環**であるという．このとき，(0) でも R でもない R のイデアル I は，ある自然数 n によって $I = \mathfrak{m}^n$ と表せる．特に，$\mathfrak{m} = R\pi$ となる $\pi \in R$ (このような π を R の**素元**という) を用いて，$I = (\pi^n) = R \cdot \pi^n$ と表せる．

証明. (1) $\Longrightarrow$ (2). R が付値環でネーター環ならば，R のイデアルは有限生成なので，前定理より単項イデアルである．

(2) $\Longrightarrow$ (1) は，前定理からすぐわかる．

(1), (2) $\Longrightarrow$ (3). $\mathfrak{m}$ が単項イデアルなのは (2) からわかる．また，R は PID なので $\operatorname{Krull\,dim} R = 1$ である．

(3) $\Longrightarrow$ (2). $\mathfrak{m} = R\pi$ とする．I は (0) でもない R でもない R のイデアルとする．I の準素イデアル分解を考えると，ある $n \in \mathbb{N}$ により，$I = \mathfrak{m}^n$ となる． □

定義 2.5. R は離散付値環，$K = Q(R)$ はその分数体とする．$\mathfrak{m}$ を R の唯一の極大イデアルとし，$\mathfrak{m} = R\pi$ となる素元 $\pi \in \mathbb{R}$ を取る．$\bigcap_{n=0}^{\infty} \mathfrak{m}^n = \{0\}$ だから，$0 \neq x \in R$ に対し $x \in R \cdot \pi^n$, $x \in R \cdot \pi^{n+1}$ を満たす $n \in \mathbb{N} \cup \{0\}$ が存在する．そこで，$\operatorname{ord} x = n$ と定義する．ただし，$\operatorname{ord} 0 = +\infty$ と約束する．

$x \in K$ のときは，$x = y/z$ $(y, z \in R)$ と書けるので，$\operatorname{ord} x = \operatorname{ord} y - \operatorname{ord} z \in \mathbb{Z} \cup \{+\infty\}$ と定義する．これは x の分数表示に依存せずに矛盾なく定義できる．ord は ord_π とか $\operatorname{ord}_{\mathfrak{m}}$ とも書く．そして，c を $c > 1$ である実数とし，$v(x) = c^{-\operatorname{ord} x}$ と定めると，v は K 上の非アルキメデス的付値になる．R は (K, v) の付値環，m は (K, v) の付値イデアルである．$\operatorname{ord} : K \longrightarrow \mathbb{Z} \cup \{\infty\}$ を**加法的付値**ともいう．v や ord は**離散的**であるといい，K は**離散付値体**であるという．離散的付値を持つ場合は，v より ord を用いて議論するほうが簡明な場合が多い．

定理 2.6. v は $\mathbb{Q}$ 上の自明でない乗法的付値とする．
(1) v がアルキメデス的ならば，v は絶対値と同値である．
(2) v が非アルキメデス的ならば，ある素数 p が存在して v は p-進付値と同値である．

証明. (1) n を 2 以上の自然数とし，しばらく固定する．$a := \max\{1, v(n)\}$ とおく．勝手な $m \in \mathbb{N}$ を取り，n 進展開して，$m = \sum_{i=0}^{k} c_i n^i$ $(c_i \in \{0, 1, \ldots, n-1\})$ とする．三角不等式より，$v(c_i) \leqq c_i v(1) \leqq n-1$ である．$l(m) := \lfloor \log_n m \rfloor = k$ とおくと，再び三角不等式より，

$$v(m) \leqq \sum_{i=0}^{k} v(c_i) c(n)^i \leqq \sum_{i=0}^{k} v(c_i) a^i \leqq \sum_{i=0}^{k} (n-1) a^i \leqq \big(l(m)+1\big)(n-1)a^{l(m)}$$

となる．m に m^j を代入すると，$l(m^j) \leqq jl(m)$ より，$v(m^j) \leqq \big(l(m^j)+1\big)(n-1)a^{l(m^j)}$ である．$v(m^j) = v(m)^j$ だから j 乗根を取ると，

$$v(m) \leqq \sqrt[j]{l(m^j)+1}\sqrt[j]{n-1}\,a^{l(m^j)/j}$$

である．$\lim_{j\to+\infty} l(m^j)/j = \log_n m$ である．

$$1 \leqq \lim_{j\to+\infty} \sqrt[j]{l(m^j)+1} \leqq \lim_{j\to+\infty} \sqrt[j]{jl(m)+1} = 1$$

なので，

$$v(m) \leqq \lim_{j\to+\infty} \sqrt[j]{l(m^j)+1}\sqrt[j]{n-1}\,a^{l(m^j)/j} \leqq a^{\log_n m}$$

が得られる．もし，$v(n) \leqq 1$ ならば $a = \max\{1, v(n)\} = 1$ で，$v(m) \leqq 1$ となる．命題 1.6 より，v は非アルキメデス的となって矛盾する．よって $v(n) > 1$ で $a = v(n)$ である．

したがって，$v(m) \leqq v(n)^{\log_n m}$ であるが，m, n は任意の 2 以上の自然数であるので，$v(n) \leqq v(m)^{\log_m n}$ も成立する．$\log_n m = 1/\log_m n$ なので，$v(n)^{\log_n m} \leqq v(m)$ である．以上から，$v(m) = v(n)^{\log_n m}$ が得られた．

再び n を固定して $c := \log_n v(n)$ とおくと，$\log_n v(m) = c \log_n m$ となる．
任意の正の $x \in \mathbb{Q}$ は，$x = m_1/m_2$ (m_1, m_2 は 2 以上の整数) と書けるので，

$$\log_n v(x) = \log_n v(m_1) - \log_n v(m_2) = c \log_n m_1 - c \log_n m_2 = c \log_n |x|$$

が成り立つ．$x \in \mathbb{Q}$ が負のときは，$v(-x) = v(x)$ より，$\log_n v(x) = c \log_n |x|$ である．よって，v は絶対値と同値である．

(2) R を $(\mathbb{Q}, v)$ の付値環，$\mathfrak{m}$ を付値イデアルとする．n が整数ならば，命題 1.3 より $v(n) \leqq 1$ なので，$\mathbb{Z} \subset R$ である．$\mathfrak{m}$ は R の素イデアルだから $\mathfrak{m} \cap \mathbb{Z}$ は $\mathbb{Z}$ の素イデアルである．よって，$\mathfrak{m} \cap \mathbb{Z} = p\mathbb{Z}$ (p は素数または 0) と書ける．もし $p = 0$ だと，任意の $0 \neq x \in \mathbb{Q}$ に対し $v(x) = 1$ となり，v は自明になってしまう．よって，p は素数である．$a := 1/v(p) \in \mathbb{R}$ とおく．$a > 1$ である．$0 \neq x \in \mathbb{Q}$ は，$x = p^n \dfrac{y}{z}$ (n, y, $z \in \mathbb{Z}$ で y, z は p と互いに素) と書ける．y, $z \in R - \mathfrak{m}$ なので $v(y) = v(z) = 1$ である．よって，$v(x) = v(p)^n \dfrac{v(y)}{v(z)} = a^{-n}$ となる．つまり，v は p-進付値と同値である． □

系 2.7. v は体 K 上の自明でない乗法的付値とする．1_K は K の単位元とする．もし，ある 2 以上の自然数 n に対して $v(n \cdot 1_K) \leqq 1$ ならば，v は非アルキメデス的である．

証明. K が正標数ならば K 上の付値は非アルキメデス的なので，K の標数が 0 の場合に証明するばよい．すると，$\mathbb{Q} \subset K$ である．もし $v|_{\mathbb{Q}}$ が $\mathbb{Q}$ 上のアルキメデス的付値ならば，2 以上の自然数 n に対して $v(n \cdot 1_K) > 1$ である．よって，$v|_{\mathbb{Q}}$ は $\mathbb{Q}$ 上の非アルキメデス的付値である．すると，任意の $n \in \mathbb{N}$ に対して $v(n \cdot 1_K) \leqq 1$ となる．命題 1.6 より，v は K 上の非アルキメデス的付値である． □

非アルキメデス的な付値体 (K, v) で，付値環 R がネーター環とは限らない場合の一般論を少し補足しておく．

定理 2.8. (K, v) は非アルキメデス的な付値体とし，R をその付値環，$\mathfrak{m}$ を R の極大イデアルとする．
(1) $\operatorname{Krull\,dim} R = 1$ である．
(2) $R \subsetneqq S \subsetneqq K$ を満たす環 S は存在しない．
(3) R は整閉整域である．
(4) I, J が R のイデアルならば $I \subset J$ または $J \subset I$ である．

証明. (1) $\mathfrak{p} \neq (0)$ を R の素イデアルとする．$\mathfrak{p} \neq \mathfrak{m}$ と仮定する．$\exists x \in \mathfrak{m} - \mathfrak{p}$ を取る．$\mathfrak{p}$ は素イデアルだから，任意の $n \in \mathbb{N}$ に対して $x^n \notin \mathfrak{p}$ である．$0 \neq y \in \mathfrak{p}$ を取る．$v(x) < 1$ だから，十分大きな $n \in \mathbb{N}$ を取ると $v(x^n) < v(y)$ となる．$v(x^n/y) < 1$ なので，$x^n/y \in \mathfrak{m} \subset R$ である．すると，$x^n \in yR \subset \mathfrak{p}$ となり，矛盾する．よって，$\mathfrak{p} \neq \mathfrak{m}$ で，$\operatorname{Krull\,dim} R = 1$ である．

(2) $R \subsetneqq S \subsetneqq K$ を満たす環 S が存在したと仮定する．R は「$x \in K$ ならば $x \in R$ または $1/x \in R$」満たから，S も「$x \in K$ ならば $x \in S$ または $1/x \in S$」を満たす．つまり，S も付値環である．よって，S はただ 1 つの極大イデアル $\mathfrak{n}$ を持つ．$\mathfrak{n} \cap R$ は R の素イデアルである．$\mathfrak{n} \cap R \neq (0)$ なので，(1) より，$\mathfrak{n} \cap R = \mathfrak{m}$ である．もし，$\exists y \in S - R$ とすると，$1/y \in R$ である．$1/y$ は R で可逆でないから $1/y \in \mathfrak{m} \subset \mathfrak{n}$ である．$y \in S$ だから，$1 = y(1/y) \subset \mathfrak{n}$ となり矛盾する．よって $R = S$ である．

(3) R の K における整閉包を R' とする．(2) より $R = R'$ なので，R は整閉整域である．

(4) $I \not\subset J$ と仮定する．$\exists x \in I - J$ を取る．勝手な $y \in J$ を取るとき，$yR \subset J$ だから $x \notin yR$ である．R は付値環だから $y \in xR \subset I$ である．よって，$J \subset I$ である． □

3. 付値体の完備化

完備化にはコーシー列を用いる方法と射影的極限を用いる方法がある．本省ではまず前者を説明する．

定義 3.1.(付値体の完備化) (K, v) は付値体とする．x, $y \in K$ に対し，$d(x, y) = v(x - y)$ で距離 $d\colon K^2 \to \mathbb{R}$ を定めると，d は距離の公理を満たし，(K, d) は距離空間になる．この距離 d によって K 上に位相を定める．また，$f_+(x, y) = x + y$ で定まる写像 $f_+\colon K^2 \to K$ と，$f_\times(x, y) = xy$ で定まる写像 $f_\times\colon K^2 \to K$ は連続写像である．つまり，K は位相体の構造を持つ．

K の元の列 $\{x_n\} = \{x_n\}_{n=1}^{\infty}$ が K 上の**コーシー列**であるとは，任意の正の実数 $\varepsilon > 0$ に対し，ある $n_0 \in \mathbb{N}$ が存在して，$k, l \in \mathbb{N}$, $k \geqq n_0$, $l \geqq n_0$ ならば $d(x_k, x_l) = v(x_k - x_l) < \varepsilon$ を満たすことをいう．$\mathfrak{C}$ を K 上のコーシー列全体の集合とする．$\{x_n\}, \{y_n\} \in \mathfrak{C}$ に対し，同値関係 $\{x_n\} \sim \{y_n\}$ を，任意の正の実数 $\varepsilon > 0$ に対し，ある $n_1 \in \mathbb{N}$ が存在して，$n \in \mathbb{N}$, $n \geqq n_1$ ならば $d(x_n, y_n) = v(x_n - y_n) < \varepsilon$ を満たすこととして定義する．

$\widehat{K} := \mathfrak{C}/\sim$ と定義し，$\{x_n\} \in \mathfrak{C}$ の同値関係 $\sim$ による同値類を $\lim_{n\to+\infty} x_n \in \widehat{K}$ と書き，$\{x_n\}$ の**極限**という．$x \in K$ に対して任意の $n \in \mathbb{N}$ に対し $x_n = x$ として定めた $\{x_n\}$ を**定数列**という．この定数列 $\{x_n\}$ はコーシー列である．$x \in K$ に対し，このような定数列 $\{x_n\}$ の極限 $\lim_{n\to+\infty} x_n \in \widehat{K}$ を対応させる写像を $\iota\colon K \longrightarrow \widehat{K}$ とする．この ι を**自然な単射**という．

体 K 上に2つの同値な乗法的付値 v, w があるとし，2つの距離 $d_v(x,y) = v(x-y), d_w(x,y) = w(x-y)$ を考える．$d_w(x, y) = \big(d_v(x, y)\big)^c$ なので，$\{x_n\}$ が d_v に関してコーシー列であることと，$\{x_n\}$ が d_w に関してコーシー列であることは同値である．よって，v を利用して作った完備化 $\widehat{K}$ と，w を利用して作った完備化 $\widehat{K}$ は一致する．

定理 3.2. (K, v) は付値体とし，$\widehat{K}$, $\iota\colon K \to \widehat{K}$ は上の定義の通りとする．

(1) $x, y \in \widehat{K}$ を取る．$\lim_{n\to+\infty} x_n = x$, $\lim_{n\to+\infty} y_n = y$ となるような $\{x_n\}, \{y_n\} \in \mathfrak{C}$ を取る．すると，$\{x_n + y_n\}, \{x_n y_n\}$ もコーシー列で，$\lim_{n\to+\infty}(x_n + y_n)$ と $\lim_{n\to+\infty} x_n y_n$ は $\lim_{n\to+\infty} x_n = x$, $\lim_{n\to+\infty} y_n = y$ を満たす $\{x_n\}, \{y_n\} \in \mathfrak{C}$ の選び方に依存せずに一意的に定まる．そこで，$x + y := \lim_{n\to+\infty}(x_n + y_n)$, $xy := \lim_{n\to+\infty} x_n y_n$ として $\widehat{K}$ 上に和と積を定める．すると，$\widehat{K}$ は体になる．

(2) $\iota\colon K \to \widehat{K}$ は単射で，体としての中への同型写像である．

(3) $x \in \widehat{K}$ に対し，$\lim_{n\to+\infty} x_n = x$ となるような $\{x_n\} \in \mathfrak{C}$ を取る．このとき，$\lim_{n\to\infty} v(x_n)$ は $\mathbb{R}$ 内の数列として収束し，この極限値は $\lim_{n\to+\infty} x_n = x$ となるような $\{x_n\}$ の選び方に依存しない．そこで，$\widehat{v}(x) := \lim_{n\to+\infty} v(x_n)$ と定義すると $\widehat{v}$ は $\widehat{K}$ 上の乗法的付値になり，$(K, \widehat{v})$ は付値体になる．また，$x \in K$ の場合，$\widehat{v}(\iota(x)) = v(x)$ が成り立つ．

(4) 位相空間として $\iota(K)$ は $\widehat{K}$ 内で調密である．

この付値体 $(\widehat{K}, \widehat{v})$ を付値体 (K, v) の**完備化**という．もし，$\iota\colon K \to \widehat{K}$ が全射ならば，(V, v) は**完備**であるという．K と $\iota(K)$ は同型であるので，通常 K と $\iota(K)$ を同一視して $K \subset \widehat{K}$ と考える．このとき，$v = \widehat{v}|_K$ である．

(5) $(\widehat{K}, \widehat{v})$ は完備である．

(6) (L, w) は完備な付値体で，L は K の拡大体，$w|_K = v$ であって，L 内で K は調密であるとする．すると，同型写像 $\psi\colon L \to \widehat{K}$ が存在し，$\psi|_K = \iota$ かつ，任意の $x \in L$ に対し $w(x) = \widehat{v}(\psi(x))$ を満たす．

証明. (0) まず，$\lim_{n\to+\infty} v(x_n) = 0$ ならば $\lim_{n\to+\infty} x_n = 0$ であることを証明する．$y_n = 0$ $(\forall n \in \mathbb{N})$ で定まる定数列 $\{y_n\}$ を考える．$0 := \lim_{n\to+\infty} y_n$ としして $\widehat{K}$ の 0 が定義される．$\lim_{n\to+\infty} v(x_n - y_n) = 0$ だから $\{x_n\} \sim \{y_n\}$ である．よって，$\widehat{K}$ の定義から $\lim_{n\to+\infty} x_n = 0$ である．

(3-i) $\widehat{v}(x)$ が $\lim_{n\to+\infty} x_n = x$ を満たす $\{x_n\}$ の選び方に依存せずに矛盾なく定義できることは，同値の定義から明らかである．

(1-i) $\lim_{n\to+\infty} x_n y_n$ が $\lim_{n\to+\infty} x_n = x$, $\lim_{n\to+\infty} y_n = y$ を満たす $\{x_n\}, \{y_n\} \in \mathfrak{C}$ の選び方に依存せずに一意的に定まることを示す．

$\lim_{n\to+\infty} x'_n = x$, $\lim_{n\to+\infty} y'_n = y$ と仮定する．$M := 2\max\{\widehat{v}(x), \widehat{v}(y)\} + 1 > 0$ とおけば，ある $n_1 \in \mathbb{N}$ が存在して，$n \geqq n_1$ のとき $v(x_n) < M$, $v(y_n) < M$ である．任意の正の実数 $\varepsilon > 0$ を取る．ある $n_2 \in \mathbb{N}$ が存在して，$n \geqq n_2$ のとき $v(x_n - x'_n) < \varepsilon/(2M)$, $v(y_n - y'_n) \leqq \varepsilon/(2M)$ が成り立つ．$n \geqq \max\{n_1, n_2\}$ のとき，

$$v(x_n y_n - x'_n y'_n) = v\big(x_n(y_n - y'_n) + y'_n(x_n - x'_n)\big)$$

$$\leqq v(x_n)v(y_n - y'_n) + v(y'_n)v(x_n - x'_n) \leqq M\varepsilon/(2M) + M\varepsilon/(2M) = \varepsilon$$

となるので，$\lim_{n\to\infty} v(x_n y_n - x'_n y'_n) = 0$ である．よって，$\lim_{n\to\infty}(x_n y_n - x'_n y'_n) = 0$ である．

$\lim_{n\to+\infty}(x_n + y_n)$ のほうはもっと簡単である．

(1-ii) $\widehat{K}$ が体になることを示す．結合法則，交換法則，分配法則は K での性質の極限として証明できる．また K の定数列 $\{0\}, \{1\}$ の極限が $\widehat{K}$ の $0, 1$ である．$-x$ の存在の証明も簡単である．$0 \neq x \in \widehat{K}$ のとき $\exists 1/x \in \widehat{K}$ を証明する．

$\lim_{n\to+\infty} x_n = x$ とする．$x \neq 0$ だから $0 \neq \widehat{v}(x) =: a \in \mathbb{R}$ である．よって，ある $n_0 \in \mathbb{N}$ が存在して，$n \geqq n_0$ ならば $a/2 < v(x_n) < 2a$ となる．よって，$1/2a < v(1/x_n) < 2/a$ となる．さらに，$k \leqq n_0$, $l \leqq n_0$ ならば $v(x_k - x_l) < \varepsilon$ であると仮定してよい．

$$v\left(\frac{1}{x_k} - \frac{1}{x_l}\right) = v\left(\frac{x_l - x_k}{x_k x_l}\right) \leqq \frac{\varepsilon}{v(x_k)v(x_l)} \leqq \frac{4\varepsilon}{a^2}$$

なので，$\{1/x_n\}$ がコーシー列であることがわかる．よって，極限 $\lim_{n\to+\infty} 1/x_n$ が存在して，これが $1/x$ を与える．

(2) は (0) からわかる．

(3) まだ証明してないのは，$\widehat{v}$ が $\widehat{K}$ 上の乗法的付値であることと，$x \in K$ ならば $\widehat{v}(\iota(x)) = v(x)$ が成り立つことであるが，前者は v の性質の極限をしてすぐわかる．後者は $\widehat{v}$ と ι の定義からはすぐわかる．

(4) $x = \lim_{n\to+\infty} x_n \in \widehat{K}$ の任意の ε-近傍 $U_\varepsilon(x)$ が K の元を含むことを証明すればよいが，極限の定義から，ある $n_0 \in \mathbb{N}$ が存在して，$x_n \geqq n_1$ ならば $x_n \in U_\varepsilon(x)$ である．

(5) (L, w) を $(\widehat{K}, \widehat{v})$ の完備化とし，$\bar{\iota}\colon \widehat{K} \to L$ を自然な単射とする．$x \in L$ は $\widehat{K}$ 内のコーシー列 $\{x_n\}$ の極限として表せる．各 x_n に対し K 内のコーシー列 $\{y_{n,m}\}_{m=1}^{\infty}$ で，$x_n = \lim_{m\to+\infty} y_{n,m}$ となるのが存在する．容易にわかるように，x は $\widehat{K}$ 内のコーシー列 $\{\iota y_{n,n}\}_{n=1}^{\infty}$ の極限になる．K 内のコーシー列 $\{y_{n,n}\}_{n=1}^{\infty}$ の極限を $y \in \widehat{K}$ とおけば，$\bar{\iota}(y) = x$ である．よって，$\bar{\iota}$ は全射で $(\widehat{K}, \widehat{v})$ は完備である．

(6) 勝手な $x \in L$ を取る．K は L 内で調密だから，$\lim_{n\to+\infty} x_n = x$ となる K 内のコーシー列 $\{x_n\}$ が存在する．$x \in L$ に対し $\widehat{K}$ 内での $\{x_n\}$ の極限を対応させる写像を $\psi\colon L \to \widehat{K}$ とする．これが付値体としての同型写像になることは，容易にわかる． □

例 3.3. (1) $\mathbb{Q}$ 上で $v(x) = |x|$ $(x \in \mathbb{Q})$ として $(\mathbb{Q}, v)$ を付値体と考える．すると $\widehat{\mathbb{Q}} = \mathbb{R}$ で，$\widehat{v}$ は $\mathbb{R}$ 上の絶対値である．

(2) $K = \mathbb{Q}(\sqrt{-1})$ 上で $v(x) = |x|$ $(x \in K)$ として (K, v) を付値体と考える．すると $\widehat{K} = \mathbb{C}$ で，$\widehat{v}$ は $\mathbb{C}$ 上の絶対値である．

(3) $K = \mathbb{Q}(\sqrt{2})$ 上に $v(x + \sqrt{2}y) = \left|x - \sqrt{2}y\right|$ として v を定めると (K, v) は付値体になる．$\widehat{K} = \mathbb{R}$ で，v の完備化は $\widehat{v}(x) := |x|$ $(x \in \mathbb{R})$ で定まる．たたし，$\iota\colon K \to \widehat{K}$ は $\iota(x + \sqrt{2}y) = x - \sqrt{2}y$ で定まる写像である．

定義&命題 3.4. (K, v) と (L, w) は付値体とし，体としての中への同型写像 $\varphi\colon K \to L$ が存在し，任意の $x \in K$ に対し $v(x) = w(\varphi(x))$ が成り立つとする．このとき，$\varphi\colon K \to L$ は**付値体としての中への同型**写像であるという．特に，φ が包含写像でそれが付値体としての中での同型写像になっているとき，(L, w) は付値体として (K, v) の**拡大体**であるといい，(K, v) は付値体として (L, w) の**部分体**であるという．

$\varphi\colon K \to L$ は付値体としての中への同型写像で，$(\widehat{K}, \widehat{v})$ と $(\widehat{L}, \widehat{w})$ はそれぞれ (K, v) と (L, w) の完備化とする．すると，付値体としての中への同型写像 $\widehat{\varphi}\colon \widehat{K} \to \widehat{L}$ で $\widehat{\varphi}|_K = \varphi$ を満たすものが一意的に存在する．

証明. $\widehat{\varphi}\left(\lim_{n\to\infty} x_n\right) := \lim_{n\to\infty} \varphi(x_n)$ によって $\widehat{\varphi}\colon \widehat{K} \to \widehat{L}$ を定める．$\widehat{\varphi}$ が中への同型写像であることは，極限の性質から容易にわかる．

$\psi\colon \widehat{K} \to \widehat{L}$ も付値体としての中への同型写像で $\psi|_K = \varphi$ を満たすとすると，$\psi = \widehat{\varphi}$ であることを証明する．$x = \lim_{n\to\infty} x_n \in \widehat{K}$ を勝手にとる．ここで $\{x_n\}$ は K 内のコーシー列である．$x_n \in K$ だから $\psi(x_n) = \varphi(x_n)$ が成り立つ．よって，

$$\psi(x) = \psi\left(\lim_{n\to\infty} x_n\right) = \lim_{n\to\infty} \psi(x_n) = \lim_{n\to\infty} \varphi(x_n) = \widehat{\varphi}\left(\lim_{n\to\infty} x_n\right) = \widehat{\varphi}(x)$$

である． □

定義 3.5. $\mathbb{R}_+ := \left\{x \in \mathbb{R} \;\middle|\; x > 0\right\}$ とおく．$\mathbb{R}_+$ は乗法についてアーベル群である．(K, v) は付値体とする．$v(K - \{0\}) \subset \mathbb{R}_+$ は乗法に対してアーベル群をなす．$v(K - \{0\})$ を v の**値群**という．

定理 3.6. (K, v) は付値体，$(\widehat{K}, \widehat{v})$ はその完備化とする．
(1) v がアルキメデス的ならば $\widehat{v}(\widehat{K}) = \mathbb{R}_+$ である．
(2) v が非アルキメデス的ならば $\widehat{v}(\widehat{K}) = v(K)$ である．また $x = \lim_{n\to\infty} x_n \in \widehat{K}$ $(x_k \in K)$ ならば，ある $n_0 \in \mathbb{N}$ が存在して $n \geqq n_0$ ならば $v(x_n) = \widehat{v}(x)$ となる．

証明. (1) v がアルキメデス的ならば，中への同型写像 $\varphi\colon \mathbb{Q} \to K$ が存在する．これより，$\widehat{\varphi}\colon \mathbb{R} \to \widehat{K}$ が誘導される．$(\mathbb{R}, |\ \ |)$ の値群は $\mathbb{R}_+$ なので，$\widehat{v}(\widehat{K}) = \mathbb{R}_+$ である．

(2) 後半を示せばよい．$a := \widehat{v}(x) \in \mathbb{R}_+, a_n := v(x_n) \in \mathbb{R}_+$ とおくと，$a = \lim_{n\to\infty} a_n$ である．$0 < \varepsilon < a/2$ を満たす $\varepsilon \in \mathbb{R}$ を取る．ある $n_0 \in \mathbb{N}$ が存在して，$k, l \in \mathbb{N}, k \geqq n_0, l \geqq n_0$ ならば $v(x_k - x_l) < \varepsilon$ かつ $|a_l - a| < \varepsilon$ を満たす．$a_l > \varepsilon$ だから，$v(x_k - x_l) < \varepsilon < a_l = v(x_l)$ である．よって，

$$a_k = v(x_k) = v\big((x_k - x_l) + x_l\big) \leqq \max\left\{v(x_k - x_l), v(x_l)\right\} = v(x_l) = a_l$$

である．対称性から $a_k \leqq a_k$ なので $a_k = a_l$ となる．よって，$k \geqq n_0$ ならば $a_k = a$ である． □

4. アルキメデス的付値

アルキメデス的付値に関する以下の基本的な定理を証明しておく．

定理 4.1. v は体 K 上の自明でないアルキメデス的付値とする．すると，ある中への同型写像 $\varphi\colon K \to \mathbb{C}$ と，ある正の実数 c が存在して，任意の $x \in K$ に対して，$v(x)^c = \left|\varphi(x)\right|$ が成り立つ．
特に (K, v) が完備ならば，$\varphi(K) = \mathbb{R}$ または $\varphi(K) = \mathbb{C}$ である．

証明. K がアルキメデス的付値を持つので $\mathbb{Q} \subset K$ である．$v|_{\mathbb{Q}}$ は $\mathbb{Q}$ 上のアルキメデス的付値なので，ある正の実数 c が存在して，任意の $x \in \mathbb{Q}$ に対して，$v(x)^c = |x|$ が成り立つ．そこで，K 上の付値 $v(y)$ $(y \in K)$ の代わりに，それと同値な付値 $v'(y) := v(y)^{1/c}$ を考えることにより，任意の $x \in \mathbb{Q}$ に対し $v(x) = |x|$ であると仮定してよい．

(K, v) の完備化を $(\widehat{K}, \widehat{v})$ とするとき，包含写像 $\iota\colon \mathbb{Q} \to K$ の中への体同型としての拡張 $\widehat{\iota}\colon \mathbb{R} \to \widehat{K}$ で，任意の $x \in \mathbb{R}$ に対し $\widehat{v}(\varphi(x)) = |x|$ を満たすものが存在する．そこで，最初から (K, v) が完備で $\mathbb{R} \subset K$ であり，$x \in \mathbb{R} \subset K$ ならば $v(x) = |x|$ であると仮定してよい．

(1) $\sqrt{-1} \in K$ ならば $K = \mathbb{C}$ であることを証明する．

$\mathbb{R} \subset K$ で $\sqrt{-1} \in K$ だから，$\mathbb{C} \subset K$ であり，$x \in \mathbb{C}$ ならば $v(x) = |x|$ である．背理法で，$\exists k \in K - \mathbb{C}$ と仮定して矛盾を導く．

$z \in \mathbb{C}$ に対し $f(z) = v(z - k)$ とおくと，$f\colon \mathbb{C} \to \mathbb{R}$ は連続関数である．$v(z - k) \geqq v(z) - v(k)$ だから，$|z| \to +\infty$ のとき $v(z - k) \to +\infty$ である．さらに，$v(z - k) \geqq 0$ だから，f は $\mathbb{C}$ 上で最小値を持つ．$f(z_0) = \delta := \min_{z\in\mathbb{C}} f(z)$ であるとする．

(1-i) $x, y \in \mathbb{C}$, $f(x) = \delta$, $|y| < \delta$ ならば $f(x + y) = \delta$ が成り立つことを証明する．

$a := x - k \in K$ とおく．$v(a) = v(x - k) = f(x) = \delta$ である．勝手な $n \in \mathbb{N}$ を取る．ζ を 1 の原始 n 乗根として，

$$\begin{aligned} v(a^n - y^n) &= v\left(\prod_{m=0}^{n-1} (a - \zeta^m y)\right) = \prod_{m=0}^{n-1} v(a - \zeta^m y) \\ &\geqq v(a - y)\delta^{n-1} = v(a - y)v(a)^{n-1} = v(a - y)v(a^{n-1}) \end{aligned}$$

である．これより，$v\left(a-\dfrac{y^n}{a^{n-1}}\right)\geqq v(a-y)$ である．三角不等式から，

$$v(a)+v\left(\frac{y^n}{a^{n-1}}\right)\geqq v(a-y)=v(x-k-y)=f(x-y)$$

となる．つまり，$\delta+\dfrac{v(y)^n}{\delta^{n-1}}\geqq f(x-y)$ である．$0\leqq v(y)=|y|<\delta$ であったから，$\lim\limits_{n\to\infty}\dfrac{v(y)^n}{\delta^{n-1}}=0$ である．これより，$\delta\geqq f(x-y)$ となる．$\delta=\min f(z)$ だから，$f(x-y)=\delta$ である．y の代わりに $-y$ を考えると $f(x+y)=\delta$ が証明された．

(1-ii) $n\in\mathbb{N}$ に関する帰納法で，(1-i) を用いて，$y\in\mathbb{C}$ が $|y|<\delta$ を満たせば，任意の $n\in\mathbb{N}$ に対し $f(x+ny)=\delta$ が成り立つことがわかる．

$|z|\gg 1$ である $z\in\mathbb{C}$ を取り，次に $N\gg|z|$ である $N\in\mathbb{N}$ を取り，$|z/N|<\delta$ となるようにしておく．$y=z/N$ とおくと，任意の $n\in\mathbb{N}$ に対して，$f(x+nz/N)=\delta$ である．$n=N$ とすれば $v(z+x-k)=f(x+z)=\delta$ である．これは $|z|\to\infty$ のとき $v(z+x-k)\to\infty$ であることと矛盾する．よって，$K=\mathbb{C}$ である．

(2) $\sqrt{-1}\notin K$ ならば K の付値 v の $K(\sqrt{-1})$ への拡張は一意的であり，その拡張を v' とすると $K(\sqrt{-1})$ は v' について完備であることを証明する．

これが証明されれば，(1) より $K(\sqrt{-1})=\mathbb{C}$ となるから，$K=\mathbb{R}$ が証明される．

$K(\sqrt{-1})$ の元 z は $z=x+\sqrt{-1}y$ $(x,\,y\in K)$ と書ける．$\overline{z}=x-\sqrt{-1}y$, $N(z)=z\overline{z}=x^2+y^2$ と書くことにする．

(2-i) v' が v の $K(\sqrt{-1})$ への勝手な拡張のとき，$v'(z)=v'(\overline{z})$ であることを証明する．

背理法で，$v'(x-\sqrt{-1}y)\neq v'(x+\sqrt{-1}y)$ と仮定して矛盾を導く．$v'(x-\sqrt{-1}y)>v'(x+\sqrt{-1}y)$ と仮定してよい．$w:=\dfrac{x+\sqrt{-1}y}{x-\sqrt{-1}y}\in K(\sqrt{-1})$ とおくと，$v'(w)<1$ で $N(w)=1$ である．$\{w^n\}$ の部分列を考えれば，各 $n\in\mathbb{N}$ に対し，ある $w_n=a_n+\sqrt{-1}b_n\in K(\sqrt{-1})$ で，$N(w_n)=1$ かつ $v'(w_n)<1/2^n$ を満たすものが存在する．必要なら w_n を $\sqrt{-1}w_n$ に取り替えることにより，$v'(a_n)\geqq v'(b_n)$ であると仮定してよい．$1/w_n=a_n-\sqrt{-1}b_n$ なので，

$$2^n<v'(a_n-\sqrt{-1}b_n)\leqq v'(a_n)+v'(b_n)\leqq 2v'(a_n)$$

が成り立つ．

$$v'\left(1+\sqrt{-1}\frac{b_n}{a_n}\right)=v'\left(\frac{w_n}{a_n}\right)=\frac{v'(w_n)}{v'(a_n)}\leqq\frac{1}{2^n}\cdot\frac{1}{2^{n-1}}=\frac{1}{2^{2n-1}}$$

である．点列 $\{b_n/a_n\}$ はコンパクト集合上の点列なので，収束する部分列を含む．その部分列と取り替えることで，極限 $c:=\lim\limits_{n\to\infty}\dfrac{b_n}{a_n}\in K$ が存在すると仮定してよい．すると，

$$0\leqq v'(1+\sqrt{-1}c)=v'\left(\lim_{n\to\infty}\left(1+\sqrt{-1}\frac{b_n}{a_n}\right)\right)=\lim_{n\to\infty}\left(1+\sqrt{-1}\frac{b_n}{a_n}\right)\leqq\lim_{n\to\infty}\frac{1}{2^{n-1}}=0$$

となるので，$v'(1+\sqrt{-1}c)=0$ である．付値の定義から $1+\sqrt{-1}c=0$ となり，$c=\sqrt{-1}$ となる．すると，$\sqrt{-1}=c\in K$ となり矛盾する．よって，$v'(z)=v'(\overline{z})$ である．

(2-ii) v の $K(\sqrt{-1})$ への拡張 v'' が存在することを証明する．つまり，$v''(z)=\sqrt{v(z\overline{z})}$ で定義される v'' が $K(\sqrt{-1})$ 上の付値であることを示す．定義 1.1 の中で (1), (2) は自明なので (3) の三角不等式だけ証明する．

$z=a+\sqrt{-1}b$, $w=c+\sqrt{-1}d$ $(a,\,b,\,c,\,d\in K)$ とし，$v''(z+w)\leqq v''(z)+v''(w)$ を示す．

$$v''(z+w)^2=v\big((a+c)^2+(b+d)^2\big)\leqq v(a^2+b^2)+v(c^2+d^2)+2v(ac+bd)$$

$$\big(v''(z)+v''(w)\big)^2=v(a^2+b^2)+v(c^2+d^2)+2\sqrt{v((a^2+b^2)(c^2+d^2))}$$

なので，$v(ac+bd)^2\leqq v(a^2+b^2)v(c^2+d^2)$ — ① を示せばよい．実変数 $t\in\mathbb{R}$ に対し，

$$f(t):=t^2v(a^2+b^2)+2tv(ac+bd)+v(c^2+d^2)$$

とおく．

$$v''(tz+w)^2=v((ta+c)^2+(tb+d)^2)=v(t^2(a^2+b^2)+2t(ac+bd)+(c^2+d^2))$$
$$\leqq t^2v(a^2+b^2)+2tv(ac+bd)+v(c^2+d^2)=f(t)$$

なので，任意の $t \in \mathbb{R}$ に対して $f(t) \geqq 0$ である．よって，t についての 2 次方式 $f(t) = 0$ の判別式は $\leqq 0$ なので，① を得る．

(2-iii) v の $K(\sqrt{-1})$ への拡張 v' は一意性で，$K(\sqrt{-1})$ は v' に関して完備であることを証明する．

$z \in K$ のとき $v''(z) = v(z)$ を満たすことは v'' の定義からすぐわかる．$K(\sqrt{-1})$ が v'' について完備であることは，2 つの完備距離空間の直積が完備であることから従う．

v' が v の $K(\sqrt{-1})$ への勝手な拡張のとき，(2-i) より，$v'(z)^2 = v'(z)v'(\overline{z}) = v'(z\overline{z})$ であるので，$v'(z) = \sqrt{v(z\overline{z})} = v''(z)$ である．よって，v' は一意的である．以上で (2) が証明された． □

アルキメデス的な乗法的付値の代数拡大体への延長の存在を証明する．

定理 4.2. (K, v) はアルキメデス的な付値体とし，L は K の代数拡大体とする．このとき以下が成り立つ．
(1) L 上の付値 w で，$w|_K = v$ を満たすものが存在する．
(2) L 上の付値 w' が $w'|_K = v$ を満たすならば，ある $\sigma \in \mathrm{Aut}(L/K)$ が存在して $w' = w \circ \sigma$ となる．

証明. (1) $z \in \mathbb{C}$ に対し $\overline{v}(z) = |z|$ で $\overline{v}$ を定める．v を適当な同値な付値に置き換えて考えれば，$K \subset \mathbb{C}$ で $v = \overline{v}|_K$ と考えてよい．ある中への同型写像 $f\colon L \to \mathbb{C}$ によって，$K \subset f(L) \subset \mathbb{C}$ とできるので，$x \in L$ に対し $w(x) = \overline{v}(f(x))$ で w を定めればよい．

(2) ある中への同型写像 $g\colon L \to \mathbb{C}$ を取れば，$x \in L$ に対し $w'(x) = \overline{v}(g(x))$ が成り立つ．

$f(L) = g(L)$ であることを示す．$f|_K = g|_K$ である．$a \in f(L)$ を取る．$f(L)$ は $f(K) = g(K)$ 上の代数拡大体なので，a の $f(K)$ 上の最小多項式 $\Phi_a(t)$ が存在する．$K = f(K)$ と同一視すれば，$\Phi_a(t)$ は $f^{-1}(a) \in L$ の K 上の最小多項式でもある．$g(L)$ は $g(K) = f(K)$ 上の $\Phi_a(t)$ の分解体だから，$\Phi_a(t) = 0$ の根 a は $g(L)$ に属する．よって，$f(L) \subset g(L)$ である．同様に $g(L) \subset f(L)$ だから $f(L) = g(L)$ である．

$\sigma\colon L \to L$ を $\sigma(x) = f^{-1}(g(x))$ で定めれば，$\sigma \in \mathrm{Aut}(L/K)$ で，

$$w'(x) = \overline{v}(g(x)) = \overline{v}(f(f^{-1}(g(x)))) = \overline{v}(f(\sigma(x))) = w(\sigma(x))$$

$(x \in L)$ が成り立つ． □

注意 4.3. $K := \mathbb{Q}(\sqrt{2})$ とし，$x = a + b\sqrt{2} \in K$ $(a, b \in \mathbb{Q})$ に対し，$v(x) := |x|$, $w(x) := \left|a - b\sqrt{2}\right|$ とおくと，v, w は K 上の乗法的付値で，互いに同値でない．

中への同型写像 $\sigma\colon K \to \mathbb{R}$ を，$\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$ で定めれば，$w(x) = \left|\sigma(x)\right|$ であり，w も $\mathbb{R}$ の絶対値から得られる．ただし，こういう自然でない埋め込み σ を使わないといけない．

5. 環の完備化

今度は可換環の完備化の話を扱う．整数論や代数幾何ではネーターでない可換環は滅多に登場せず，したがって付値環は離散付値環になっているのが普通である．以下，そういう場合を中心に話す．少しネーター環について復習しておく．

定理 5.1.(中山の補題) R は可換環，M は有限生成 R-加群，N は M の部分 R-加群とする．また，R のすべての極大イデアルの共通部分を J とする (J は **Jacobson 根基**とよばれる)．このとき，もし，

$$JM + N = M$$

が成り立つならば，$M = N$ である．

証明. $L = M/N$ とおく．$L \neq 0$ と仮定して矛盾を導く．$JM + N = M$ より，$JL = L$ となる．L も有限生成 R-加群なので，生成元を $x_1, \ldots, x_n \in L$ とする．$JL = L$ より，各 $1 \leqq i \leqq n$ に対し，

$$x_i = \sum_{j=1}^{n} a_{ij} x_j \quad (\exists a_{ij} \in J)$$

と書ける．a_{ij} を第 i 行第 j 列の成分とする n 次正方行列を A とする．また，$x_1, \ldots, x_n$ を縦に並べてできる列ベクトルを $\mathbf{x}$，n 次の単位行列を I_n とすると，$(I_n - A)\mathbf{x} = \mathbf{0}$ (0-ベクトル) なので，$(I_n - A)$

の余因子行列を B とし $a=\det(I_n-A)$ とおけば，$a\mathbf{x}=B(I_n-A)\mathbf{x}=\mathbf{0}$ である．他方，$a_{ij}\in J$ なので，ある $m\in J$ が存在して，$a=\det(I_n-A)=1+m\notin J$ である．もし，a が可逆元でないとすると $(a)\subsetneqq R$ だから，$(a)\subset\mathfrak{m}\subsetneqq R$ を満たす極大イデアルが存在する．$m\in J\subset\mathfrak{m}$ だから $1=a-m\in\mathfrak{m}$. よって，$\mathfrak{m}=R$ となり矛盾する．よって，$a^{-1}\in R$ で，$\mathbf{x}=a^{-1}\mathbf{0}=\mathbf{0}$ となり矛盾する．したがって，$L=0$ で，$M=N$ である． □

系 5.2.(Krull の共通部分定理)

(1) $(R,\mathfrak{m})$ がネーター局所環ならば，$\bigcap_{n=1}^{\infty}\mathfrak{m}^n=(0)$ である．

(2) R がネーター整域で，$I\neq R$ がそのイデアルのとき，$\bigcap_{n=1}^{\infty}I^n=(0)$ である．

証明. (1) $M=\bigcap_{n=1}^{\infty}\mathfrak{m}^n$ とする．$\mathfrak{m}M\supset M$ を示す．$\mathfrak{m}=(a_1,\ldots,a_r)$ と書ける．多項式環 $S=R[X_1,\ldots,X_r]$ を考え，自然な準同型写像 $\varphi\colon S\to R$ を $\varphi(X_i)=a_i$ で定める．

$$S_n=\{f\in S\mid f\text{ は }n\text{ 次斉次多項式}\}\cup\{0\},$$
$$J_n:=\{f\in S_n\mid\varphi(f)\in M\}$$

とし，$\bigcup_{n\in\mathbb{N}}J_n$ で生成される S のイデアルを J とする．$J=(f_1,\ldots,f_s)$ と書ける．J の定義から，各 f_i は斉次元であると仮定してよい．$d_i=\deg f_i$, $n_0=\max\{d_1,\ldots,d_s\}$ とする．$\varphi(S_n)=\mathfrak{m}^n$ に注意する．

勝手な $b\in M$ を取る．$n=n_0+1$ とすると，$b\in\mathfrak{m}^n$ なので，$\varphi(g)=b$ となる $g\in S_n$ が存在する．$g=h_1f_1+\cdots+h_sf_s$ ($h_i\in S$ はある $(n-d_i)$ 次斉次式) と書ける．

$$b=\varphi(g)=\sum_{i=1}^{s}\varphi(h_i)\varphi(f_i)\in\sum_{i=1}^{s}\mathfrak{m}^{n-d_i}M\subset\mathfrak{m}^{n-n_0}M\subset\mathfrak{m}M$$

となる．よって，$\mathfrak{m}M\supset M$ である．$\subset$ は自明なので，$\mathfrak{m}M=M$ である．そこで，$N=0$ として中山の補題を使うと，$M=0$ が得られる．

(2) I を含む極大イデアル $\mathfrak{m}$ を取る．$S=R_{\mathfrak{m}}$, $\mathfrak{n}=\mathfrak{m}R_{\mathfrak{m}}$ とおく．$R\subset S$ とみなしたとき，$I^n\subset\mathfrak{n}^n$ である．(1) より，$\bigcap_{n=1}^{\infty}I^n\subset\bigcap_{n=1}^{\infty}\mathfrak{n}^n=(0)$ である． □

定義 5.3.(可換環のイデアルによる完備化) R は可換環，$I\subsetneqq R$ は R のイデアルとする．$f_n\colon R/I^{n+1}\longrightarrow R/I^n$ $(n\in\mathbb{N})$ を自然な全射とする．$A:=\prod_{n=1}^{\infty}R/I^n$ とし，A の元を $x=(x_n)_{n=1}^{\infty}$ $(x_n\in R/I^n)$ と表すことにする．

$$\varprojlim_n R/I^n:=\{(x_n)_{n=1}^{\infty}\in A\mid\text{任意の }n\in\mathbb{N}\text{ に対して }f_n(x_{n+1})=x_n\}$$

と書く．$\varprojlim_n R/I^n$ は単に $\varprojlim R/I^n$ と書くことも多い．簡単のため，$\widehat{R}:=\varprojlim R/I^n$ とおく．$x=(x_n)_{n=1}^{\infty}\in\widehat{R}$, $y=(y_n)_{n=1}^{\infty}\in\widehat{R}$ のとき，$(x_n+y_n)_{n=1}^{\infty}\in A$, $(x_ny_n)_{n=1}^{\infty}\in A$ も $f_n(x_{n+1}+y_{n+1})=x_n+y_n$, $f_n(x_{n+1}y_{n+1})=x_ny_n$ を満たすから，$\widehat{R}$ に属する．そこで，$x+y:=(x_n+y_n)_{n=1}^{\infty}$, $xy:=(x_ny_n)_{n=1}^{\infty}$ として $\widehat{R}$ に和と積を定める．これによって $\widehat{R}$ が可換環になることは容易にわかる．$\widehat{R}$ を I による R の**完備化**とか I-**進完備化**という．

また，$\pi_n\colon R\to R/I^n$ を自然な全射とするとき，$x\in R$ ならば $(\pi_n(x))_{n=1}^{\infty}\in A$ は $\widehat{R}$ に属する．そこで，$\pi\colon R\to\widehat{R}$ を $\pi(x)=(\pi_n(x))_{n=1}^{\infty}$ によって定義する．

例. R は可換環とする．多項式環 $R[X_1,\ldots,X_n]$ のその極大イデアル $\mathfrak{m}=(X_1,\ldots,X_n)$ による完備化は形式 (的) 巾級数環 $R[[X_1,\ldots,X_n]]$ と同型である．

命題 5.4. R, I, π 等は上の定義の通りとする．もし $\bigcap_{n=1}^{\infty} I^n = (0)$ が成り立つならば，$\pi\colon R \to \widehat{R}$ は単射準同型写像である．

証明. $\pi(x) = 0$ $(x \in R)$ ならば，任意の $n \in \mathbb{N}$ に対して $\pi_n(x) = 0$ だから，$x \in I^n$ であり，$\bigcap_{n=1}^{\infty} I^n = (0)$ より $x = 0$ となる．よって，π は単射である． □

定理 5.5. R はネーター環，$\mathfrak{m}$ は R の極大イデアルとし，$\widehat{R} = \varprojlim_n R/\mathfrak{m}^n$ とおく．今，R は整域であるか，または，局所環であると仮定する．すると，$\widehat{R}$ は $\mathfrak{m}\widehat{R}$ を唯一の極大イデアルとする局所環である．

証明. (1) R が局所環の場合に証明する．$K = R/\mathfrak{m}$, $R_n = R/\mathfrak{m}^n$ と置く．$R_n/\mathfrak{m}R_n \cong R/\mathfrak{m} = K$ なので，$\widehat{R}/\mathfrak{m}\widehat{R} = \varprojlim R_n/\mathfrak{m}R_n = K$ である．よって，$\mathfrak{m}\widehat{R}$ は $\widehat{R}$ の極大イデアルである．

次に，I は $\widehat{R}$ の極大イデアルとする．$J = I \cap R$ とおくと，準同型定理より $R/J \subset \widehat{R}/I$ である．$1 \notin J$ より $R/J \neq 0$ で R/J は整域で，$J \neq R$ は R のイデアルである．よって，$J \subset \mathfrak{m}$ で，$I \subset \mathfrak{m}\widehat{R}$ となる．I は極大だから，$I = \mathfrak{m}\widehat{R}$ となる．

(2) R が整域の場合に証明する．$R \subset R_{\mathfrak{m}}$ ($\mathfrak{m}$ による局所化) である．$R/\mathfrak{m}^n \cong R_{\mathfrak{m}}/(\mathfrak{m}R_{\mathfrak{m}})^n$ より，$\widehat{R} \cong \widehat{R_{\mathfrak{m}}}$ である．(1) より，これは局所環である． □

定理 5.6. $(R, \mathfrak{m})$ がネーター局所環ならば，$\widehat{R} = \varprojlim_n R/\mathfrak{m}^n$ もネーター局所環である．

証明. $\mathfrak{m} = (a_1, \ldots, a_r)$ と書ける．$S = R[X_1, \ldots, X_r]$, $T = R[[X_1, \ldots, X_r]]$, $\mathfrak{a} = (X_1 - a_1, \ldots, X_r - a_r) \subset S$, $\mathfrak{b} = (X_1 - a_1, \ldots, X_r - a_r) \subset T$ とおく．R がネーター環ならば S, T もネーター環であるという定理は既知として証明を進める．$S/\mathfrak{a} \cong R$ である．$\mathfrak{n} = (X_1, \ldots, X_r) \subset S$ とするとき，$S/\mathfrak{n}^n \twoheadrightarrow S/(\mathfrak{n}^n + \mathfrak{a}) \cong R/\mathfrak{m}^n$ だから，自然な全射 $\varphi : \varprojlim_n S/\mathfrak{n}^n \longrightarrow \varprojlim_n R/\mathfrak{m}^n$ が存在する．つまり，全射 $\varphi\colon T \to \widehat{R}$ が存在する．T がネーター環なので，$\widehat{R}$ もネーター環である．なお，$\operatorname{Ker}\varphi = \mathfrak{b}$ である． □

定理 5.7. (K, v) は非アルキメデス的な付値体，$(\widehat{K}, \widehat{v})$ はその完備化とする．また $(R, \mathfrak{m})$ は K の付値環とする．いま，R はネーター環 (よって離散付値環) であると仮定する．$\tilde{R} := \varprojlim R/\mathfrak{m}^n$, $\tilde{\mathfrak{m}} = \mathfrak{m}\tilde{R}$ とおくと，$(\tilde{R}, \tilde{\mathfrak{m}})$ は $(\widehat{K}, \widehat{v})$ の付値環と同型である．

証明. $(\widehat{K}, \widehat{v})$ の付値環を $(\widehat{R}, \widehat{\mathfrak{m}})$ とする．R はネーター環なので $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = (0)$ である．v を同値な非アルキメデス的付値でおきかえて，$\log_2 v(x) = -\operatorname{ord}_{\mathfrak{m}} x$ $(x \in K)$, $\log_2 \widehat{v}(x) = -\operatorname{ord}_{\widehat{\mathfrak{m}}} x$ $(x \in \widehat{K})$ であると仮定してよい．$\pi_n\colon R \longrightarrow R/\mathfrak{m}^n$ と $\tilde{\pi}_n\colon \tilde{R} \longrightarrow \tilde{R}/\tilde{\mathfrak{m}}^n = R/\mathfrak{m}^n$ を自然な全射とする．

$x = (x_n)_{n=1}^{\infty} \in \tilde{R}$ を取る．$x_n \in \tilde{R}/\tilde{\mathfrak{m}}^n \cong R/\mathfrak{m}^n$ なので，$y_n \in R$ を $\pi_n(y_n) = x_n$ となるように選べる．$\{y_n\}$ がコーシー列であることを証明する．勝手な正の実数 ε を取る．$n_0 \in \mathbb{N}$ を $1/2^{n_0} < \varepsilon$ となるように取る．$k \geqq n_0$, $l \geqq n_0$ のとき $y_k - y_l \in \mathfrak{m}^{n_0}$ だから，$\operatorname{ord}_{\mathfrak{m}}(y_k - y_l) \geqq n_0$ である．よって $v(y_k - y_l) \leqq 1/2^{n_0} < \varepsilon$ である．したがって $\{y_n\}$ はコーシー列である．ある $n_1 \in \mathbb{N}$ が存在して $\widehat{v}(x) = v(x_{n_1}) \leqq 1$ だから，$\varphi(x) \in \widehat{R}$ である．そこで，$\varphi(x) = \lim_{n\to\infty} y_n \in \widehat{R}$ によって写像 $\varphi\colon \tilde{R} \to \widehat{R}$ を定める．$z_n \in R$ を $\pi_n(z_n) = x_n$ となるように選んだとき，$\lim_{n\to\infty} y_n = \lim_{n\to\infty} z_n$ が成り立つことは，$y_n - z_n \in \mathfrak{m}^n$ であることからわかる．よって，φ は列 $\{y_n\}$ の選び方に依存せずに矛盾なく定義されている．

$\varphi(x) = 0$ ならば $x \in \bigcap \widehat{\mathfrak{m}}^n = (0)$ なので $x = 0$ であり，φ は単射準同型写像である．

$\varphi\colon \tilde{R} \to \widehat{R}$ が全射であることを示す．勝手な $y = \lim_{n\to\infty} y_n \in \widehat{R}$ を取る．必要なら $\{y_n\}$ をその部分列に置き換えることにより，$\operatorname{ord}_{\widehat{\mathfrak{m}}}(y_n - y) \geqq n$ が任意の $n \in \mathbb{N}$ について成り立つと仮定できる．

$\widehat{\pi}_n\colon \widehat{R} \longrightarrow \widehat{R}/\widehat{\mathfrak{m}}^n = R/\mathfrak{m}^n$ を自然な全射とする．$x_n \in R$ を $\pi_n(x_n) = \widehat{\pi}_n(y_n) \in \widehat{R}/\widehat{\mathfrak{m}}^n$ を満たすように選べる．$x = (x_n)_{n=1}^{\infty} \in \tilde{R}$ とおけば $\varphi(x) = y$ となるので，φ は全射である． □

例 5.8. p を素数とし，$\mathbb{Q}$ 上で $v_p(x) = p^{-\operatorname{ord}_p x}$ $(x \in \mathbb{Q})$ で定まる非アルキメデス付値に関する完備化を $\mathbb{Q}_p$ と書き p **進数体**という．その付値環を

$$\mathbb{Z}_p := \left\{ x \in \mathbb{Q}_p \;\middle|\; v_p(x) \leqq 1 \right\}$$

と書き，p **進整数環**という．上の定理より，

$$\mathbb{Z}_p \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

が成り立つ．

$\mathbb{Q}_p$ の元を具体的に表示する方法を考える．$x = a/b \in \mathbb{Q}_p$ $(a,\, b \in \mathbb{Z}_p)$ を取る．$\operatorname{ord}_p b = n$ のとき，$b \in p^n\mathbb{Z}_p$ だから $b = p^n b_1$，$\operatorname{ord}_p b_1 = 0$ と書ける．このとき b_1 は $\mathbb{Z}_p$ の可逆元であるので，$a_1 = b_1^{-1}a$ とおけば，$x = a_1/p^n$ $(a_1 \in \mathbb{Z}_p)$ と書ける．$\pi_k\colon \mathbb{Z}_p \longrightarrow \mathbb{Z}_p/p^k\mathbb{Z}_p \cong \mathbb{Z}/p^k\mathbb{Z}$ を自然な全射とするとき，$\pi_k(a_1) = \sum_{i=0}^{k-1} c_i^{(k)} p^i$ $(c_i^{(k)} \in \{0,\, 1,\, 2,\ldots,\, p-1\})$ と一意的に表わされる．ここで，$k > i$ かつ $l > i$ ならば $c_i^{(k)} = c_i^{(l)}$ が成り立つ．そこで，$k > i$ となる k を 1 つ選んで $c_i = c_i^{(k)}$ とおく．すると，$a_1 = \sum_{i=0}^{\infty} c_i p^i$ $c_i \in \{0,\, 1,\ldots,\, p-1\}$ と一意的に表すことができる．また，$x = \sum_{i=-n}^{\infty} c_{i+n} p^i$ と表すことができる．

6. 環の整拡大

定義 6.1. R は整域，$K = Q(R)$ は R の分数体, L は K を含む体とする．$z \in L$ に対し，ある自然数 n と $a_0,\, a_1,\ldots,\, a_{n-1} \in R$ が存在して

$$z^n + a_{n-1}z^{n-1} + a_{n-2}z^{n-2} + \cdots + a_2z^2 + a_1z + a_0 = 0 \qquad ①$$

を満たすとき，z は R 上**整** (integral) であると言う．$z \in R$ ならば z は R 上整である $(n = 1,\, a_0 = -z \in R$ とすればよい)．特に，R が体のとき，R 上整な元を R 上**代数的** (algebraic) と言い，R 上代数的でない元を R 上**超越的** (transcendental) と言う．R 上整な元 z に対し，① を満たす R 上のモニック多項式のうち，2 つの 1 次以上の R 上のモニック多項式の積に表せない多項式を x の R 上の**最小多項式**と呼ぶことにする．例えば，R が UFD であれば z の最小多項式は一意的に定まるが，一般の整域 R では z の最小多項式は必ずしも一意的でないことに注意する．

R を含む整域 S の各元が R 上整であるとき，S は R 上**整**であるとか，S は R の**整拡大** (integral extension) である言う．特に，$R,\, S$ が体で，S が R 上整のとき，S は R 上**代数的**であるとか，S は R の**代数拡大**であると言う．S が R 上代数的でないとき，S は R 上**超越的**であるとか，S は R の**超越拡大**であると言う．

$x_1,\ldots,\, x_n \in S$ に対し，R-多元環として $R[X_1,\ldots,\, X_n] \cong R[x_1,\ldots,\, x_n]$ (左辺は多項式環) であるとき，$x_1,\ldots,\, x_n$ は R 上**代数的独立**であると言い，代数的独立でないとき**代数的従属**であると言う．

命題 6.2. 上の定義と同じ記号を用いる．$z \in L$ とする．
(1) $M \neq 0$ が $R[z]$-加群で，R-加群として有限生成ならば，z は R 上整である．
(2) z が R 上整であるための必要十分条件は，$R[z]$ が有限生成 R-加群であることである．

証明. (1) $M = Rx_1 + \cdots + Rx_n$ とする．M は $R[z]$-加群だから，$zx_i \in M$ であり

$$zx_i = \sum_{j=1}^{n} a_{ij}x_j \quad (a_{ij} \in R)$$

と書ける．a_{ij} を $(i,\, j)$-成分とする n 次正方行列を A, n 次の単位行列を I, $f(z) = \det(zI - A)$ とおくと，体 $Q(R[z])$ の元を成分とする行列とベクトルとして，連立方程式 $(zI - A)\mathbf{x} = \mathbf{0}$ がゼロベクトル以外の解を持つから，$f(z) = 0$ である．$f(z)$ は z^n の係数が 1 の，z についての n 次多項式だから，z は R 上整である．

(2) z が R 上整ならば ① を満たすから，逆に，$R[z]$ が有限生成 R-加群ならば，(1) を $M = R[z]$ として用いれば z は R 上整となる． □

命題 6.3. 定義 6.1 と同じ記号を用いる．
(1) $z \in L$ が R 上整で，$w \in L$ が $R[z]$ 上整ならば，w は R 上整である．
(2) $x, y \in L$ が R 上整ならば，$x+y$, xy も R 上整である．
(3) R が体で，$0 \neq x \in L$ が R 上代数的ならば，$1/x$ は R 上代数的である．
(4) S が R の整拡大ならば，$Q(S)$ は $Q(R)$ の代数拡大である．
(5) 整域 S が体 R 上整ならば S は体である．

証明. (1) $w \in L$ が $R[z]$ 上整ならば，$M := (R[z])[w] = R[z, w]$ も有限生成 R-加群である．前命題 (1) より，z は R 上整である．
(2) $R[x, y]$ は有限生成 R-加群だから，$x+y$, xy は R 上整である．
(3) x が R 上代数的ならば，$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ $(a_i \in R)$ と書ける．$a_0 \neq 0$ と仮定してよい．すると，

$$\frac{1}{x^n} + \frac{a_1}{a_0} \cdot \frac{1}{x^{n-1}} + \cdots + \frac{a_{n-1}}{a_0} \cdot \frac{1}{x} + \frac{1}{a_0} = 0$$

なので，$1/x$ は R 上代数的である．
(4) は明らかである．
(5) $x \in S$ が (3) の証明のように表せるとき，

$$\frac{1}{x} = \frac{1}{a_0}(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_2x + a_1) \in S$$

なので，S は体である． □

定義 6.4. 定義 6.1 と同じ記号を使う．前命題より，

$$R'_L := \left\{ x \in L \;\middle|\; x \text{ は } R \text{ 上整} \right\}$$

とおくと，R'_L は整域になる．R'_L を L における R の**整閉包**という．$R'_K = R$ が成り立つとき，R は**整閉** (integrally closed) であるという．R がネーター整域であって整閉であるとき，R は**正規環**であるという．

補題 6.5. R, S は可換環で，$R \subset S$ とする．このとき，S の素イデアル $\mathfrak{q}$ に対し，$\mathfrak{p} = \mathfrak{q} \cap R$ は R の素イデアルである．

証明. $x, y \in R$, $xy \in \mathfrak{p} \subset \mathfrak{q}$ ならば，$x \in \mathfrak{q}$ または $y \in \mathfrak{q}$ だから，$x \in \mathfrak{p}$ または $y \in \mathfrak{p}$ となる． □

定理 6.6.(Lying-over Theorem) R, S はネーター整域で，$R \subset S$ かつ S は R 上整とする．このとき，R の素イデアル $\mathfrak{p}$ に対し，$\mathfrak{q} \cap R = \mathfrak{p}$ となる S の素イデアル $\mathfrak{q}$ が存在する．また，R の素イデアル列 $\mathfrak{p}_0 \supsetneqq \mathfrak{p}_1 \supsetneqq \cdots \supsetneqq \mathfrak{p}_r$ に対し，S の素イデアル列 $\mathfrak{q}_0 \supsetneqq \mathfrak{q}_1 \supsetneqq \cdots \supsetneqq \mathfrak{q}_r$ で，$\mathfrak{q}_i \cap R = \mathfrak{p}_i$ を満たすものが存在する．
特に，$\operatorname{Krull\,dim} S = \operatorname{Krull\,dim} R$ である．

証明. まず，$\mathfrak{p}$ が R の極大イデアルの場合を考える．$\mathfrak{p}S \neq S$ であることを示す．もし $\mathfrak{p}S = S$ ならば，$1 = p_1s_1 + \cdots + p_ks_k$ $(p_i \in \mathfrak{p},\ s_i \in S)$ と書ける．$S' = R[s_1, \ldots, s_k]$ は有限生成 R-加群で，$S' = Rx_1 + \cdots + R_nx_n$ $(x_1 = 1)$ と表せば，$S' = \mathfrak{p}S'$ より，$x_i = \sum_{j=1}^{n} a_{ij}x_j$ $(a_{ij} \in \mathfrak{p})$ と表せる．a_{ij} を (i, j)-成分とする n 次正方行列を A とし，I を単位行列として，$b = \det(I - A) \in 1 + \mathfrak{p}$ とすれば，$bx_i = 0$ より $b = 0$ となり矛盾する．したがって，$\mathfrak{p}S \neq S$ である．
S における $\mathfrak{p}S$ の準素イデアル分解 $\mathfrak{p}S = J_1 \cap \cdots \cap J_m$ を取る．$I = \sqrt{J_1} \cap R$ とおけば，I は R の素イデアルで，$I \supset \mathfrak{p}$ である．$\mathfrak{p}$ は極大イデアルだから，$I = \mathfrak{p}$ である．そこで，$\mathfrak{q} = \sqrt{J_1}$ とおく．$S/\mathfrak{q}$ は $R/\mathfrak{p}$ 上整なので体であり，$\mathfrak{q}$ は極大イデアルである．そして，$\mathfrak{q} \cap R = \mathfrak{p}$ を満たす．

$\mathfrak{p}$ が R の素イデアルの場合は，$S_{\mathfrak{p}} = \{x/y \in Q(S) \mid x \in S,\, y \in R - \mathfrak{p}\}$ とおくと，$S_{\mathfrak{p}}$ は $R_{\mathfrak{p}}$ の整拡大である．$\mathfrak{p}R_{\mathfrak{p}}$ は $R_{\mathfrak{p}}$ の極大イデアルなので，上の議論から $S_{\mathfrak{p}}$ の極大イデアル $\tilde{\mathfrak{q}}$ で $\tilde{\mathfrak{q}} \cap R_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$ を満たすものが存在する．そこで，$\mathfrak{q} = \tilde{\mathfrak{q}} \cap S$ とおけば，$\mathfrak{q} \cap R = \mathfrak{p}R_{\mathfrak{p}} \cap R = \mathfrak{p}$ である．

さて，R の素イデアル列 $\mathfrak{p}_0 \supsetneqq \mathfrak{p}_1 \supsetneqq \cdots \supsetneqq \mathfrak{p}_r$ に対し，S の素イデアル列 $\mathfrak{q}_1 \supsetneqq \mathfrak{q}_2 \supsetneqq \cdots \supsetneqq \mathfrak{q}_r$ で $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ $(1 \leqq i \leqq r)$ を満たすものが存在することを帰納法の仮定として，$\mathfrak{q}_0$ の存在を証明する．$\overline{S} = S/\mathfrak{q}_1$ は $\overline{R} = R/\mathfrak{p}_1$ の整拡大である．上の議論から，$\overline{S}$ の素イデアル $\bar{\mathfrak{q}}$ で，$\bar{\mathfrak{q}} \cap \overline{R} = \mathfrak{p}_0/\mathfrak{p}_1$ を満たすものが存在する．そこで，自然な全射 $S \to \overline{S}$ による $\bar{\mathfrak{q}}$ の原像を $\mathfrak{q}_0 \subset S$ とすれば，$\mathfrak{q}_0 \cap R = \mathfrak{p}_0$, $\mathfrak{q}_0 \supsetneqq \mathfrak{q}_1$ となる．これより，$\operatorname{Krull\,dim} R \leqq \operatorname{Krull\,dim} S$ がわかる．

また，$\mathfrak{q}_0 \supsetneqq \mathfrak{q}_1 \supsetneqq \cdots \supsetneqq \mathfrak{q}_r$ が S の素イデアル列のとき，$\mathfrak{q}_0 \cap R \supset \mathfrak{q}_1 \cap R \supset \cdots \supset \mathfrak{q}_r \cap R$ は R の素イデアル列であり，上の議論から，もし $\mathfrak{q}_i \cap R = \mathfrak{q}_{i+1} \cap R$ ならば $\mathfrak{q}_i = \mathfrak{q}_{i+1}$ である．よって，$\operatorname{Krull\,dim} S \leqq \operatorname{Krull\,dim} R$ である． □

補題 6.7. (1) K は体で無限個の要素を持つとする．$f \in K[X_1,\ldots, X_n] - K$ ならば，$c_2,\ldots, c_n \in K$ をうまく選んで，$Y_i = X_i + c_iX_1$ $(2 \leqq i \leqq n)$ とおくと，$K[X_1,\ldots, X_n]$ は $K[f, Y_2,\ldots, Y_n]$ 上整になる．

(2) K は標数 p の有限体とする．$f \in K[X_1,\ldots, X_n] - K$ ならば，$m_2,\ldots, m_n \in \mathbb{N}$ をうまく選んで，$Y_i = X_i + X_1^{pm_i}$ $(2 \leqq i \leqq n)$ とおくと，$K[X_1,\ldots, X_n]$ は $K[f, Y_2,\ldots, Y_n]$ 上整になる．

証明. (1) f の $X_1,\ldots, X_n$ について i 次の部分を f_i として，$f = f_d + f_{d-1} + \cdots + f_0$ $(f_d \neq 0)$ とする．今，$f_d(1, -c_2, -c_3,\ldots, -c_n) \neq 0$ となるように，$c_2,\ldots, c_n \in K$ を選んでおく．すると，f を X_1, $Y_2,\ldots, Y_n$ $(Y_i = X_i + c_iX_1)$ の多項式で表し，

$$f = \sum_{i=0}^{d} g_i(Y_2, \ldots, Y_n) \cdot X_1^i$$

としたとき，$g_d \in K$ かつ $g_d = f_d(1, -c_2,\ldots, -c_n) \neq 0$ となる．上の等式を定数 g_d で割ると

$$X_1^d + \sum_{i=0}^{d-1} \frac{g_i(Y_2, \ldots, Y_n)}{g_d} \cdot X^i - \frac{f}{g_d} = 0$$

という $K[f, Y_2,\ldots, Y_n]$ 上の X_1 に関するモニック多項式が得られるので，X_1 は $K[f, Y_2,\ldots, Y_n]$ 上整である．

$2 \leqq i \leqq n$ に対し，$X_i = Y_i - c_iX_1$ も $K[f, Y_2,\ldots, Y_n]$ 上整であるから，$K[X_1,\ldots, X_n]$ は $K[f, Y_2,\ldots, Y_n]$ 上整である．

(2) の証明は，永田雅宜「可換環論」p.104 を見よ． □

定理 6.8. K は体，I は多項式環 $S = K[X_1,\ldots, X_n]$ の高さ r の素イデアルとする．すると，ある K 上代数的独立な $f_1,\ldots, f_n \in S$ が存在し，

(1) S は $R = K[f_1,\ldots, f_n]$ 上整.

(2) $I \cap R = \sum_{i=1}^{r} Rf_i$.

が成り立つようにできる．

証明. r に関する帰納法で証明する．$r = 0$ のときは $I = (0)$ だから主張は自明である．

$r \geqq 1$ とし，高さが r 未満のイデアルについては主張は正しいと仮定する．$J \subset I$ で $\operatorname{ht} J = r-1$ を満たす素イデアル J を取る．帰納法の仮定から，代数的独立な $Y_1,\ldots, Y_n \in S$ が存在し，S は $R' = K[Y_1,\ldots, Y_n]$ 上整，かつ，$J \cap R' = \sum_{i=1}^{r-1} R'Y_i$ を満たす．

Lying-over Theorem より $\operatorname{ht}(I \cap R') = r$ である．$Y_1,\ldots, Y_{r-1} \in J \cap R' \subset I$ に注意する．$0 \neq f_r \in I \cap K[Y_r, Y_{r+1},\ldots, Y_n]$ を取る．前補題から，ある $f_i = Y_i + c_iY_r$ または $f_i = Y_i + Y_r^{pm_i}$ $(r+1 \leqq i \leqq n)$ が存在し，$K[Y_r,\ldots, Y_n]$ は $K[f_r, f_{r+1},\ldots, f_n]$ 上整になる．$f_1 = Y_1,\ldots, f_{r-1} = Y_{r-1}$ とおけば，S は R' 上整，R' は $R = K[f_1,\ldots, f_n]$ 上整だから，S は R 上整になる．

また，$I \cap R$, $(f_1,\ldots, f_r) \subset R$ はいずれも素イデアルで，$\operatorname{ht}(I \cap R) = r = \operatorname{ht}(f_1,\ldots, f_r)$ だから，$I \cap R = (f_1,\ldots, f_r)$ である．構成の方法から，$f_{r+1},\ldots, f_n$ は $K(Y_1,\ldots, Y_r)$ 上代数的独立だから，$f_1,\ldots, f_n \in S$ は K 上代数的独立である． □

定理 6.9.(正規化定理) R が体 K 上有限生成な整域ならば，K 上代数的独立なある $x_1,\ldots, x_m \in R$ を選んで，R が $K[x_1,\ldots, x_m]$ 上整であるようにできる．

証明. $R = S/I$ のとき，前の定理の $f_{r+1},\ldots, f_n$ の I を法とする同値類を $x_1,\ldots, x_m$ とおけばよい. □

定義 6.10.(超越次数) 体 K を含む体 L が，K 上代数的に独立な d 個の超越元を含み，L 内のどの $d+1$ 個の元も代数的従属のとき，$d = \mathrm{tr.deg}_K L$ と書き，K 上の**超越次数**と言う．また，$d = \mathrm{tr.deg}_K L < +\infty$ で，K 上代数的独立なある元 $x_1,\ldots, x_d \in L$ が存在し，L が有理関数体 $K(x_1,\ldots, x_d)$ の有限次代数拡大体である場合，L は K 上**有限生成**な体であると言う．正規化定理により，これは，L が K 上有限生成なある整域の分数体であることと同値である．

定理 6.11. R が体 K 上有限生成な整域で，

$$\mathfrak{p}_d \supsetneqq \mathfrak{p}_{d-1} \supsetneqq \mathfrak{p}_{d-2} \supsetneqq \cdots \supsetneqq \mathfrak{p}_1 \supsetneqq \mathfrak{p}_0 = (0)$$

が細分できない R の素イデアル列で，$\mathfrak{p}_d$ が極大イデアルであれば，

$$\mathrm{Krull\ dim}\, R = \mathrm{tr.deg}_K Q(R) = d$$

である．

証明. $\mathrm{tr.deg}_K Q(R) = d$ を d に関する帰納法で証明する．$d = 0$ のとき，(0) が極大イデアルだから R は体で，$R = Q(R)$ は K の代数拡大で，$\mathrm{tr.deg}_K Q(R) = 0$ である．

$d \geqq 1$ とする．前の系と定理 6.8 より，K 上代数的独立な $x_1,\ldots, x_m \in R$ を選んで，R が $S = K[x_1,\ldots, x_m]$ 上整かつ，$\mathfrak{p}_1 \cap S = Sx_1$ となるようにできる．

$S' = S/(\mathfrak{p}_1 \cap S) \cong K[x_2, x_3,\ldots, x_m]$ とおく．準同型定理より，$S' = S/(\mathfrak{p}_1 \cap S) \subset R/\mathfrak{p}_1$ とみなせ，$R/\mathfrak{p}_1$ は S' 上整である．

$R/\mathfrak{p}_1$ と S' に対して帰納法の仮定を適用して，$\mathrm{tr.deg}_K Q(S') = d-1$ を得る．これより，$\mathrm{tr.deg}_K Q(R) = \mathrm{tr.deg}_K Q(S) = 1 + \mathrm{tr.deg}_K Q(S') = d$ を得る．

長さ d の素イデアル列が存在するから，$\mathrm{Krull\ dim}\, R \geqq d$ であるが，もし，$\mathrm{Krull\ dim}\, R > d$ とすると，長さ $d+1$ 以上の素イデアル列が存在し，上の結果から，$\mathrm{tr.deg}_K Q(R) \geqq d+1$ となって矛盾する．したがって，$\mathrm{Krull\ dim}\, R = d$ である． □

系 6.12. R が体 K 上有限生成な整域，I が R の素イデアルのとき，

$$\mathrm{ht}\, I + \mathrm{coht}\, I = \mathrm{Krull\ dim}\, R$$

である．

系 6.13. K が体のとき，$\mathrm{Krull\ dim}\, K[X_1,\ldots, X_n] = n$ である．

証明. $\mathrm{Krull\ dim}\, K[X_1,\ldots, X_n] = \mathrm{tr.deg}_K K(X_1,\ldots, X_n) = n$ である． □

7. 近似定理

命題 7.1. (K, v) は付値体とし，$c \in K$ とする．すると以下が成り立つ．

(1) $v\left(\dfrac{c}{1+c}\right) - 1 \leqq \dfrac{1}{v(1+c)}$.

(2) $v(c) < 2$ ならば $\dfrac{1}{2} < v\left(\dfrac{c}{1+c}\right) < 2$.

(3) $v(c) < \dfrac{1}{2}$ ならば $v\left(\dfrac{c}{1+c}\right) < 2v(c)$.

証明. (1) は $\dfrac{c}{1+c} = 1 - \dfrac{1}{1+c}$ の両辺の v を取り，三角不等式を用いればわかる．

(2) $1 < v(c) - v(1) < v(1+c) \leqq v(1) + v(c) = 1 + v(c)$ より，$\dfrac{1}{1+v(c)} \leqq \dfrac{1}{v(1+c)}$ である．よって，

$$\frac{1}{2} < \frac{v(c)}{1+v(c)} \leqq \frac{v(c)}{v(1+c)} = v\left(\frac{c}{1+c}\right) \leqq \frac{1}{v(1+c)} + 1 < 2$$

である．

(3) $v(1+c) \geqq 1 - v(c) > \dfrac{1}{2}$ より，$\dfrac{1}{v(1+c)} < 2$ なので，$v\left(\dfrac{c}{1+c}\right) = \dfrac{v(c)}{v(1+c)} < 2v(c)$ である．

□

定理 7.2.(近似定理) v_1,..., v_n は体 K 上の自明でない乗法的付値で，どの 2 つも同値でないとする．x_1,..., $x_n \in K$ は任意の元，ε は任意の正の実数とする．このとき，ある $y \in K$ で任意の $i = 1$,..., n に対して $v_i(y - x_i) < \varepsilon$ を満たすものが存在する．

証明. (1) $v_1(z) > 1$ で $i = 2$,..., n に対して $v_i(z) < 1$ となる $z \in K$ が存在することを，n に関する帰納法で証明する．

$n = 2$ のときは，v_1 と v_2 は同値でないから，定理 1.5 より $v_1(z_1) > 1$, $v_2(z_1) \leqq 1$ を満たす $z_1 \in K$ と，$v_2(z_2) \leqq 1$, $v_1(z_2) > 1$ を満たす $z_2 \in K$ が存在する．$v_2(z_1) < 1$ なら $z = z_1$ とおけばよい．$v_2(z_1) = 1$ なら $z = z_1/z_2$ とおけばよい．

$n \geqq 3$ とし，$n-1$ まで主張は正しいとする．帰納法の仮定から，ある $z_1 \in K$ で，$v_1(z_1) > 1$ であって，$i = 2$,..., $n-1$ に対して $v_i(z_1) < 1$ を満たすものが存在する．もし $v_n(z_1) < 1$ なら $z = z_1$ とおけばよいから，$v_n(z_1) \geqq 1$ と仮定する．

自然数 m を十分大きくえらべば，$v_1(z_1^m) > 2$ で，$i = 2$,..., $n-1$ に対して $v_i(z_1^m) < 1/2$ が成り立つ．そこで，z_1 の代わりに z_1^m を取ることにより，$v_1(z_1) > 2$, $v_i(z_1) < 1/2$ $(i = 2,\ldots, n-1)$ と仮定してよい．

再び帰納法の仮定から，ある $z_2 \in K$ で，$v_1(z_2) > 1$ であって，$i = 3$,..., n に対して $v_i(z_2) < 1$ を満たすものが存在する．もし $v_2(z_2) < 1$ なら $z = z_2$ とおけばよいから，$v_2(z_2) \geqq 1$ と仮定する．必要なら添え字 2 と n を入れ替え，$v_n(z_1) \leqq v_2(z_2)$ と仮定してよい．$v_2(z_2) = 1$ の場合は，$v_n(z_1) = 1$ となるから，$z = z_1 z_2$ が求める z になる．

そこで，$v_2(z_2) > 1$ の場合を考える．z_2 の代わりに z_2^k $(k \gg 1)$ を考えることにより，$v_2(z_2) > 2$ であって，かつ，$i = 3$,..., n に対して $v_i(z_2) < 1/2$ であると仮定してよい．さらに，$v_n(z_2) < 1/(2v_n(z_1))$ であると仮定してよい．すると，前命題より $z := \dfrac{z_1 z_2}{1+z_2}$ が (1) を満たす．

(2) $0 < \varepsilon' < \varepsilon/\big(v_i(x_1) + \cdots + v_i(x_n)\big)$ $(\forall i = 1,\ldots, n)$ となる ε' を取る．$\varepsilon' < 1/2$ と仮定してもよい $v_i(z_i) > 1$ で $j \neq i$, $1 \leqq j \leqq n$ に対して $v_j(z_i) < 1$ となる $z_i \in K$ を取る．$m \in \mathbb{N}$ を十分大きく選んで，$v_i(z_i^m) > 1 + 1/\varepsilon'$ であって，$j \neq i$, $1 \leqq j \leqq n$ に対して $v_j(z_i^m) < \varepsilon'/2$ となるようにできる．そこで，$y_i := \dfrac{z_i^m}{1+z_i^m}$ とおく．$j \neq i$ として，

$$v_i(y_i - 1) = \frac{v_i(-1)}{v_i(1+z_i^m)} \leqq \frac{1}{v_i(z_i^m) - 1} < \varepsilon',$$

$$v_j(y_i) = \frac{v_j(z_i^m)}{v_j(1+z_i^m)} \leqq \frac{v_j(z_i^m)}{v_j(1) - v_j(z_i^m)} < \frac{\varepsilon'/2}{1 - \varepsilon'/2} < \varepsilon'$$

となる．$y := x_1 y_1 + \cdots + x_n y_n$ とおく．

$$v_i(y - x_i) = v_i\left(x_i(y_i - 1) + \sum_{j \neq i} x_j y_j\right) \leqq v_i(x_i) v_i(y_i - 1) + \sum_{j \neq i} v_i(x_j) v_i(y_j)$$

$$< v_i(x_i)\varepsilon' + \sum_{j \neq i} v_i(x_j)\varepsilon' = \varepsilon' \sum_{j=1}^{n} v_i(x_j) < \varepsilon$$

となり，目的の不等式を得る． □

整閉整域と整閉包の一般論について，少し補足しておく．

定理 7.3. (1) R は整閉整域，$\mathfrak{p}$ は R の素イデアルとする．すると，$R_{\mathfrak{p}}$ は整閉整域である．
(2) R はネーター整域とする．R の任意の素イデアル $\mathfrak{p}$ に対し局所環 $R_{\mathfrak{p}}$ が整閉整域であれば，R が整閉整域 (正規環) である．

証明. (1) R は整閉整域，$\mathfrak{p}$ は R の素イデアルとする．$x \in Q(R_{\mathfrak{p}}) = Q(R)$ が $R_{\mathfrak{p}}$ 上整であるとすると，ある $n \in \mathbb{N}$ と $a_i \in R$ $(1 \leqq i \leqq n)$ と $b \in R - \mathfrak{p}$ が存在して，

$$x^n + \frac{a_1}{b}x^{n-1} + \frac{a_2}{b}x^{n-2} + \cdots + \frac{a_n}{b} = 0$$

と書ける．この式の両辺に b^n を掛けると，bx が R 上整であることがわかる．R は整閉だから，$bx \in R$ である．したがって，$x \in R_{\mathfrak{p}}$ である．よって，$R_{\mathfrak{p}}$ は整閉整域で，R は正規環である．
(2) R はネーター整域とする．$x \in Q(R)$ は R 上整な元とすると，R の任意の素イデアル $\mathfrak{p}$ について，x は任意の $R_{\mathfrak{p}}$ 上整で $R_{\mathfrak{p}}$ は整閉だから，$x \in R_{\mathfrak{p}}$ である．よって，$x \in \bigcap_{\mathfrak{p}} R_{\mathfrak{p}} = R$ となり，R は整閉整域である． □

定理 7.4.(整閉包の有限性 1) R はネーター整閉整域，L は $K := Q(R)$ の有限次分離的代数拡大体とする．また，A は整域で $R \subset A \subset L$ かつ A は R 上整であると仮定する．このとき，A は R-加群として有限生成である．特に，A はネーター環である．

証明. 必要なら L/K のガロア閉包を取ることにより，最初から L は K のガロア拡大であると仮定してよい．すると L は K の単純拡大になることがガロア理論で知られている．よって，ある $a \in L$ により，$L = K(a)$ と書ける．a の K 上の最小多項式は $f(X) = c_0X^n + c_1X^{n-1} + \cdots + c_n$ $(c_0,\ldots, c_n \in R)$ という形に書ける．$L = K(c_0a)$ だから，a の代わりに c_0a を取ることにより，$c_0 = 1$ で a は R 上整であると仮定してよい．$S := R[a]$ は R の整拡大なので，$S'_L = R'_L$ である．S'_L が有限 S-加群であることが証明できれば，S は有限 R-加群だから S'_L は有限 R-加群であることがわかり，その部分加群である A も有限 A-加群であることがわかる．
$f'(a)S_L \subset S$ を証明しよう．$f(X) = 0$ の根全体を $a_1 := a, a_2,\ldots, a_n$ とし，$g_i(X) = f(X)/(X - a_i)$ とおく．$f'(X) = g_1(X) + \cdots + g_n(X)$ である．任意の元 $b \in S'_L$ を取る．体拡大 L/K のガロア群を $G = \{\sigma_1, \sigma_2,\ldots, \sigma_n\}$ とする．ただし，$\sigma_1 = \mathrm{id}$, $\sigma_i(a) = a_i$ となるように添え字をつけておく．$g_1(X) = e_{n-1}X^{n-1} + e_{n-2}X^{n-2} + \cdots + e_0$ $(e_i \in S)$ と表す．$g_i(X) = \sigma_i(e_{n-1})X^{n-1} + \cdots + \sigma_i(e_0)$ である．$\gamma_j = \sum_{i=1}^{n} \sigma_i(be_j)$ とおく．任意の $\tau \in G$ に対して，$\tau(\gamma_j) = \sum_{i=1}^{n} \tau \circ \sigma_i(be_j) = \sum_{i=1}^{n} \sigma_i(be_j) = \gamma_j$ だから，$\gamma_j \in R$ である．$i \geqq 2$ のとき $g_i(a) = 0$ だから，

$$bf'(a) = bg_1(a) = \sum_{i=1}^{n} \sigma_i(b)g_i(a) = \sum_{i=1}^{n}\sum_{j=0}^{n-1} \sigma_i(be_j)a^j = \sum_{j=0}^{n-1} \gamma_j a^j \in R[a] = S$$

となる．以上で，$S'_L \subset (1/f'(a))S$ が証明された．
$(1/f'(a))S$ はネーター加群なので，その部分加群である S'_L もネーター加群であり，有限 S-加群である． □

定理 7.5.(整閉包の有限性 2) R は体 K 上有限生成な整閉整域で，L は $Q(R)$ の有限次代数拡大体とする．また，A は整域で $R \subset A \subset L$ かつ A は R 上整であると仮定する．このとき，A は R-加群として有限生成である．特に，A はネーター環である．

証明. L が K の分離拡大である場合には，前定理から結論を得る．L が K 上非分離的な場合に証明する．K, L の標数 p は 0 でない．
$A = R'_L$ の場合に証明すれば十分である．正規化定理により，K 上代数的独立なある $z_1,\ldots, z_l \in R$ を選んで，A が $K[z] := K[z_1,\ldots, z_l]$ 上整であるようにできる．以下の (1) を L の K 上の非分離次数 $[L : K]_i$ に関する帰納法で証明する．

(1) ある $q = p^e$ $(\exists e \in \mathbb{N})$ と，ある $c_1,\ldots, c_m \in K$ が存在して，$L(c_1^{1/q},\ldots, c_m^{1/q}, z_1^{1/q},\ldots, z_l^{1/q})$ が $K(c_1^{1/q},\ldots, c_m^{1/q}, z_1^{1/q},\ldots, z_l^{1/q})$ 上分離的になるようにできる．

$K[z]$ 上非分離的な元 $y \in A$ が存在する．y の $K[z]$ 上の最小多項式は $f(X) = X^{p^r} + a_1 X^{p^{r-1}} + \cdots + a_{r-1}X^p + a_r$ $(a_1,\ldots, a_r \in K[z])$ とい形である．$a_i = a_1(z_1,\ldots, z_l)$ を $z_1,\ldots, z_l$ の多項式と考えたとき登場する係数を $i = 1,\ldots, r$ について全部あわせて，$c_1,\ldots, c_m \in K$ であるとする．$K' := K(c_1^{1/p},\ldots, c_m^{1/p}, z_1^{1/p},\ldots, z_l^{1/p})$ とおくと，$y \in A$ の K' 上の最小多項式は $X^r + a_1' X^{r-1} + \cdots + a_{r-1}' X + a_r'$ $(a_i' = a_i^{1/p})$ である．よって，$L' := K(c_1^{1/p},\ldots, c_m^{1/p}, z_1^{1/p},\ldots, z_l^{1/p})$ とおくと，$[L' : K']_i < [L : K]_i$ となる．以下，帰納法で証明が完了るする．

(2) $B := K(c_1^{1/q},\ldots, c_m^{1/q})[z_1^{1/q},\ldots, z_l^{1/q}]$, $F := L(c_1^{1/q},\ldots, c_m^{1/q}, z_1^{1/q},\ldots, z_l^{1/q})$ とおく．F は $Q(B)$ の分離拡大体だから，B_F' は B-加群として有限生成である．定義から B は $K[z]$-加群として有限生成である．よって B_F' は $K[z]$-加群としても有限生成である．A は B_F' の部分 $K[z]$-加群だから，$K[z]$-加群として有限生成である． □

8．付値の拡大

補題 8.1. R は可換環，I は R のイデアル，$\mathfrak{p}_1,\ldots, \mathfrak{p}_n$ は R の素イデアルで，$I \not\subset \mathfrak{p}_i$ $(\forall i = 1,\ldots, n)$ が成り立つとする．すると，$I - \bigcup_{i=1}^{n} \mathfrak{p}_i \neq \phi$ である．

証明. $n = 1$ ならば自明である．$n \geqq 2$ とする．帰納法の仮定から $\exists y \in I - \bigcup_{i=1}^{n-1} \mathfrak{p}_i \neq \phi$ である．$\mathfrak{p}_i \subset \mathfrak{p}_j$ ならば最初から $\mathfrak{p}_i$ は取り除いて考えればよいから，はじめから，$i \neq j$ ならば $\mathfrak{p}_i \not\subset \mathfrak{p}_j$ と仮定して証明すればよい．$y \notin \mathfrak{p}_n$ なら証明完了だから，$y \in \mathfrak{p}_n$ とする．$i < n$ のとき $\exists x_i \in \mathfrak{p}_i - \mathfrak{p}_n$ である．また，$\exists x_0 \in I - \mathfrak{p}_n$ をとる．

$$x_0 x_1 x_2 \cdots x_{n-1} \in I\mathfrak{p}_1 \cdots \mathfrak{p}_{n-1} - \mathfrak{p}_n$$

なので，$z = x_0 x_1 x_2 \cdots x_{n-1}$ とおく．さらに，$x = y + z$ とおく．$y, z \in I$ だから $x \in I$ である．もし，$x \in \bigcup_{i=1}^{n-1} \mathfrak{p}_i$ とすると，$z \in \bigcap_{i=1}^{n-1} \mathfrak{p}_i - \mathfrak{p}_n$ だから，$y = x - z \in \bigcup_{i=1}^{n-1} \mathfrak{p}_i$ となり矛盾する．$y \in \mathfrak{p}_n$, $z \notin \mathfrak{p}_n$ だから $x = y + z \notin \mathfrak{p}_n$ である．よって，$x \in I - \bigcup_{i=1}^{n} \mathfrak{p}_i \neq \phi$ である． □

非アルキメデス的な乗法的付値の代数拡大体への延長の存在を証明する．体 K の代数拡大体 L に対し，

$$\mathrm{Aut}(L/K) := \left\{\sigma : L \to L \;\middle|\; \sigma \text{ は体の同型写像で，} \sigma|_K = \mathrm{id}_K\right\}$$

とおく．L が K のガロア拡大のときは $\mathrm{Aut}(L/K)$ を $\mathrm{Gal}(L/K)$ とも書く．L の K 上の分離的拡大次数を $[L : K]_s$ とするとき，$\#\,\mathrm{Aut}(L/K) \leqq [L : K]_s$ であった．

補題 8.2. K は体，$v_1,\ldots, v_k$ は K 上の非アルキメデス的付値で，R_i は v_i に関する K の付値環，$\mathfrak{m}_i$ は R_i の極大イデアルとする．また，$i \neq j$ ならば $R_i \not\subset R_j$ であると仮定する．$S = R_1 \cap \cdots \cap R_k$ とおく．このとき，以下が成り立つ．

(1) すると，任意の $x \in K$ に対して，ある $n = n(x) \in \mathbb{N}$ が存在して，

$$\frac{1}{x^n + x^{n-1} + \cdots + x + 1} \in S, \quad \frac{x}{x^n + x^{n-1} + \cdots + x + 1} \in S$$

を満たす．

(2) $\mathfrak{n}_i := \mathfrak{m}_i \cap S$ とおくと，$R_i = S_{\mathfrak{n}_i}$ ($\mathfrak{n}_i$ による局所化) が成り立つ．

(3) S の極大イデアル全体は $\mathfrak{n}_1,\ldots, \mathfrak{n}_k$ である．

証明. (1) $x = 1$ のときは簡単に証明できるから，$x \neq 1$ の場合を考える．$y := x^n + x^{n-1} + \cdots + x + 1$ とおく．

(i) $v_i(x) > 1$ の場合．

$$v_i(y) = v_i(x^n + x^{n-1} + \cdots + x + 1) = \max\left\{v_i(x^k) \;\middle|\; k = 0,\ldots, n\right\} = v_i(x^n) = v_i(x)^n$$

となる，よって，$v_i(1/y) = v_i(x)^{-n} < 1$, $v_i(x/y) = v_i(x)^{1-n} < 1$ となり，$y,\, x/y \in R_i$ となる．

(ii) $v_i(x) < 1$ の場合．$x \in \mathfrak{m}_i$ であるが，上と同様に，$v_i(y) = v_i(1) = 1$ となるので，$v_i(1/y) = 1$, $v_i(x/y) = v_i(x) < 1$ となり，$y,\, x/y \in R_i$ となる．

(iii) $v_i(x) = 1$ の場合．$x \in R_i - \mathfrak{m}_i$, $1/x \in R_i - \mathfrak{m}_i$ に注意する．$y = \dfrac{1-x^{n+1}}{1-x}$ なので，$v_i(y) = \dfrac{v_i(1-x^{n+1})}{v_i(1-x)}$ である．$k \in \mathbb{N}$ に対し $v_i(1-x^k) \leqq \max\{v_i(1),\, v_i(x^k)\} = 1$ である．$M_i := \{m \in \mathbb{Z} \mid v_i(x^m - 1) < 1\}$ とおく．$v_i(x^m - 1) = v_i(x^{-m} - 1)$ だから，$m \in M_i$ ならば $-m \in M_i$ である．もし $M_i = \{0\}$ ならば $v_i(y) = 1$ となり，$y,\, x/y \in R_i$ となる．

以下，$M_i \neq \{0\}$ の場合を考える．M_i に含まれる最小の正の整数を m_i とする．

(iii-1) $m_i \geqq 2$ の場合を考える．しばらく $m = m_i$ とおく．

$x^{lm} - 1 = (x^m - 1)(x^{(l-1)m} + x^{(l-2)m} + \cdots + x^m + 1)$ で $v_i(x^{(l-1)m} + x^{(l-2)m} + \cdots + x^m + 1) \leqq 1$ だから，$v_i(x^{lm} - 1) \leqq v_i(x^m - 1)$ である．$m \in M_i$ ならば，$v_i(x^{lm} - 1) \leqq v_i(x^m - 1) < 1$ となって，$lm \in M_i$ となる．また，$v_i(x^{-m} - 1) = v_i(1 - x^m) = v_i(x^m - 1) < 1$ となるので，M_i は，$\mathbb{Z}$ の部分加群となる．よって $M_i = m_i\mathbb{Z}$ となる．よって $1/y \notin R_i$ または $x/y \notin R_i$ となるのは，$(n+1)$ が m_i の倍数の場合に限る．

(iii-2) $m_i = 1$，つまり $v_i(1-x) < 1$ の場合を考える．

$a = 1 - x \in \mathfrak{m}_i$ とおくと，$y = \sum_{k=0}^{n} (1+a)^k = (n+1) + ab$ $(b \in R_i)$ という形に書けるので，$n+1 \notin \mathfrak{m}_i$ ならば，$v_i(y) = 1$ で $y,\, x/y \in R_i$ となる．つまり，$R_i/\mathfrak{m}_i$ の標数を p_i とするとき，よって $1/y \notin R_i$ または $x/y \notin R_i$ となるのは，$(n+1)$ が p_i の倍数の場合に限る．

(iv) 以上より，$(n+1)$ が，ある m_i または p_i の倍数でない限り，$1/y \in S$ かつ $x/y \in S$ となる．

(2) $S \subset R_i$ より，$S_{\mathfrak{n}_i} \subset (R_i)_{\mathfrak{n}_i} = R_i$ である．以下 $\supset$ を示す．

勝手な $x \in R_i$ を取る．(1) よりある $n \in \mathbb{N}$ が存在して，$y := x^n + x^{n-1} + \cdots + x + 1$ とおくとき，$1/y,\, x/y \in S$ となる．$x \in R_i$ より $y \in R_i$ で，$v_i(y) = 1$ で y は R_i の可逆元になる．$1/y \in R_i - \mathfrak{m}_i$ より，$1/y \notin \mathfrak{n}_i$ で，$x = (x/y)/(1/y) \in S_{\mathfrak{n}_i}$ となる．よって $S = R_i$ である．

(3) $i \neq j$ のとき $S_{\mathfrak{n}_i} = R_i \not\subset R_j = S_{\mathfrak{n}_j}$ だから，$\mathfrak{n}_1, \ldots, \mathfrak{n}_k$ は相異なるイデアルで，互いに包含関係はない．また，各 $\mathfrak{n}_i \subsetneqq I \subsetneqq S$ となる S のイデアル I があれば，$\mathfrak{m}_i \subsetneqq IR_i \subsetneqq R_i$ となって矛盾するから，各 $\mathfrak{n}_i$ は S の極大イデアルである．

$\mathfrak{n}$ を S の勝手なイデアルとする．任意の $1 \leqq \forall i \leqq k$ に対して $\mathfrak{n} \not\subset \mathfrak{n}_i$ であると仮定して矛盾を導く．

$x_i \in \mathfrak{n} - \mathfrak{n}_i$ を取る．また各 $\mathfrak{n}_i$ は S の素イデアルであるから，補題 8.1 より，$\exists y_i \in \bigcap_{j \neq i} \mathfrak{n}_j - \mathfrak{n}_i \neq \phi$ である．$z := x_1y_1 + \cdots + x_ky_k \in \mathfrak{n} \subset S$ とおく．$z - x_1y_1 = x_2y_2 + \cdots + x_ky_k \in \mathfrak{n}_1$ で $x_1y_1 \notin \mathfrak{n}_1$ なので $z \notin \mathfrak{n}_1$ である．同様に $z \notin \mathfrak{n}_i$ $(\forall i)$ である．よって，$v_i(z) = 1$ なので，$1/z \in R_i$ $(\forall i)$ となる．したがって $1/z \in S$ である．これは $z \in \mathfrak{n}$ に矛盾する．

以上より，ある $1 \leqq i \leqq k$ が存在して $\mathfrak{n} \subset \mathfrak{n}_i$ となる．$\mathfrak{n}$ は極大イデアルだから，$\mathfrak{n} = \mathfrak{n}_i$ である． □

定理 8.3. $(K,\, v)$ は非アルキメデス的な付値体とし，L は K の代数拡大体とする．$(R,\, \mathfrak{m})$ を K の付値環とし，L における R の整閉包を R'_L とする．S は $R \subset S \subset L$, $Q(S) = L$ を満たす整域とする．このとき，S が定義 2.2 の意味で付値環であって $S \cap K = R$ を満たすための必要十分条件は，R'_L のある極大イデアル $\mathfrak{n}$ が存在して，$S = (R'_L)_{\mathfrak{n}}$ となることである．

証明. (I) L が K の有限次代数拡大の場合に証明する．

(I-1) (十分性) (必要性) が証明できれば (十分性) も成り立つことを先に示しておく．$\mathfrak{n}$ を R'_L の勝手な極大イデアルとし $S := (R'_L)_{\mathfrak{n}}$ とおく．$S \cap K = R$ はすぐわかる．$S := (R'_L)_{\mathfrak{n}}$ が付値環であることを証明する．

まず，$S \subset T \subset L$ を満たす付値環 T が存在することを証明する．$S \subset A \subsetneqq L$ かつ $1 \notin \mathfrak{n}A$ かつ $A \cap K = R$ を満たす環 A 全体の集合を $\boldsymbol{\mathcal{A}}$ とおく．$S \in \boldsymbol{\mathcal{A}}$ だから $\boldsymbol{\mathcal{A}} \neq \phi$ である．$\boldsymbol{\mathcal{A}}$ が包含関係に関して帰納的順序集合になることは容易にわかる．Zorn の補題により $\boldsymbol{\mathcal{A}}$ の極大元 T が存在する．

この T は整閉で，付値環であることを示す．

$T \subsetneqq T' \subset L$ を満たす T の整拡大 T' が存在したと仮定する．定理 6.6 より $\mathfrak{n}T'$ は T' の極大イデアルである．T' の極大イデアル $\mathfrak{a}$ は $\mathfrak{a} \cap S = \mathfrak{n}$ を満たすので，$\mathfrak{a} = \mathfrak{n}T'$ となり，T' は局所環である．ま

た，$1 \notin \mathfrak{n}T'$ である．$T \cap K = R$ で T' は T の整拡大だから $T' \cap K = R$ である．よって，$T' \in \boldsymbol{\mathcal{A}}$ となり，T の極大性に反する．従って，T は整閉である．

$x \in K - R$ をとる．$T[x] \notin \boldsymbol{\mathcal{A}}$ だから $1 \in \mathfrak{n}T$ である．したがって，ある $m \in \mathbb{N}$ と $c_0, \ldots, c_m \in \mathfrak{n}T$ により，$1 = c_0 + c_1 x + c_2 x^2 + \cdots + c_m x^m$ — ① と書ける．$1 - c_0 \notin \mathfrak{n}T$ である．したがって，$c_0 - 1$ は T の可逆元である．① を変形すると $\left(\dfrac{1}{x}\right)^n + \displaystyle\sum_{k=1}^{m} \frac{c_i}{c_0 - 1} \left(\frac{1}{x}\right)^{m-k} = 0$ であるから，$1/x$ は T 上整である．T は整閉だから $1/x \in T$ である．定理 2.3 より T は付値環である．

T は付値環で $Q(T) = L, T \cap K = R$ を満たすから，(必要性) から，R'_L のある極大イデアル $\mathfrak{n}$ が存在して，$T = (R'_L)_{\mathfrak{n}}$ となる．よって，$(R'_L)_{\mathfrak{n}}$ は付値環である．また $(R'_L)_{\mathfrak{n}} \cap R = T \cap K = R$.

(I-2) (必要性) S が付値環で $Q(S) = L, S \cap K = R$ を満たすならば，R'_L のある極大イデアル $\mathfrak{n}$ が存在して，$S = (R'_L)_{\mathfrak{n}}$ となることを証明する．

(I-2-i) L が K の有限次正規拡大 (分離性は仮定しない) の場合を考える．

$G := \mathrm{Aut}(L/K)$, $A := \displaystyle\bigcap_{\sigma \in G} \sigma(S)$ とおく．$H := \left\{\sigma \in G \;\middle|\; \sigma(S) = S\right\}$ とし，G/H の完全代表系を $\sigma_1, \ldots, \sigma_n \in G$ とすれば，$A = \sigma_1(S) \cap \cdots \cap \sigma_n(S)$ で，$1 \leqq i < j \leqq n$ のとき $\sigma_i(S) \neq \sigma_j(S)$ である．

S の極大イデアルを $\mathfrak{p}$ とし，$S_i := \sigma_i(S)$，$\mathfrak{p}_i = \sigma_i(\mathfrak{p}) \subset S_i$, $\mathfrak{n}_i = \mathfrak{p}_i \cap A$ とおく．補題 8.2(2) より，$S_i = A_{\mathfrak{n}_i}$ である．

$A \subset R'_L$ を示す．$a \in A \subset L$ を取る．$m := \#G$ とし，$\left\{\sigma(a) \;\middle|\; \sigma \in G\right\}$ の k 次の基本対象式を c_k とする．$c_k \in K$ である．$f(X) := x^m + \displaystyle\sum_{k=1}^{n} (-1)^k c_k X^{m-k} = \prod_{\sigma \in G} \big(X - \sigma(a)\big)$ とおくと，$f(X) \in K[X]$ で $f(a) = 0$ である．S_i に対応する L の非アルキメデス的付値を v_i とするとき，$\sigma(a) \in A \subset R_i$ だから $v_i(\sigma(a)) \leqq 1$ である．c_k は $\sigma(a)$ 達の多項式だから $v_i(c_k) \leqq 1$ である．よって，$c_k \in R$ で $f(X) \in R[X]$ である．したがって a は R 上整で $a \in R'_L$ となる．これより $A \subset R'_L$ である．よって $\mathfrak{n} = \mathfrak{n}_i R'_L$ とおけば，これは R'_L の極大イデアルで，$S_i = A_{\mathfrak{n}_i} \subset (R'_L)_{\mathfrak{n}}$ である．定理 2.8(2) より，$S_i \subsetneqq (R'_L)_{\mathfrak{n}}$ となることはない．ゆえに $S_i = (R'_L)_{\mathfrak{n}}$ である．

L が K の有限次正規拡大の場合は，当初の議論から (十分性) も成立することに注意する．

(I-2-ii) L が K の有限次代数拡大の場合を考える．

ガロア理論でよく知られているように，L の有限次代数拡大体 M で K の正規拡大になっているようなものが存在する．このとき，M は L の正規拡大でもある．

S は付値環で $Q(S) = L, S \cap K = R$ を満たすとする．すると，M の付値環 T で $Q(T) = M, T \cap L = S$ を満たすものが存在する．このとき $T \cap K = R$ も成り立つ．R'_M のある極大イデアル $\overline{\mathfrak{n}}$ が存在して，$T = (R'_M)_{\overline{\mathfrak{n}}}$ となる．$\mathfrak{n} := \overline{\mathfrak{n}} \cap R'_L$ とおく．$\mathfrak{n}$ は R'_L の極大イデアルである．補題 8.2(2) より，$S = (R'_L)_{\mathfrak{n}}$ となる．

(II) L が K の一般の代数拡大体の場合を考える．

(II-1) (十分性)

$\mathfrak{n}$ が R'_L の極大イデアルのとき，$S := (R'_L)_{\mathfrak{n}}$ が付値環で $S \cap K = R$ を満たすことを示す．勝手な $0 \neq a \in L$ を取る．$K(a)$ は K の有限次代数拡大だから，$T := S \cap K(a)$, $\mathfrak{q} := \mathfrak{n} \cap T$ とおけば，T は $K(a)$ の付値環で $\mathfrak{q}$ は T の極大イデアルである．(I) より $T \cap K = R$ である．これより $S \cap K = R$ が得られる．また，T は付値環だから $a \in T$ または $1/a \in T$ である．よって，$a \in S$ または $1/a \in S$ だから，S は付値環である．

(II-2) (必要性) S が付値環で $Q(S) = L, S \cap K = R$ を満たすならば，R'_L のある極大イデアル $\mathfrak{n}$ が存在して，$S = (R'_L)_{\mathfrak{n}}$ となることを証明する．

S の極大イデアルを $\mathfrak{p}$ とし，$\mathfrak{n} := \mathfrak{p} \cap R'_L$ とおく．勝手な $a \in S$ を取る．$T := S \cap K(a)$, $\mathfrak{q} := \mathfrak{n} \cap K(a)$ とすれば，$R'_a := R'_L \cap K(a)$ は $K(a)$ における R の整閉包だから，(I) の結果から $T = (R'_a)_{\mathfrak{q}}$ となる．$a \in T = (R'_a)_{\mathfrak{q}} \subset (R'_L)_{\mathfrak{n}}$ だから，$S \subset (R'_L)_{\mathfrak{n}}$ である．

逆に $S \supset R'_L$ だから，$S = S_{\mathfrak{n}} \subset (R'_L)_{\mathfrak{n}}$ である． □

9. 付値の分岐

ネーター環でない付値環では，以下のような現象が起きる．

補題 9.1. (K, v) は非アルキメデス的な付値体とし，その付値環 $(R, \mathfrak{m})$ はネーター環でないと仮定する．$0 \neq a \in R$ に対し $\varphi(a) = -\log_2 v(a)$ として加法的付値を定める．すると，任意の正の実数 ε に対し，$0 < \varphi(x) < \varepsilon$ を満たす $x \in \mathfrak{m}$ が存在する．

証明. 形式的に $\varphi(0) = +\infty$ と約束しておく．任意の $y \in \mathfrak{m}$ は $\varphi(y) > 0$ を満たす．$m_0 := \min\left\{\varphi(y) \,\middle|\, y \in \mathfrak{m}\right\}$ が存在したと仮定する．$\varphi(\pi) = m_0$ を満たす $\pi \in \mathfrak{m}$ を取る．$y \in \mathfrak{m}$ ならば $\varphi(y/\pi) \geqq 0$, つまり $v(y/\pi) \leqq 1$ なので $y/\pi \in R$ である．よって，$y = a\pi$ $(\exists a \in R)$ と書ける．よって，$\mathfrak{m} \subset \pi R$ である，$\mathfrak{m}$ は極大イデアルなので $\mathfrak{m} = \pi R$ となり，R は離散付値環となり，ネーター環になる．よって，上のような最小値 m_0 は存在しない． □

以下の定理の証明はネーター環なら簡単であるが，一般の場合はちょっと面倒である．

定理 9.2. (K, v) は非アルキメデス的な付値体とし，L は K の代数拡大体とする．$(R, \mathfrak{m})$ は K の付値環とする．また，$(S, \mathfrak{n})$ は付値環で，$Q(S) = L$ かつ $S \cap K = R$ を満たすものとする．すると L 上の付値 w で，$w|_K = v$ を満たし，

$$S = \left\{x \in L \,\middle|\, w(x) \leqq 1\right\}, \quad \mathfrak{n} = \left\{x \in S \,\middle|\, w(x) < 1\right\}$$

となるものが一意的に存在する．

証明. L における R の整閉包を R'_L とする．$0 \neq q \in \mathfrak{m}$ を取る．

(1) $0 \neq x \in S$ ならば，任意の $n \in \mathbb{N}$ に対して $x \in q^n S$ となることはないことを示す

$x \in R'_L$ の場合を考える．x の R 上の最小多項式を $f(X) = X^m + c_{m-1}X^{m-1} + \cdots + c_1 X + c_0$ とする．$x \in q^n S$ とすると，$c_0 \in q^n S \cap R = q^n R$ である．よって，$n \leqq \log v(c_0)/\log v(q)$ となる．ここで $v(q) < 1$ なので $\log v(q) \neq 0$ である．

一般の $x \in S$ は $x = x_1/x_2$ $(x_1, x_2 \in R'_L)$ と書ける．$x \in q^n S$ ならば $x_1 \in q^n S$ だから，(1) が成立する．

(2) $0 \neq x \in S$ を $m \in \mathbb{N}$ に対し，$x^m \in q^{n(m)}S$, $x^m \notin q^{n(m)+1}S$ を満たす $n(m) \in \mathbb{N} \cup \{0\}$ を取り，$\psi_q(x) := \lim\limits_{m\to\infty} \dfrac{n(m)}{m} \in \mathbb{R}$ とおく．

(2-1) $0 \neq r \in \mathfrak{m}$ を取るとき，$\psi_r(x) = \psi_q(x) \log_{v(q)} v(r)$ が成り立つことを証明する．

$M/N \leqq \log_{v(q)} v(r) < (M+1)/N$ $(M, N \in \mathbb{N})$ とすると，$v(q^M) \geqq v(r^N) > v(q^{M+1})$ であるから，$r^N \in q^M R$, $r^N \notin q^{M+1}R$ となる．これと，ψ_q, ψ_r の定義から，容易に結論が得られる．

そこで，$\psi(x) := -\psi_q(x) \log_2 v(q)$ とおくと，この値は $0 \neq q \in \mathfrak{m}$ の選び方に依存しない．

(2-2) $0 \neq x \in \mathfrak{n}$ を取る．$x \in qS$ となる $q \in \mathfrak{m}$ が存在する．$0 \neq y \in S$ が $y \in x^n S$ を満たせば $y \in q^n S$ であるから，$y \notin x^n S$ を満たす $n \in \mathbb{N}$ が存在する．そこで，$\psi_x(y)$ を (2) と同じ方法で定義することができる．上の議論から，$\psi(y) = -\psi_x(y) \log_2 w(x)$ が任意の $0 \neq y \in S$ に対して成り立つように $w(x) \in \mathbb{R}$ を定義できる．$z = y_1/y_2 \in L$ $(y_1, y_2 \in S)$ に対しては，$w(z) = w(y_1)/w(y_2)$ と定める．この w が L 上の非アルキメデス的付値であることは容易に確認できる．また，定義から $x \in \mathfrak{n}$ ならば $w(y) < 1$ である．さらに，$w|_R = v$ である．

(2-3) $w(x) = 1$ $(x \in L)$ ならば，$1/x \in S$ であることを示す．

x の R 上の最小多項式を $f(X) = X^m + c_1 X^{m-1} + \cdots + c_1 X + c_0$ とする．すると，

$$w(c_0) \geqq \max\left\{w(-x^m), \ldots, w(-c_1 x)\right\} \geqq 1$$

より $v(c_0) = w(c_0) = 1$ となる．$c_0/x = -(x^{m-1} + \cdots + c_1) \in S$ であるが，$1/c_0 \in R$ なので $1/x \in S$ である．以上より，

$$S = \left\{x \in L \,\middle|\, w(x) \leqq 1\right\}, \quad \mathfrak{n} = \left\{x \in S \,\middle|\, w(x) < 1\right\}$$

が成り立つ．w は必然的に $\psi(y) = -\psi_x(y) \log_2 w(x)$ を満たさないといけないから，一意的である． □

系 9.3. (K, v) は非アルキメデス的な付値体とし，L は K の代数拡大体とする．L 上の付値 w_1, w_2 が $w_1|_K = v$, $w_2|_K = v$ を満たすならば，ある $\sigma \in \mathrm{Aut}(L/K)$ が存在して $w_2 = w_1 \circ \sigma$ となる．

証明. $S_i = \left\{x \in L \,\middle|\, w_i(x) \leqq 1\right\}$ とおく．前定理の証明からわかるように，$S_2 = \sigma(S_1)$ を満たす $\sigma \in \mathrm{Aut}(L/K)$ が存在する．$S := \left\{x \in L \,\middle|\, w_1(\sigma^{-1}(x)) \leqq 1\right\}$ とおくと，$S = \sigma(S_1) = S_2$ となるので，前定理の一意性から $w_2 = w_1 \circ \sigma^{-1}$ である． □

命題 9.4. (K, v) は非アルキメデス的付値体とし，1 変数有理関数体 $L := K(X)$ を考える．このとき，L 上の非アルキメデス的付値 w で，$w|_K = v$ を満たすものが存在する．

証明. R を K の付値環とし，$S = R[X] \subset L$ とおく．$Q(S) = L$, $S \cap K = R$ である．$f(X) = c_n X^n + \cdots + c_1 X + c_0 \in R[X] = S$ を取る．$c_0, \ldots, c_n$ で生成されるイデアルを I とすると，R は付値環なので I は単項イデアルになる．$I = dR$ $(\exists d \in R)$ と書けるので，$w(f(X)) = v(d)$ と定まる．この w を拡張して L の付値を定めれば，(L, w) は非アルキメデス的付値体になる． □

以下の分岐の理論は，ネーター性を仮定しないと簡明な理論にならない．

定義 9.5. K は非アルキメデス的付値体で，その付値環 $(R, \mathfrak{m})$ は離散付値環であると仮定する．さらに，K の標数は 0 であるか，あるいは，R はある体上有限生成な環であると仮定する．L は K の有限次代数拡大体とし，$(S, \mathfrak{n})$ は L の付値環で $Q(S) = L$, $S \cap K = R$ を満たすものとする．整閉包の有限性定理より S も離散付値環になる．$\mathfrak{m}$, $\mathfrak{n}$ は単項イデアルだから，$\mathfrak{m} = \pi R$, $\mathfrak{n} = pS$ と書ける．$e := \operatorname{ord}_p \pi \in \mathbb{N}$ を S の R 上の**分岐指数**といい，体の拡大次数 $f := [S/\mathfrak{n} : R/\mathfrak{m}]$ を**相対次数**とか単に**次数**という．

定理 9.6.(分岐定理) K, L, R, $\mathfrak{m} = \pi R$ は上の定義と同じとする．すると，$Q(S) = L$, $S \cap K = R$ を満たす L の付値環 S の全体は有限個である．それを $S_1, \ldots, S_n$ とする．S_i の R 上の分岐指数と相対次数をそれぞれ e_i, f_i とする．このとき，

$$e_1 f_1 + \cdots + e_n f_n = [L : K]$$

が成り立つ．

証明. $Q(S_i) = L$, $S_i \cap K = R$ を満たす L の付値環 S_i の全体の集合を $\{S_i \mid i \in I\}$ とする．S_i の極大イデアルを $\mathfrak{n}_i = p_i S_i$ とする．ここで，$p_i = a/b$ $(a \in R'_L, b \in R'_L - \mathfrak{n}_i)$ と書けるが，$p_i S_i = a S_i$ だから，$p_i \in R'_L$ と仮定してよい．$\mathfrak{p}_i := \mathfrak{n}_i \cap R'_L = p_i R'_L$ とおくとき，$S_i = (R'_L)_{\mathfrak{p}_i}$ であった．$\operatorname{Krull\,dim} R'_L = 1$ で $\mathfrak{p}_i$ は R'_L の素イデアルだから，R'_L の極大イデアルである．また，定理 8.3 より，R'_L の極大イデアル全体が $\mathfrak{p}_i$ $(i \in I)$ である．

$\mathfrak{m} R'_L$ の (0) でない準素イデアル $\mathfrak{q}$ を取ると，$\sqrt{\mathfrak{q}}$ は (0) でない素イデアルであるから，いずれかの $\mathfrak{p}_i$ と一致する．よって，$\mathfrak{q} = \mathfrak{p}_i^k = p_i^k R'_L$ の形に書ける．便宜的に $\mathfrak{p}_i^0 = R'_L$ とする．$\pi R'_L$ の準素イデアル分解は，

$$\pi R'_L = \mathfrak{p}_1^{k_1} \cap \cdots \cap \mathfrak{p}_n^{k_n} = p_1^{k_1} R'_L \cap \cdots \cap p_n^{k_n} R'_L = \left(p_1^{k_1} \cdots p_n^{k_n}\right) R'_L$$

と書ける．よって，$\pi = u p_1^{k_1} \cdots p_n^{k_n}$ (u は R'_L の可逆元) である．特に $I = \{1, \ldots, n\}$ である．

$$e_i = \operatorname{ord}_{p_i} \pi = \operatorname{ord}_{p_i} \left(p_1^{k_1} \cdots p_n^{k_n}\right) = k_i$$

だから，$k_i = e_i$ がわかる．中国剰余定理により，

$$R'_L / \pi R'_L \cong R'_L / p_1^{e_1} R'_L \oplus \cdots \oplus R'_L / p_n^{e_n} R'_L$$

となる．$R'_L / \pi R'_L$ は $R/\pi R$-加群なので，$R'_L / p_i^{e_i} R'_L$ も $R/\pi R$-加群で，

$$\dim_{R/\pi R} R'_L / p_i^{e_i} R'_L = \dim_{R/\pi R} R'_L / p_i R'_L \times \dim_{R'_L/p_i R'_L} R'_L / p_i^{e_i} R'_L = f_i \times e_i = e_i f_i$$

である．よって，$\dim_{R/\pi R} R'_L / \pi R'_L = e_1 f_1 + \cdots + e_n f_n$ である．

あと，$\dim_{R/\pi R} R'_L / \pi R'_L = [L : K]$ を証明すれば，定理が得られる．

$R/\pi R$-ベクトル空間としての $R'_L / \pi R'_L$ の基底を $\overline{x_1}, \ldots, \overline{x_m}$ (ただし $x_i \in R'_L$ で，$\overline{x_i}$ は $\pi R'_L$ を法とする x_i の同値類) とする．$M := R x_1 + \cdots + R x_n \subset R'_L$ とするとき，$M + \pi R'_L = R'_L$ が成り立つので，中山の補題から $M = R'_L$ となる．

また，L の元は a/b $(a, b \in R'_L)$ の形であるが，b の K 上のすべての共役元を a/b の分母・分子に掛けることにより，$b \in K \cap R'_L = R$ と仮定してよい．よって，$L = K x_1 + \cdots + K x_m$ がわかる．

$x_1, \ldots, x_m$ が K 上 1 次独立であることを示す．$a_1 x_1 + \cdots + a_m x_m = 0$ $(\exists a_1, \ldots, a_m \in K)$ とする．$a_i = b_i / c_i$ $(b_i, c_i \in R)$ として，$c_1 \cdots c_m$ を乗じて考えれば，最初から $a_1, \ldots, a_m \in R$ であると仮定してよい．$j := \min \left\{ \operatorname{ord}_\pi a_i \mid i = 1, \ldots, m \right\}$ とし，$a_1, \ldots, a_m$ を π^j で割っておいて，ある $1 \leqq i \leqq m$ に対して $\operatorname{ord}_\pi a_i = 0$ であると仮定してよい．

$a_1x_1+\cdots+a_mx_m=0$ これを $\pi R'_L$ を法として考えると，a_1,..., $a_m\in\pi R$ であることがわかる．これは，$\operatorname{ord}_\pi a_i=0$ と矛盾する．よって，x_1,..., x_m は K-ベクトル空間として L の基底であって，$[L:K]=m=\dim_{R/\pi R}R'_L/\pi R'_L$ である． □

上の定理で，R が離散付値環であるという仮定や，K の標数は 0 とか，R はある体上有限生成な環であるという仮定をはずした場合の定理が，永田雅宜「可換体論」p.185 定理 4.9.6 に紹介されている．その場合，証明が複雑になるのに，$e_1f_1+\cdots+e_nf_n\leqq[L:K]$ という弱い結果しか得られない．実用上，上の分岐定理は，代数的整数論や代数幾何学で使われる場合が主で，その場合は上の定理の仮定が成立している．

定理 9.7.(積公式 1) $0\neq x\in\mathbb{Q}$ と素数 p に対し，$v_p(x)=p^{-\operatorname{ord}_p x}$ によって $\mathbb{Q}$ 上の p 進付値 v_p を定める．また，$v_\infty(x)=|x|$ とし，

$$V_{\mathbb{Q}}=\{v_\infty\}\cup\big\{v_p\;\big|\;p\text{ は素数}\big\}$$

とおく．このとき，任意の $0\neq x\in\mathbb{Q}$ に対し，

$$\prod_{v\in V_{\mathbb{Q}}}v(x)=1$$

が成り立つ．

証明. $f(x):=\prod_{v\in V_{\mathbb{Q}}}v(x)\in\mathbb{Q}$ とおく．$x,y\in\mathbb{Q}-\{0\}$ に対し，$v(xy)=v(x)v(y)$ より $f(xy)=f(x)f(y)$ が成り立つ．特に，$x=y/z$ $(y,z\in\mathbb{Z})$ ならば $f(x)=f(y)/f(z)$ である．また，$v(-x)=v(x)$ だから $f(-x)=f(x)$ である．そこで，$x\in\mathbb{N}$ に対して $f(x)=1$ が成り立つことを示せば十分である．$v(1)=1$ $(\forall v\in V_{\mathbb{Q}})$ だから $f(1)=1$ である．

$x=p_1^{n_1}\cdots p_r^{n_r}$ $(p_1,\ldots,p_r$ は素数) と素因数分解するとき，$f(x)=f(p_1)^{n_1}\cdots f(p_r)^{n_r}$ だから，p が素数のとき $f(p)=1$ を示せば十分である．$v_\infty(p)=|p|=p$, $v_p(p)=p^{-\operatorname{ord}_p p}=1/p$ で，q が p 以外の素数のときは $v_q(p)=q^{-\operatorname{ord}_q p}=q^0=1$ である．よって，$f(p)=p\dot{(}1/p)=1$ となる． □

定理 9.8.(積公式 2) 実数 $0<c<1$ を 1 つ固定する．K は体，$K(X)$ は K 上の 1 変数有理関数体とし．$K[X]$ の素元 $p(X)$ と $f(X)\in K[X]$ に対し，$K[X]$ 上の付値 $v_{p(X)}$ を

$$v_{p(X)}\big(f(X)\big):=c^{\deg p(x)\cdot\operatorname{ord}_{p(X)}f(X)}$$

と定め，$v_{p(X)}$ を自然に $K(X)$ まで拡張する．また，$Y:=1/X$ とおいて $f(Y)=f(1/X)\in K[1/X]$ に対し，

$$v_\infty\big(f(1/X)\big)=c^{\operatorname{ord}_Y f(Y)}$$

として $K[1/X]$ 上に定めた付値 v_∞ を自然に $K(X)$ まで拡張する．

$$V=\{v_\infty\}\cup\big\{v_{p(X)}\;\big|\;p(X)\text{ は }K[X]\text{ のモニックな素元}\big\}$$

とおく．このとき，任意の $0\neq f(X)\in K(X)$ に対し，

$$\prod_{v\in V}v\big(f(X)\big)=1$$

が成り立つ．

証明. $f(X)\in K(X)$ に対して $\varphi(f(X)):=\prod_{v\in V}v\big(f(X)\big)$ とおく．前定理の証明と同じ理由で，$f(X)$ が $K[X]$ の素元のとき $\varphi(f(X))=1$ であることを証明すれば十分である．$d:=\deg f(X)$ とおく．$f(X)$ が $p(X)$ と異なる $K[X]$ の素元のとき $v_{p(X)}f(X)=1$ で，$v_{f(X)}f(X)=c^d$ である．

また，$Y=1/X$ とし，$f(X)=c_dX^d+c_{d-1}X^{d-1}+\cdots+c_1X+c_0$ $(c_d\neq0)$ とおく．$f(X)$ は素元なので既約で $c_0\neq0$ である．$g(Y):=c_0Y^d+c_1Y^{d-1}+\cdots+c_{d-1}Y+c_d$ とおくと，$f(X)=g(Y)/Y^d$ で $\operatorname{ord}_Y g(Y)=0$ である．これより，

$$v_\infty\big(f(X)\big)=\frac{c^{\operatorname{ord}_Y g(Y)}}{c^{\operatorname{ord}_Y Y^d}}=\frac{1}{c^d}=c^{-d}$$

となる．したがって，$\varphi((f(X))=1$ である． □

第 II 部 実体

10. 順序体と実体

定義 10.1. K が体であり，かつ全順序集合であって，以下の (1), (2), (3) を満たすとき，K は**順序体**であるという．ただし，以下で a, b, c, d は K の任意の元である．
(1) $a \geqq b$, $c \geqq d$ ならば $a+c \geqq b+d$.
(2) $a \geqq b$ ならば $-a \leqq -b$.
(3) $a > 0$, $b > 0$ ならば $ab > 0$.

K と L が順序体のとき，$f\colon K \to L$ が体としての中への同型写像であって，かつ $a, b \in K$ に対し「$a > b \iff f(a) > f(b)$」が成り立つとき，f は**順序体としての中への同型写像**であるという．さらに，f が全射であるとき，f は**順序体としての同型写像**であるという．順序体としての同型写像 $f\colon K \to L$ が存在するとき，K と L は**順序体として同型**であるとか，**順序同型**であるという．

1 つの体を順序体にするような順序は一通りとは限らない．例えば $K = \mathbb{Q}(\sqrt{2})$ においては，通常の順序 $\geqq$ 以外に,「$a + b\sqrt{2} \succeq c + d\sqrt{2} \iff a - b\sqrt{2} \geqq c - d\sqrt{2}$」として順序 $\succeq$ を定めると，$\succeq$ についても K は順序体になる．

定義 10.2. K は体とする．部分集合 $X \subset K$ に対して，

$$\Sigma(X) := \left\{ a_1^2 + \cdots + a_n^2 \;\middle|\; n \in \mathbb{N},\ a_1, \ldots, a_n \in X \right\}$$

と書くとにする．$-1 \notin \Sigma(K)$ のとき，K は**実体**であるという．
K が実体であって，任意の代数拡大体 $L \supsetneqq K$ について L が実体にならないとき，K は**実閉体**であるという．

命題 10.3. (1) 順序体は実体である．
(2) 順序体や実体の標数は 0 である．

証明. (1) K は順序体であると仮定する．$a \in K$ に対し，$a > 0$ ならば順序体の定義の (3) から $a^2 > 0$ であり，$a < 0$ ならば $-a > 0$ だから $a^2 = (-a)^2 > 0$ である．よって，$a \in K$ ならば $a^2 \geqq 0$ である．これより，$a \in \Sigma(K)$ ならば $a \geqq 0$ である．$1 = 1^2 > 0$ だから $-1 < 0$ であり，$-1 \notin \Sigma(K)$ である．
(2) 体 K の標数が素数 $p > 0$ であるとすると，$-1 = \underbrace{1^2 + \cdots + 1^2}_{p-1 \text{ 個}} \in \Sigma(K)$ だから K は実体でない．
(1) より K は順序体でない． □

上の命題の逆は，後で証明する．

命題 10.4. K は体とする．
(1) $a, b \in \Sigma(K)$ ならば $a + b \in \Sigma(K)$ かつ $ab \in \Sigma(K)$.
(2) $a \in \Sigma(K)$, $a \neq 0$ ならば $1/a \in \Sigma(K)$.
(3) K の標数が 2 でなく，K が実体でないならば $\Sigma(K) = K$ である．
(4) K が実体で，$a \in \Sigma(K)$ かつ $-a \in S(K)$ ならば，$a = 0$ である．

証明. (1) $a = a_1^2 + \cdots + a_n^2$, $b = b_1^2 + \cdots + b_m^2$ ならば，$ab = \displaystyle\sum_{i=1}^{n}\sum_{j=1}^{m}(a_i b_j)^2 \in \Sigma(K)$ である．$a+b \in \Sigma(K)$ は自明.
(2) $\dfrac{1}{a} = \dfrac{a}{a^2} = \displaystyle\sum_{i=1}^{n}\left(\frac{a_i}{a}\right)^2 \in \Sigma(K)$.
(3) K が実体でないとすると，$-1 \in \Sigma(K)$ である．任意の $a \in K$ をとると，

$$a = \left(\frac{a+1}{2}\right)^2 + (-1)\left(\frac{a-1}{2}\right)^2 \in \Sigma(K)$$

なので，$K = \Sigma(K)$.

(4) $a, -a \in \Sigma(K)$, $a \neq 0$ と仮定すると，(2) より $-1 = (-a)/a \in \Sigma(K)$ となってしまう． □

定理 10.5. K は実閉体で，$a \in K$ とする．
(1) もし $a \in \Sigma(K)$ ならば，ある $b \in K$ が存在して $a = b^2$ と書ける．
(2) もし $a \notin \Sigma(K)$ ならば，ある $b \in K$ が存在して $a = -b^2$ と書ける．
(3) $-\Sigma(K) = \{a \in K \mid -a \in \Sigma(K)\}$ とおくと，

$$K = \Sigma(K) \cup (-\Sigma(K)), \quad \Sigma(K) \cap (-\Sigma(K)) = \{0\}$$

である．
(4) $a_1^2 + \cdots + a_n^2 = 0$, $a_1, \ldots, a_n \in K$ ならば $a_1 = \cdots = a_n = 0$ である．

証明. (1) $\overline{K}$ を K の代数閉包とし，$a \in K$ に対し $\sqrt{a} \in \overline{K}$ を考える．$\sqrt{a} \notin K$ と仮定してみる．$K(\sqrt{a}) \supsetneqq K$ だから $K(\sqrt{a})$ は実体でない．よって，ある $n \in N$ と $b_i + c_i\sqrt{a} \in K(\sqrt{a})$ ($\exists b_i, \exists c_i \in K$. $i = 1, \ldots, n$) により，

$$-1 = \sum_{i=1}^{n} \left(b_i + c_i\sqrt{a}\right)^2 = \sum_{i=1}^{n} b_i^2 + a\sum_{i=1}^{n} c_i^2 + 2\sqrt{a}\sum_{i=1}^{n} b_i c_i$$

と書ける．$B := \sum_{i=1}^{n} b_i^2 \in \Sigma(K) \subset K$, $C := \sum_{i=1}^{n} c_i^2 \in \Sigma(K) \subset K$ だから，$\sqrt{a} \notin K$ の係数は $\sum_{i=1}^{n} b_i c_i = 0$.
よって，$1 + B + aC = 0$ で $1 + B \neq 0$ だから前命題より $-a = (1 + B)/C \in \Sigma(K)$ である．$a \neq 0$ であるが，もし $a \in \Sigma(K)$ ならば，前命題から $-1 = (-a)/a \in \Sigma(K)$ となり矛盾する．
対偶をとれば，$a \in \Sigma(K)$ ならば $\sqrt{a} \in K$ である．

(2) $b = -a$ とおいて上の議論を使うと，もし $\sqrt{-a} \notin K$ ならば $a = -b \in \Sigma(K)$ となる．対偶を取ると，$a \notin \Sigma(K)$ ならば $\sqrt{-a} \in K$ である．

(3) 上の議論から，$a \in K$ ならば $\sqrt{a} \in K$ または $\sqrt{-a} \in K$ である．$\sqrt{a} \in K$ ならば $a \in \Sigma(K)$ であり，$\sqrt{-a} \in K$ ならば $a \in (-\Sigma(K))$ なので，$\Sigma(K) \cup (-\Sigma(K)) = K$ である．
$a \in \Sigma(K) \cap (-\Sigma(K))$ を取る．$a = -b^2$ ($\exists b \in K$) と書ける．もし，$a \neq 0$ ならば $b \neq 0$ で，$a \in \Sigma(K)$ だから，$-1 = a/b^2 \in \Sigma(K)$ となり矛盾する．

(4) $n = 1$ のときは自明．$n \geqq 2$ のとき，$a_1 \neq 0$ とすると，$-1 = \sum_{i=2}^{n} (a_i/a_1)^2 \in \Sigma(K)$ となり矛盾する．よって，$a_1 = 0$ である．同様に，$a_2 = \cdots = a_{n-1} = 0$ である． □

実閉体とは限らない実体 K の中には $\Sigma(K) \cup (-\Sigma(K)) \subsetneqq K$ となるものもある．例えば有理関数体 $K = \mathbb{R}(X)$ は実体であるが，$X \notin \Sigma(\mathbb{R}(X)) \cup (-\Sigma(\mathbb{R}(X)))$ である．

命題 10.6. K は体，$P \subset K$ は部分集合で，以下の (1), (2), (3) を満たすとする．
(1) $a, b \in P$ ならば $a + b \in P$ かつ $ab \in P$.
(2) $0 \notin P$.
(3) $0 \neq a \in K$ ならば $a \in P$ または $-a \in P$.
すると，$x, y \in K$ に対して
(4) $x > y \iff x - y \in P$
によって順序を定めると K は順序体になる．また，$(K, \leqq')$ が順序体になるような順序 $\leqq'$ が

$$P = \{x \in K \mid 0 \leqq' x, x \neq 0\}$$

を満たせば，$\leqq'$ は (4) によって定めた順序 $\leqq$ と一致する．

証明. $N := \{x \in K \mid -x \in P\}$ とおく．もし，$a \in P \cap N$ ならば $0 = a + (-a) \in P$ となって矛盾するので，$P \cap N = \phi$ である．(3) より，$K = P \sqcup N \sqcup \{0\}$ となる．これより (4) によって定まる順序 $\leqq$ は全順序であることが容易にわかる．定義 10.1 の (1), (2), (3) の確認も簡単で，K は順序体であることがわかる．

(一意性) $\leqq'$ と $\leqq$ が一致することを示す．$x \leqq' y$, $x \neq y$ ならば，順序体の性質から $0 \leqq' y - x$ かつ $y - x \neq 0$ である．よって，$y - x \in P$ であり，$x < y$ となる．逆に　$x < y$ ならば $x \leqq' y$, $x \neq y$ であることも同様にしてわかる，よって $\leqq'$ と $\leqq$ は一致する． □

定理 10.7. (1) K が実閉体ならば，K 上に適当な順序 $\leqq$ を定めて，$(K, \leqq)$ が順序体になるようにできる．$(K, \leqq)$ が順序体になるような順序 $\leqq$ は一意的である．
(2) K, L が実閉体で，$f\colon K \to L$ が体としての同型写像ならば，順序体としての同型写像になる．

証明. (1) $P := \left\{x^2 \in K \;\middle|\; 0 \neq x \in K\right\}$ とおく．これが前命題の (1), (2), (3) を満たすことを確認する．(1) 後半の $(x^2)(y^2) = (xy)^2 \in P$ と (2) は自明. (3) は定理 10.5 からわかる．
残った (1) の前半の $x^2 + y^2 \in P$ を証明する．$x \neq 0$, $y \neq 0$ のとき $x^2 + y^2 \neq 0$ である (そうでないと $-1 = (y/x)^2 \in \Sigma(K)$ となる)．$x^2 + y^2 \notin P$ とすると，定理 10.5 より $-(x^2 + y^2) \in P$ である．$-(x^2 + y^2) = z^2$ $(\exists z \in K)$ であるが，$-1 = (x/z)^2 + (y/z)^2$ となり K が実体であることと矛盾する．
以上から，前命題を用いて K は順序体にできる．
$(K, \leqq')$ が順序体になるような別の順序 $\leqq'$ があったとする．$a = x^2 \in P$ ならば $0 \leqq' a$, $a \neq 0$ である ($a >' 0$ と書くことにする)．逆に，$0 \neq b \in K$, $b \notin P$ ならば $-b \in P$ だから $-b >' 0$ であり，$b <' 0$ である．よって，$a > b \iff a - b > 0 \iff a - b >' 0 \iff a >' b$ となり，順序 $\leqq'$ と $\leqq$ は一致する．
(2) $P' := \left\{x^2 \;\middle|\; 0 \neq x \in L\right\}$ とおくと，$f(P) \subset P'$ である．$P' \subset f^{-1}(P)$ でもあるから，$f(P) = P'$ である．これより，f が順序同型であることがわかる． □

定義 10.8. $(K, \leqq)$ は順序体とする．K の標数は 0 なので，$\mathbb{N} \subset \mathbb{Q} \subset K$ と考える．任意の $x \in K$ に対し，ある $n \in \mathbb{N}$ を選べば $x \leqq n$ となるとき，K は**アルキメデス的**順序体であるといい，そうでないとき**非アルキメデス的**順序体であるという．

$(K, \leqq)$ が非アルキメデス的順序体のとき，任意の $n \in \mathbb{N}$ に対し $n < y$ を満たす $y \in K$ が存在する．$x = 1/y$ とおけば，任意の $n \in \mathbb{N}$ に対し $0 < x < \dfrac{1}{n}$ を満たす．したがって，極限値 $\lim\limits_{n\to\infty} \dfrac{1}{n}$ は存在せず (そもそも，極限の定義をどうすればいいかわからない)，K 上で普通の解析学の真似事をしようとしても苦労が多い．

11. 実閉体

定理 11.1. K は体で，$a \in K$, $a \notin \Sigma(K)$ であると仮定する．すると，K の代数拡大体であるような実閉体 K^* で，K^* 上の順序で $a < 0$ となるようなものが存在する (一意的とは限らない)．特に，実体は (一般には複数の) 順序体の構造を持つ．

証明. $\overline{K}$ を K の代数閉包とし，

$$\boldsymbol{\mathcal{A}} := \left\{L \;\middle|\; L \text{ は体で } K \subset L \subset \overline{K} \text{ で } a \notin \Sigma(L)\right\}$$

とおく．$\boldsymbol{\mathcal{A}}$ は包含関係に関して空でない帰納的順序集合であるので，Zorn の補題により極大元 L_1 を持つ．命題 10.4(3) より L_1 は実体である．

$$\boldsymbol{\mathcal{B}} := \left\{L \;\middle|\; L \text{ は実体で } L_1 \subset L \subset \overline{K}\right\}$$

も帰納的順序集合だから極大元 K^* を持つ．$K^* \subsetneqq L \in \boldsymbol{\mathcal{B}}$ となる L はないから K^* は実閉体である．K^* を順序体にするような順序 $>$ が一意的に存在する．この順序を L_1, K に制限して考える．
$\sqrt{-a} \notin L_1$ と仮定すると $L_1(\sqrt{-a}\,) \supsetneqq L_1$ だから，L_1 の極大性により $a \in \Sigma\left(L_1(\sqrt{-a}\,)\right)$ である．よって，

$$a = \sum_{i=1}^{n} \left(b_i + c_i\sqrt{-a}\,\right)^2 \quad (\exists n \in \mathbb{N}.\ \exists b_i, \exists c_i \in L_1)$$

と書ける．$B := \sum\limits_{i=1}^{n} b_i^2$, $C := \sum\limits_{i=1}^{n} c_i^2$ とおくと $\sum\limits_{i=1}^{n} b_i c_i = 0$ で $a = B - aC$ となる．命題 10.4 より $a = B/(C+1) \in \Sigma(L_1)$ となり矛盾する．よって，$\sqrt{-a} \in L_1$ で $-a = \left(\sqrt{-a}\,\right)^2 > 0$ となる．この不等式は K^* で成立していて $a < 0$ である． □

定理 11.2. K が実体のとき，K に適当な順序を定めて順序体になるようにできる．

証明. K は実体だから $-1 \notin \Sigma(K)$ である．前定理より，K の代数拡大体であるような実閉体 K^* が存在する．K^* 上に適当な順序 $\leqq$ を定めて，$(K^*, \leqq)$ が順序体になるようにできる．この順序を K に制限すれば，K も順序体になる． □

注意. 前定理において，K から L への中への同型写像は一意的とは限らないので，K 上の順序は一意的とは限らない．

補題 11.3. G は有限群で $\#G = 2^n$ $(n \in \mathbb{N})$ であるとする．すると，G の部分群 H で $\#H = 2^{n-1}$ を満たすものが存在する．

証明. G の演算は積で表すことにする．
n に関する帰納法で証明する．$n = 1$ のときは，$H = \{1\}$ とおけばよい．
$n \geqq 2$ の場合を考える．

$$Z(G) := \left\{ a \in G \;\middle|\; \text{任意の } x \in G \text{ に対し } ax = xa \right\}$$

を G の中心といった．群論でよく知られているように，$Z(G)$ は G の正規部分群である．また，類等式に関する次の定理があった．$x \in G$ に対し，

$$Cx := \left\{ axa^{-1} \in G \;\middle|\; a \in G \right\}$$

と書くことにする．このとき，以下が成り立つ．
(1) 有限個の $x_1, x_2, \ldots, x_r \in G$ が存在して，

$$G = Cx_1 \sqcup Cx_2 \sqcup \cdots \sqcup Cx_r$$

が成り立つ．
(2) $\#G = \#Z(G) + \sum_{\#Cx_i \geqq 2} \#Cx_i$ が成り立つ．

(2) が類等式である．ところで，$Z_x := \left\{ a \in G \;\middle|\; ax = xa \right\}$ とおくと，Z_x は G の部分群である．

(3) $\#Cx = \#(G/Z_x)$ を示す．

$f\colon G \to C_x$ を $f(a) = axa^{-1} \in Cx$ $(a \in G)$ で定めるとき，「$f(a) = f(b) \iff axa^{-1} = bxb^{-1} \iff x = (a^{-1}b)xb^{-1}a = (a^{-1}b)x(a^{-1}b)^{-1} \iff (a^{-1}b)x = x(a^{-1}b) \iff a^{-1}b \in Z_x$」である．よって，$f$ から全単射 $\overline{f}\colon G/Z_x \longrightarrow Cx$ が導かれる．

(4) Z_x は G の部分群なので $\#Z_x$ は $\#G = 2^n$ の約数である．よって，$\#Cx$ も 2^n の約数である．特に，$\#Cx \geqq 2$ ならば $\#Cx$ は偶数である．類等式 (2) より，$\#Z(G)$ は偶数である．特に，$Z(G) \neq \{1\}$ である．

(5) もし $Z(G) = G$ ならば，G はアーベル群だから，有限アーベル群の構造定理により，G は $\mathbb{Z}/2^k\mathbb{Z}$ という形の巡回群の直和であり，この場合，定理は簡単に証明できる．

(6) $Z(G) \neq G$ の場合を考える．$\#G/Z(G) < \#G$ で $\#G/Z(G) = 2^k$ $(1 \leqq k < n)$ だから，帰納法の仮定により，ある部分群 $H' \subset G/Z(G)$ で $\#H' = 2^{k-1}$ を満たすものが存在する．$\pi\colon G \to G/Z(G)$ を自然な単射として $H := \pi^{-1}(H')$ とおけば，$G/H \cong (G/Z(G))/H' \cong \mathbb{Z}/2\mathbb{Z}$ だから $\#H = 2^{n-1}$ となる． □

$\mathbb{R}$ は実閉体であって，その代数閉体 $\mathbb{C}$ は $\mathbb{C} = \mathbb{R}[\sqrt{-1}]$ を満たす．これが，一般の実閉体でも成り立つことを示していこう．

定理 11.4. (1) K が実閉体ならば $K(\sqrt{-1}\,)$ は代数閉体である．
(2) K が実体で，$K(\sqrt{-1}\,)$ が代数閉体ならば，K は実閉体である．

証明. (1) K は実閉体とする．
(i) $f(X) \in K[X]$ が奇数次のモニック多項式ならば，$f(a) = 0$ を満たす $a \in K$ が存在することを $d := \deg f(X)$ に関する帰納法で証明する．
$d = 1$ ならば自明なので $d \geqq 3$ とする．$f(X)$ が可約ならば奇数次の既約因子を持つので，$f(X)$ が既約な場合に証明すればよい．K の代数閉包 $\overline{K}$ における $f(X) = 0$ の勝手な根 α を取るとき，$\alpha \notin K$

である．$K(\alpha) \supsetneqq K$ なので $K(\alpha)$ は実体でない．よって，ある $n \in \mathbb{N}$ と $b_1, \ldots, b_n \in K(\alpha)$ により，$-1 = \sum_{i=1}^{n} b_i^2$ と書ける．また，$b_i \in K(\alpha) = K[\alpha]$ なので，$b_i = \sum_{j=0}^{d-1} c_{ij}\alpha^j$ $(\exists c_{ij} \in K)$ と書ける．$g_i(X) = \sum_{j=0}^{d-1} c_{ij}X^j$, $g(X) = 1 + \sum_{i=1}^{n} g_i(X)^2 \in K[X]$ とおく．$g(\alpha) = 0$ なので，$g(X)$ は $f(X)$ の倍数で，$g(X) = f(X)h(X)$ $(\exists h(X) \in K[X])$ と書ける．$\deg g(X)$ は偶数，$\deg f(X)$ は奇数なので，$\deg h(X)$ は奇数で，$\deg h(X) \leqq d-2$ である．帰納法の仮定から $h(\beta) = 0$ を満たす $\beta \in K$ が存在する．すると，$g(\beta) = 0$ となり，$-1 = \sum_{i=1}^{n} g_i(\beta) \in \Sigma(K)$ となって，K が実体であることと矛盾する．

(ii) $C := K(\sqrt{-1})$ とし，$a \in C$ ならば $\sqrt{a} \in C$ であることを証明する．
$a = b + c\sqrt{-1}$ $(a, b \in K)$ とする．

$$\left(\sqrt{\frac{\sqrt{b^2+c^2}+b}{2}} + \sqrt{-1}\sqrt{\frac{\sqrt{b^2+c^2}-b}{2}}\right)^2 = b + c\sqrt{-1}$$

なので，$\sqrt{a} \in C$ である．

(iii) $C := K(\sqrt{-1})$ とし，$\overline{K}$ を C を含む代数閉包とする．$\omega \notin K(\sqrt{-1})$ となる $\omega \in \overline{K}$ が存在したと仮定して矛盾を導く．

C を含む K の有限次ガロア拡大 L を取る．ガロア群を $G := \mathrm{Gal}(L/K)$ とし，G の 2-シロー群 S を取る．

$$M := \left\{a \in L \;\middle|\; \text{任意の } \sigma \in S \text{ に対し } \sigma(a) = a\right\}$$

とすると，M の K 上の拡大次数は $[M : K] = \#G/\#S$ で，これは奇数である．勝手な $\alpha \in M$ の K 上の最小多項式 $f_\alpha(X)$ は奇数次であるが．(i) より $f_\alpha(X)$ は 1 次式であり，$M = K$ となる．よって，$G = S$ で $\#G = 2^n$ と書ける．$n \geqq 2$ と仮定して矛盾を導こう．

$$H = \left\{\sigma \in G \;\middle|\; \text{任意の } a \in C \text{ に対し } \sigma(a) = a\right\}$$

とおく．$\#(G/H) = 2$ だから $\#H = 2^{n-1}$ である．前補題より，H の部分群 I で，$\#I = 2^{n-2}$ を満たすものが存在する．I に対応する C の 2 次拡大 $C(\sqrt{\alpha})$ $(\exists \alpha \in C)$ が存在する．しかし，(ii) の結果から $\sqrt{\alpha} \in C$ で，これは矛盾である．よって，$n = 1$ で $C = \overline{K}$ である．

(2) $K(\sqrt{-1})$ が代数閉体ならば，$K \subsetneqq L \subset K(\sqrt{-1})$ を満たす体 L は $L = K(\sqrt{-1})$ 以外になく，$K(\sqrt{-1})$ は実体でないから，K は実閉体である． □

上の定理の (2) からわかるように，$\mathbb{R}$ は実閉体である．

命題 11.5.(中間値の定理) K は実閉体，$f(X) \in K[X]$, $a, b \in K$ で，$a < b$, $f(a)f(b) < 0$ であると仮定する．すると，$f(c) = 0$, $a < c < b$ を満たす $c \in K$ が存在する．

証明. $f(X)$ はモニックであると仮定してよい．K の代数閉包を $\overline{K}$ とするとき $[\overline{K} : K] = 2$ である．したがって，

$$f(X) = \prod_{i=1}^{r}(X - a_i)\prod_{j=1}^{s} g_j(X), \quad (a_i \in K,\ g_j(X) \in K[X] \text{ は既約なモニック 2 次多項式})$$

と因数分解できる．$g_j(X)$ は既約なモニック 2 次多項式だから，$g_j(X) = (X - b_j)^2 + c_j$ $(b_j, c_j \in K$ で $c_j > 0)$ という形に表すことができる．よって，任意の $x \in K$ に対して $g_j(x) > 0$ である．この因子は $f(x)$ の符号の変化に関係しないから，$f(X) = (X - a_1)\cdots(X - a_r)$ の場合の証明すれば十分である．$a_1 < a_2 < \cdots < a_r$ と仮定してよい．もし，$a < a_i < b$ となる a_i が存在すれば $c = a_i$ とおけばよい．そういう a_i が存在しなければ，$a_{i-1} < a < b < a_i$ $(1 \leqq \exists i \leqq r)$ か $a > a_r$ か $b < a_1$ である．いずれの場合も，$f(a)$ と $f(b)$ は同符号になるから，$f(a)f(b) < 0$ に反する． □

命題 11.6. K は順序体，$f(X) = X^n + c_1X^{n-1} + \cdots + c_{n-1}X + c_n \in K[X]$ で $a \in K$ は $f(a) = 0$ を満たすとする．$M := \max\left\{1, |c_1| + \cdots + |c_n|\right\}$ とおく．このとき，$|a| \leqq |M|$ である．

証明. $|a| \leqq 1$ なら定理は自明なので，$|a| > 1$ の場合を考える．すると，

$$\begin{aligned} |a| = |-a| &= \left|c_1 + c_2 a^{-1} + \cdots + c_{n-1} a^{2-n} + c_n a^{1-n}\right| \\ &\leqq |c_1| + |c_2 a^{-1}| + \cdots + |c_{n-1} a^{2-n}| + |c_n a^{1-n}| \\ &\leqq |c_1| + |c_2| + \cdots + |c_{n-1}| + |c_n| \leqq M \end{aligned}$$

となる． □

12. スツルムの定理

定義 12.1.(基準列) K は体とする．一般に，$g(X) = c_n X^n + \cdots + c_1 X + c_0 \in K[X]$ に対し，$\dfrac{d}{dX} g(X) = \sum_{i=1}^{n} i c_i X^{i-1}$ と定義する．$f(X) \in K[X]$ に対し，まず，$f_0(X) := f(X)$, $f_1(X) = \dfrac{d}{dX} f(X)$ とおく．$i \geqq 1$ として，帰納的に $f_0(X)$,..., $f_i(X)$ まで定まったとき，$f_{i+1}(X)$ は $f_{i-1}(X)$ を $f_i(X)$ で割った余りの (-1) 倍とする．つまり，$f_{i-1}(X) = f_i(X) q_i(X) - f_{i+1}(X)$, $\deg f_{i+1}(X) < \deg f_i(X)$ $(\exists q_i(X) \in K[X])$. ここで，もし $f_{i+1}(X) = 0$ となったら，その直前の $f_i(X)$ を最後の多項式として，この操作はここで終了するものとする．このとき得られた多項式の列 $f_0(X)$,..., $f_i(X)$ を $f(X)$ の**基準列**という．

定義 12.2.(符号変化) K は順序体とし，$a_0, a_1, \ldots, a_n \in K$ とする．まず，K の元の列 $a_0, a_1, \ldots, a_n$ から $a_i = 0$ である項をすべて取り除いた部分列を $b_0, \ldots, b_m$ とする．そして，符号が変化する場所の個数 $N := \#\{i \in \mathbb{N} \mid b_{i-1} b_i < 0,\ i \leqq m\}$ を $a_0, \ldots, a_n$ の**符号変化の数**といい，以下本章では $N = V(a_0, \ldots, a_n)$ という記号で表すことにする．

また，$f(X) \in K[X]$, $a, b \in K$, $a < b$ に対し，開区間 (a, b) 内での $f(X) = 0$ の (重複度を数えない) 根の個数を

$$R_f(a, b) := \#\{c \in K \mid f(c) = 0,\ a < c < b\}$$

で表す．

補題 12.3. K は実閉体，$g_0(X), g_1(X) \in K[X]$ は定数でない互いに素な多項式とする．また，$g_i(X) \in K[X]$ $(i = 2, 3, \ldots, s-1)$ と，$q_i(X) \in K[X]$ $(i = 1, 2, \ldots, s-1)$ は，次の (1), (2) を満たすとする．

(1) 各 $i = 1, 2, \ldots, s-1$ に対して $g_{i-1}(X) = g_i(X) q_i(X) - g_{i+1}(X)$ が成り立つ．

(2) $g_s(X)$ は 0 でない定数多項式である．

また，$a, b \in K$, $a < b$ で，以下が成り立つと仮定する．

(3) $g_0(a) \neq 0$, $g_0(b) \neq 0$.

(4) $g_0(X)$ は開区間 (a, b) 上に重根を持たない．

$c \in K$ に対し，$W(c) := V(g_0(c), g_1(c), \ldots, g_s(c))$ とおく．

(I) もし，$R_{g_0}(a, b) = 0$ ならば $W(a) = W(b)$ が成り立つ．

(II) 上の (1)〜(4) に加えて，$g_0(X), g_1(X)$ が以下の条件 (5) を満たすならば，$R_{g_0}(a, b) = W(a) - W(b)$ が成り立つ．

(5) $g_0(c) = 0$, $c \in K$, $a < c < b$ ならば，$\varepsilon > 0$ を満たす $\varepsilon \in K$ が存在し，$c - \varepsilon < x < c + \varepsilon$ 任意の x に対して $\operatorname{sign} g_0(x) g_1(x) = \operatorname{sign}(x - c)$ が成り立つ．

証明. (Step 1) $g_i(c) = 0$ $(a < c < b,\ 1 \leqq i < s)$ ならば $g_{i-1}(c) g_{i+1}(c) < 0$ であることを示す．

$g_{i-1}(c) = g_i(c) q_i(c) - g_{i+1}(c) = -g_{i+1}(c)$ である．ユークリッドの互除法の原理から，定数倍を無視すれば $g_s(X)$ は $g_{i-1}(X)$ と $g_i(X)$ の最大公約数である．よって，$g_{i-1}(c) = 0$ ならば $g_s(c) = 0$ となって (2) に反する．したがって $g_{i-1}(c) g_{i+1}(c) < 0$ である．

(Step 2) $R_i := \{c \in K \mid g_i(c) = 0 \text{ かつ } a < c < b\}$ とし，$R := (R_1 \cup \cdots \cup R_{s-1}) - R_0$ とおく．いま，$a = c_0 < c_1 < \cdots < c_n = b$ を，次の条件を満たすように取る．ただし，条件 (i) は (II) の場合にのみ課し，(I) の場合には課さない．

(i) $R \subset \{c_0, \ldots, c_n\}$.

(ii) $R_1 \cap \{c_0, \ldots, c_n\} = \phi$.

(iii) $R_{g_0}(c_{i-1}, c_i) \leqq 1$ $(1 \leqq \forall i \leqq n)$.

(iv) $[c_{i-1}, c_i] \cap R_0 \neq \phi$ ならば $[c_{i-1}, c_i]$ 上で $\operatorname{sign} g_0(x) g_1(x) = \operatorname{sign}(x - c)$ であって $[c_{i-1}, c_i] \cap (R_1 \cup R_2 \cdots \cup R_s) = \phi$.

$$\sum_{i=1}^{n} R_{g_0}(c_{i-1}, c_i) = R_{g_0}(a, b), \quad \sum_{i=1}^{n} \big(W(c_{i-1}) - W(c_i)\big) = W(a) - W(b)$$

だから，各 $1 \leqq i \leqq n$ に対して $R_{g_0}(c_{i-1}, c_i) = W(c_{i-1}) - W(c_i)$ が成り立つことが証明できれば，定理が得られる．つまり，「$R_{g_0}(c_{i-1}, c_i) = 0$ ならば $W(c_{i-1}) = W(c_i)$」と「$R_{g_0}(c_{i-1}, c_i) = 1$ ならば $W(c_{i-1}) = W(c_i) + 1$」を証明すればよい．c の添え字がうるさいので，改めて $a = c_{i-1}$, $b = c_i$ と書くことにする．

(Step 3) $R_{g_0}(a, b) = 0$ ならば $W(a) = W(b)$ であることを示す．

$g_i(x) = 0$ $(0 \leqq \exists i \leqq s)$ を満たす $a < x < b$ はないのだから，開区間 (a, b) 上では $W(x) = V(g_0(y),\ldots, g_s(y))$ の値は一定である．$\#\big(R \cap [a, b]\big) \leqq 1$ であったから，$g_i(a) = 0$ $(1 \leqq \exists i \leqq s-1)$ または $g_i(b) = 0$ $(1 \leqq \exists i \leqq s-1)$ の場合を考えればよい．(そうでなければ $W(a) = W(x) = W(b)$ となる.)

$g_i(a) = 0$ と仮定する．もし $g_{i+1}(a) = 0$ ならば，$g_i(a) = g_{i+1}(a)q_{i+1}(a) - g_{i+2}(a)$ より，$0 = g_i(a) = g_{i+1}(a) = g_{i+2}(a) = \cdots = g_s(a) \neq 0$ となり矛盾する．よって，$g_{i-1}(a) \neq 0$, $g_{i+1}(a) \neq 0$ である．

$1 \leqq j < s$ に対して $W_j(x) = V\big(g_{i-1}(x),\, g_i(x),\, g_{i+1}(x)\big)$ とおく．$x \in (a, b)$ とし，$W_j(x) = W_j(a)$ が任意の j について成立すれば，$W(x) = W(a)$ が成り立つ．$g_j(a) \neq 0$ のときは $W_j(x) = W_j(a)$ である．

$g_i(a) = 0$ のとき，$g_{i-1}(a) = g_i(a)q_i(a) - g_{i+1}(a) = -g_{i+1}(a)$ だから，$g_{i-1}(a)g_{i+1}(a) < 0$ である．よって，$g_{i-1}(x)g_{i+1}(x) < 0$ であり，

$$W_i(a) = V\big(g_{i-1}(a),\, g_i(a),\, g_{i+1}(a)\big) = V\big(g_{i-1}(a),\, g_{i+1}(a)\big) = 1 = V\big(g_{i-1}(x),\, g_i(x),\, g_{i+1}(a)\big) = W_i(x)$$

である．

$g_i(b) = 0$ の場合の証明も同様である．

(Step 4) $R_{g_0}(a, b) = 1$ ならば $W(a) = W(b) + 1$ であることを示す．$R_{g_0}(a, b) = 1$ は (II) の場合にのみ有り得る．

$g_0(c) = 0$, $a < c < b$ を満たす $c \in K$ がただ 1 つ存在する．$a \leqq x \leqq b$ ならば $\operatorname{sign} g_0(x)g_1(x) = \operatorname{sign}(x - c)$ である．特に，区間の両端 $x = a,\, b$ で $g_0(x) \neq 0$, $g_1(x) \neq 0$ である．閉区間 $[a,\, b]$ 上に $g_i(x) = 0$ $(\exists i \geqq 2)$ を満たす x はないから，$y \in [a,\, c)$ に対して $W(y) = V(g_0(y),\ldots, g_s(y))$ の値は一定である．同様に $z \in (c,\, b]$ に対して $W(z)$ の値は一定で，$\operatorname{sign} g_0(x)g_1(x) = \operatorname{sign}(x - c)$ より，$W(a) = W(y) = W(z) + 1 = W(b) + 1$ である． □

定理 12.4.(Sturm の定理) K は実閉体，$f(X) \in K[X]$ は定数でない多項式とし，$f(X)$ の基準列を $f_0(X),\ldots, f_s(X)$ とする．各 $c \in K$ に対し $V_f(c) := V(f_0(c),\ldots, f_s(c))$ (符号変化の数) とおく．また，$a,\, b \in K$, $a < b$ で $f(a) \neq 0$, $f(b) \neq 0$ とする．このとき，

$$R_f(a, b) = V_f(a) - V_f(b)$$

が成り立つ．

証明. $f_s(X) = \mathrm{GCD}(f_0(X),\, f_1(X))$ であるので $f_s(a) \neq 0$, $f_s(b) \neq 0$ である．以下，$\dfrac{d}{dX}g(X)$ を $g'(X)$ で表す．ユークリッドの互除法の過程を考察すれば，任意の $0 \leqq i < s$ に対し，$\mathrm{GCD}(f_i(X),\, f_{i+1}(X)) = f_s(X)$ が成り立つ．よって，$f_i(X)$ は $f_s(X)$ の倍数で，$f_i(X) = g_i(X)f_s(X)$ $(\exists g_i(X) \in K[X])$ と書ける．

$g_0(X),\ldots, g_s(X)$ は前補題の条件 (1) 〜 (5) を満たすことを確認しよう．

$f_{i-1}(X) = f_i(X)q_i(X) - f_{i+1}(X)$ を満たす $q_i(X) \in K[X]$ を取っておく．すると，(1) の $g_{i-1}(X) = g_i(X)q_i(X) - g_{i+1}(X)$ が成り立つ．

(2) の $g_s(X)$ は 0 でない定数多項式であることも，$g_s(X)$ の定義から自明．また，$g_0(X)$ の作り方から，$g_0(X)$ は重根を持たず，(4) も成立している．

$W(c) := V(g_0(c),\ldots, g_s(c))$ とおく．$f_i(c) = g_i(c)f_s(c)$ より，$f_s(c) \neq 0$ ならば $V_f(c) = W(c)$ が成り立つ．$g_0(X)$ は $f(X)$ の約数なので，(3) の $g_0(a) \neq 0$, $g_0(b) \neq 0$ が成り立つ．

(i) $g_0(c) = 0$, $a < c < b$ ならば十分小さな $\varepsilon > 0$ $(\varepsilon \in K)$ を取れば $c - \varepsilon < x < c + \varepsilon$ のとき $\operatorname{sign} g_0(x)g_1(x) = \operatorname{sign}(x - c)$ となることを示す．

$X = c$ が $f(X)$ の r 重根であるとすると，$f_s(X) = (X - c)^{r-1}h_s(X)$ $(\exists h_s(X) \in K[X],\, h_s(c) \neq 0)$ と書ける．$g_0(X) = (X - c)h_0(X)$ $(\exists h_0(X) \in K[X])$ とおくと．$f(X) = (X - c)^r h_0(X)h_s(X)$,

$$f'(X) = (X - c)^{r-1}\big(rh_0(X)h_s(X) + (X - c)(h_0'(X)h_s(X) + h_0(X)h_s'(X))\big) = (X - c)^{r-1}g_1(X)h_s(X)$$

となる．$rh_0(X)h_s(X)+(X-c)\big(h_0'(X)h_s(X)+h_0(X)h_s'(X)\big)=g_1(X)h_s(X)$ なので，$\operatorname{sign}h_0(c)=\operatorname{sign}g_1(c)$ である．$g_0(X)$ は重根も持たないから，$h_0(c)\neq 0$ で，$\operatorname{sign}g_0(x)=\operatorname{sign}(x-c)h_0(x)$ である．$c-\varepsilon<x<c+\varepsilon$ のとき，$\operatorname{sign}g_1(x)=\operatorname{sign}g_1(c)=\operatorname{sign}h_0(c)$ だから，$\operatorname{sign}g_0(x)g_1(x)=\operatorname{sign}(x-c)h_1(c)^2=\operatorname{sign}(x-c)$ となり，(i) が成立する．

以上で $g_0(X),\ldots,g_s(X)$ は前補題の条件 (1) 〜 (5) を満たすことがわかった．よって，$R_{g_0}(a,b)=W(a)-W(b)$ が成り立つ．

$g_0(X)$ が重根を持たないから，$V_f(a)=W(a)$, $V_f(b)=W(b)$ である．また，$f_s(c)=0$ ならば $f(c)=f'(c)=0$ であるから，$X=c$ は $f(X)$ の重根であり，$g_0(c)=0$ となる．よって，$R_f(a,b)=R_{g_0}(a,b)$ が成り立つ．よって，$R_f(a,b)=R_{g_0}(a,b)=W(a)-W(b)=V_f(a)-V_f(b)$ である． □

命題 12.5. K は実閉体，$a,b\in K$, $a<b$ とする．$f(X)\in K[X]$ は定数でない多項式とし，$f(a)\neq 0$, $f(b)\neq 0$ を満たすとする．また，導関数 $f'(X)$ は任意の $a<x<b$ に対して $f'(x)\neq 0$ を満たすとする．すると，$f(x)=0$, $a<x<b$ を満たす $x\in K$ は高々1 個しか存在しない．

証明. ある $0<\varepsilon<(b-a)/2\in K$ を選んで，$[a,\,a+\varepsilon]$ および $[b-\varepsilon,\,b]$ 上には $f(X)$ の根は存在しないようにしておく．定理 12.4 の証明ように $g_0(X),\ldots,g_s(X)$ を作る．$a<x<b$ に対して $f'(x)\neq 0$ だから，$R_{g_1}(a+\varepsilon,\,b-\varepsilon)=0$ である．$R_{g_0}(a,\,b)\leqq 1$ を証明すればよい．最初の $g_0(X)$ を取り除いた多項式列 $g_1(X),\ldots,g_s(X)$ を考え，$W'(c):=V(g_1(c),\,g_2(c),\ldots,\,g_s(c))$ とおく．$\operatorname{sign}g_0(c)=\operatorname{sign}g_1(c)$ ならば $W(c)=W'(c)$, $\operatorname{sign}g_0(c)\neq\operatorname{sign}g_1(c)$ ならば $W(c)=W'(c)+1$ である．

$g_1(X),\ldots,\,g_s(X)$ を補題 12.3 の $g_0(X),\ldots,\,g_s(X)$ と考えるとき，(1) 〜 (4) を満たしているので，$R_{g_1}(a+\varepsilon,\,b-\varepsilon)=0$ から，$W'(a+\varepsilon)=W'(b-\varepsilon)$ が成り立つ．定理 12.4 より $W(a+\varepsilon)\geqq W(b-\varepsilon)$ なので，$W(a+\varepsilon)-W(b-\varepsilon)\leqq 1$ である．定理 12.4 より $W(a+\varepsilon)=W(a)=V_f(a)$, $W(b-\varepsilon)=V_f(b)$ なので，$R_f(a,\,b)=V_f(a)-V_f(b)\leqq 1$ である． □

命題 12.6. K は実閉体，$f(X)\in K[X]$ は定数でない多項式とし，また，$f(X)$ は重根を持たないと仮定する．また，$f'(X)=0$ の K 内の根全体の集合を $\alpha_1<\alpha_2<\cdots<\alpha_r$ とする．M を命題 11.6 のように定め，$\alpha_0<\min\{-M,\,\alpha_1\}$, $\alpha_{r+1}>\max\{M,\,\alpha_r\}$ を満たす $\alpha_0,\,\alpha_{r+1}\in K$ を 1 つ選んでおく．すると，$f(X)=0$ の K における根全体は $r+1$ 個以下で，各 $i=0,\,1,\ldots,\,r$ に対し $\alpha_i<x<\alpha_{i+1}$ を満たす $f(X)=0$ の根 x は高々1 個しか存在しない．

証明. $f(X)$ の基準列を $f_0(X),\ldots,\,f_s(X)$ とする．$f(X)$ と $f_1(X)=f'(X)$ は共通根を持たないから，$f(\alpha_i)\neq 0$ $(0\leqq\forall i\leqq r+1)$ である．すると，前命題から $\alpha_i<x<\alpha_{i+1}$ を満たす $f(X)=0$ の根 x は高々1 個しか存在しない． □

定理 12.7. K, L は順序体，K^*, L^* はそれらの実閉包とする．また $\varphi\colon K\to L$ は順序を保つ中への体の同型写像とする．このとき，順序を保つ中への体の同型写像 $\varphi^*\colon K^*\to L^*$ で $\varphi^*|_K=\varphi$ を満たすものが一意的に存在する．

証明. 一般に，$f(X)=c_nX^n+c_{n-1}X^{n-1}+\cdots+c_1X+c_0\in K[X]$ に対し，$\varphi(f(X))=\varphi(c_n)X^n+\varphi(c_{n-1})X^{n-1}+\cdots+\varphi(c_1)X+\varphi(c_0)\in L[X]$ と書く．$\varphi(f(X))$ は $(\varphi(f))(X)$ とも書く．$f(X)$ が K^* で重根を持たないとき，$\varphi(f(X))$ も L^* で重根を持たない．

さて，$a\in K^*$ の K 上の最小多項式 $f_a(X)$ を書くことにし，今，$f_a(X)=0$ の K^* 内での解全体を $\alpha_1<\alpha_2<\ldots<\alpha_m$, $\varphi(f_a(X))=0$ の L^* 内での解全体を $\beta_1<\beta_2<\ldots<\beta_m$ とおく．$a=\alpha_k$ $(1\leqq\exists k\leqq m)$ なので，$\varphi^*(a)=\beta_k$ によって写像 $\varphi^*\colon K^*\to L^*$ を定める．この定義によると，任意の $i=1,\ldots,\,m$ に対し $\varphi^*(\alpha_i)=\beta_i$ となることに注意する．$a\in L$ ならば $f_a(X)=X-a$, $\varphi(f_a(X))=X-\varphi(a)$ だから，$\varphi^*(a)=\varphi(a)$ で，$\varphi^*|_K=\varphi$ である．

(1) 上の φ^* が準同型写像であることを示す．$a,\,b\in K$ に対し $a,\,b,\,a+b,\,ab$ の K 上の最小多項式 $f_a(X)$, $f_b(X)$, $f_{(a+b)}(X)$, $f_{ab}(X)$ に対し，$\varphi(f_a)(X)$, $\varphi(f_b(X))$, $\varphi(f_{(a+b)}(X))$, $\varphi(f_{ab}(X))$ の L^* 内での根の大小関係を考えれば，$\varphi^*(a+b)=\varphi^*(a)+\varphi^*(b)$, $\varphi^*(ab)=\varphi^*(a)\varphi^*(b)$ が成り立つことがわかる．よって，$\varphi^*\colon K^*\to L^*$ は環準同型写像であり，体として中への同型写像である．

(2) $a,\,b\in K^*$, $a<b$ ならば $\varphi^*(a)<\varphi^*(b)$ であることを示す．

$\sqrt{b-a} \in K^*$ なので，$\varphi^*(b-a) = \big(\varphi^*(\sqrt{b-a})\big)^2 > 0$ である．よって，$\varphi^*(b) > \varphi^*(a)$ である．以上より，$\varphi^*\colon K^* \to L^*$ は順序を保つ中への体の同型写像である．

(3) 一意性を証明する．$\psi\colon K^* \to L^*$ も順序を保つ中への体の同型写像で $\psi|_K = \varphi$ を満たすとする．

$a \in K^*$ の最小多項式を $f_a(X)$ とするとき，$(\varphi(f_a))(\psi(a)) = \varphi(f_a(a)) = 0$ である．このことから，$f_a(X) = 0$ の K^* 内での解全体を $\alpha_1 < \alpha_2 < \ldots < \alpha_m$ とするとき，$\psi(\alpha_1) < \psi(\alpha_2) < \ldots < \psi(\alpha_m)$ は $(\varphi(f_a))(X) = 0$ の L^* 内での解全体と一致する．よって，前の記号で $\beta_i = \psi(\alpha_i)$ $(1 \leqq \forall i \leqq m)$ であり，$\psi(a) = \psi(\alpha_k) = \beta_k = \varphi^*(\alpha_k) = \varphi(a)$ となる． □

13. 半代数的集合

定義 13.1. K は順序体，$R \subset K$ は部分整域とする．ある $n \in \mathbb{N}$ と $m_1,\ldots, m_n \in \mathbb{N}$ と，n 変数多項式 $f_{i,j} \in R[X_1,\ldots, X_n]$ および不等号または等号 $*_{i,j} \in \{>, =\}$ をうまく選んで，

$$A = \bigcup_{i=1}^{n} \bigcap_{j=1}^{m_i} \big\{(a_1,\ldots,a_n) \in K^n \;\big|\; f_{i,j}(a_1,\ldots,a_n) *_{i,j} 0\big\}$$

と表せる集合 A を K^n 内の R-係数の**半代数的集合**という．$R = K$ の場合には「K-係数の」という語は省略する．

さらに，K を含む実閉体 L に対し，

$$A \otimes_K L := \bigcup_{i=1}^{n} \bigcap_{j=1}^{m_i} \big\{(a_1,\ldots,a_n) \in L^n \;\big|\; f_{i,j}(a_1,\ldots,a_n) *_{i,j} 0\big\}$$

と書くことにする．

以下，次回証明する Tarski-Seidenberg の定理のための準備をしておく．

K は実閉体とする．$E := \{-1,\ 0,\ 1\}$ とし，$a \in K$ に対し，$a > 0$ なら $\mathrm{sign}(a) = 1$, $a = 0$ なら $\mathrm{sign}(a) = 0$, $a < 0$ なら $\mathrm{sign}(a) = -1$ と約束する．d を非負整数，s は自然数とする．E の元を成分とする s 行 $2N+1$ 列の行列全体の集合を $\widehat{W}_{s,N}$ とし，$W_{s,d} = \bigsqcup_{N=0}^{sd} \widehat{W}_{s,N}$ とおく．一般に，d 次以下の 1 変数多項式 $0 \neq f_i(X) \in K[X]$ $(i = 1,\ldots,\ s)$ に対して，E の元を成分とする行列 $S(f_1,\ldots,\ f_s)$ を以下のように定義する．まず，$f_1,\ldots,\ f_s$ のうちゼロ多項式以外の K 内での根全体を $\alpha_1 < \alpha_2 < \cdots < \alpha_N$ とする．形式的に，$\alpha_0 = -\infty$, $\alpha_{N+1} = +\infty$ とおく．各開区間 $I_k := (\alpha_k,\ \alpha_{k+1})$ $(k = 0,\ldots,\ N)$ 上では，$\mathrm{sign}(f_i(X))$ は一定であるので，その値を $\mathrm{sign}(f_i(I_k)) \in E$ と定める．$p_{i,k} := \mathrm{sign}(f_i(I_k))$, $q_{i,k} := \mathrm{sign}(f_i(\alpha_k))$ とし，符号を並べた長さ $2s+1$ の行ベクトル $S(f_i)$ を

$$S(f_i) := \big(p_{i,0},\ q_{i,1},\ p_{i,1},\ q_{i,2},\ p_{i,2},\ \ldots,\ p_{i,N-1},\ q_{i,N},\ p_{i,N}\big)$$

と定める．行ベクトル $S(f_1),\ldots,\ S(f_s)$ を縦に並べてできる s 行 $2N+1$ 列の符号の行列を $S(f_1,\ldots,\ f_s)$ と書く．ここで，$N \leqq sd$ だから，$S(f_1,\ldots,\ f_s) \in W_{s,d}$ である．

$K = \mathbb{R}$ の場合に次の補題を証明する．

補題 13.2. 写像 $\varphi : W_{2s,d} \longrightarrow W_{s,d}$ で以下の条件 $(*)$ を満たすものが存在する．

$(*)$ $h,\ f_2,\ldots,\ f_s \in \mathbb{R}[X] - \{0\}$ が d 次以下の多項式で $\deg h \geqq 1$ であるならば，h を $h',\ f_2,\ldots,\ f_s$ で割った余りをそれぞれ $r_1,\ldots,\ r_s$ とするとき，

$$S(h, f_2,\ldots,f_s) = \varphi\big(S(h', f_2,\ldots,f_s, r_1,\ldots,r_s)\big)$$

が成り立つ．ここで，$h' = \dfrac{d}{dX}h(X)$ である．

証明. $w \in \widehat{W}_{2s,N} \subset W_{2s,d}$ をとる．w の $(i,\ j)$-成分を w_{ij} $(1 \leqq i \leqq 2s,\ 1 \leqq j \leqq 2N+1)$ とする．$w = S(h',\ f_2,\ldots,\ f_s,\ r_1,\ldots,\ r_s)$ を満たす d 次以下の $h,\ f_2,\ldots,\ f_s \in \mathbb{R}[X] - \{0\}$ が存在しないときは $\varphi(w)$ の値はどのように定めてもよいから，$w = S(h',\ f_2,\ldots,\ f_s,\ r_1,\ldots,\ r_s)$ を満たす d 次以下の $h,\ f_2,\ldots,\ f_s \in \mathbb{R}[X] - \{0\}$ が存在する場合に，$w = S(h',\ f_2,\ldots,\ f_s,\ r_1,\ldots,\ r_s)$ を満たす $h,\ f_2,\ldots,\ f_s$ の選び方に依存せずに，$\varphi(w)$ の値を定理の結論を満たすように定めることができることを示せばよい．

考察として，h', f_2,..., f_s, r_1,..., r_s の $\mathbb{R}$ 内での根全体が $\alpha_1 < \alpha_2 < \cdots < \alpha_N$ であったと仮定してみよう．形式的に $f_1 = h'$ とおく．$1 \leqq p \leqq s$ に対し，$w_{p,2i} = 0$ であることと $f_p(\alpha_i) = 0$ は同値である．そこで

$$A := \left\{ i \;\middle|\; 1 \leqq i \leqq N \text{ で，ある } 1 \leqq p \leqq s \text{ に対し } w_{p,2i} = 0 \right\}$$

とおき，$L = \#A$ とし，A の元全体を $i_1 < \cdots < i_L$ とおく．$\alpha_{i_1} < \cdots < \alpha_{i_L}$ が h', f_2,..., f_s の根全体である．

(I) $L = 0$ の場合．$f_1 = h'$, f_2,..., f_s は根を持たず，w の各行は定符号 ($w_{ij} = \varepsilon_i \in E$) である．すると h は単調増加または単調減少な多項式だから，根 α を 1 個だけ持ち $N = 1$ である．v の 1 行目は $(-\varepsilon_1, 0, \varepsilon_1)$ で，i 行目 $(2 \leqq i \leqq s)$ は $(\varepsilon_i, \varepsilon_i, \varepsilon_i)$ である．このように定まる v を用いて $\varphi(w) = v$ と定めればよい．

(II) 以下，$L \geqq 1$ の場合を考える．今 $k \in \{1,..., L\}$ が与えられたとき $w_{p,2i_k} = 0$ を満たす $p \in \{1,..., s\}$ が存在する．この p を $p(k)$ と書く．$p = p(k)$ のとき $f_p(\alpha_{i_k}) = 0$ である．$h = q_p f_p + r_p$ ($\exists q_p \in \mathbb{R}[X]$) なので，$h(\alpha_{i_k}) = r_p(\alpha_{i_k})$ が成り立つ．よって，$\mathrm{sign}(h(\alpha_{i_k})) = w_{s+p(k),i_k}$ である．後の便宜上，$u_{i_k} := w_{s+p(k),i_k}$ とおく．

以下，h の根のある場所をさがそう．

(1) 区間 $I_0 := (-\infty, \alpha_{i_1})$ では，$\mathrm{sign}(h'(X)) = w_{1,1} = w_{1,2} = \cdots = w_{1,i_1-2} \neq 0$ である．よって，I_0 上の h の根は高々1 個である．$\mathrm{sign}(h(\alpha_{i_1})) = u_{i_1}$ である．$w_{1,1}u_{i_1} = 1$ のとき $m_0 := 1$, それ以外のとき $m_0 := 0$ と定める．例えば $w_{1,1} = u_{i_1} = 1$ だと, 多項式 h は I_0 で単調増加だから，$x << 0$ のとき $h(x) < 0$ で，$h(\alpha_{i_1}) > 0$ だから，I_0 上に h の根が重複度を込めて丁度 1 個ある．$w_{1,1} = u_{i_1} = -1$ のときも同様．$w_{1,1}u_{i_1} \neq 1$ のとき I_0 上に h の根がないことも，同様な考察でわかる．

(2) 区間 $I_k := (\alpha_{i_k}, \alpha_{i_{k+1}})$ $(1 \leqq k \leqq L-1)$ 上では，$u_{i_k}u_{i_{k+1}} = -1$ のとき $m_k := 1$, それ以外のとき $m_k := 0$ と定める．$m_k = 1$ ならば $h(\alpha_{i_k})$ と $h(\alpha_{i_{k+1}})$ は異符号で，I_k 上で h は単調だから，命題 12.5 より I_k 上に h の根が重複度を込めて丁度 1 個ある．同様に $m_k = 0$ のときは，I_k 上に h の根はなり．

(3) 区間 $I_L := (\alpha_{i_N}, +\infty)$ 上では，$\mathrm{sign}(h'(x)) = w_{1,2N+1} \neq 0$ である．そこで，$u_{i_L}w_{1,2N+1} = 1$ のとき $m_L := 1$, それ以外のとき $m_L := 0$ と定めると，(1) の議論と同様に，$m_L = 1$ のときに限って I_L 上に h の根が 1 個ある．

(4) さて，

$$B_1 := \left\{ k \in \mathbb{Z} \;\middle|\; 0 \leqq k \leqq L \text{ かつ } m_k = 1 \right\}$$
$$B_2 := \left\{ i \in A \;\middle|\; w_{2,2i}w_{3,2i}\cdots w_{s,2i} = 0 \right\}$$

とおき，$M = \#B_1 + \#B_2$ とおく．h, f_2,..., f_s の相異なる根全体の個数は M である．B_1 の元 l を J_l と書く．B_2 の元 i はある $1 \leqq k \leqq L$ により $i = i_k$ と書ける．$i < J_l \Longleftrightarrow k \leqq l$, $J_l < i \Longleftrightarrow l < k$ とし，B_1, B_2 上では通常の順序で，$B := B_1 \sqcup B_2$ に順序を定める．B は全順序集合になる．B の元は h, f_2,..., f_s の相異なる根全体 $\beta_1 < \cdots < \beta_M$ に対応している．β_k に対応する B の元を $\psi(k)$ $(1 \leqq k \leqq M)$ と書くことにする．$\psi\colon \{1,..., M\} \to B$ は順序を保つ全単射である．$\psi(k) \in B_2$ なら $\beta_k = \alpha_{\psi(k)}$ であり，$\psi(k) = J_l \in B_1$ なら $\beta_k \in I_l$ である．

(5) さて，$v := \varphi(w)$ を定めよう．v は s 行 M 列行列とし，その (i, j)-成分を v_{ij} とする．

(i) $i = 1$ の場合．これは，h の符号変化に対応する行である．

もし，$\psi(k) \in B_2$ $(1 \leqq k \leqq M)$ ならば，$v_{1,2k} := u_{\psi(k)} = \mathrm{sign}(h(\alpha_{\psi(k)}))$ とおく．もし，$\psi(k) \in B_1$ ならば $h(\beta_k) = 0$ だから，$v_{1,2k} := 0$ とおく．

奇数列目については，まず，h の増減を考え，$v_{1,1} := -w_{1,1}$ とおく．$1 \leqq k \leqq M$ に対しては帰納的に以下のように定める．もし $v_{1,2k} \neq 0$ ならば β_k の前後で h の符号は変わらないので，$v_{1,2k+1} := v_{1,2k}$ とおく．$v_{1,2k} = 0$ の場合は $h(\beta_k) = 0$ なので以下のようにする．$\psi(k) \in B_1$ ならば，$h'(\beta_k) \neq 0$ だから，h のグラフは β_k で横断的に x 軸を横切る．そこで，$v_{1,2k+1} := -v_{1,2k-1}$ とおく．$\psi(k) \in B_2$ の場合は $\beta_k = \alpha_{\psi(k)}$ は h の重根なので少し難しい．もし，$w_{1,2\psi(k)-1}w_{1,2\psi(k)+1} = 1$ ならば，h は β_k を奇数重根にを持つから $v_{1,2k+1} := -v_{1,2k-1}$ とおく．もし，$w_{1,2\psi(k)-1}w_{1,2\psi(k)+1} = -1$ ならば，h は β_k を偶数重根にを持つから $v_{1,2k+1} := v_{1,2k-1}$ とおく．以上で，v の 1 行目が定まった．

(ii) $2 \leqq i \leqq s$ の場合．これは，f_i の符号変化に対応する行で，それは W の i 行目から簡単に決定できる．$1 \leqq k \leqq M$ に対し，もし $\psi(k) \in B_2$ ならば，$\beta_k = \alpha_{\psi(k)}$ だから，$v_{i,2k} := w_{i,2\psi(k)}$, $v_{i,2k-1} := w_{i,2\psi(k)-1}$, $v_{i,2k+1} := w_{i,2\psi(k)+1}$ とおけばよい．もし $\psi(k) \in B_1$ ならば $f_i(\beta_k) \neq 0$ なので，$\psi(k) = J_l$ とするとき，$v_{i,2k-1} = v_{i,2k} = v_{i,2k+1} := w_{i,2i_l+1}$ が $I_l \ni \beta_k$ 上での f_i の符号である．

(6) 以上のように v を定めるとき，$w = S(h', f_2,..., f_s, r_1,..., r_s)$ を満たす h, f_2,..., f_s の選び方に依存せずに v が定まっていることは，容易にわかるであろう． □

上の補題において h, f_2,..., $f_s \in \mathbb{Z}[X]$ ならば，h', r_1,..., $r_s \in \mathbb{Z}[X]$ であることに注意する．

14. Hilbert の第 17 問題

補題 14.1. K は実閉体とし，自然に $\mathbb{Z} \subset K$ と考える．

$$f_i(x, y_1, \ldots, y_n) = \sum_{k=0}^{m_i} h_{i,k}(y_1, \ldots, y_n) x^k \in \mathbb{Z}[x, y_1, \ldots, y_n] - \{0\}$$

($m_i = \deg_x f_i$; $i = 1$,..., s) とし，$d = \max\{m_1, \ldots, m_s\}$ とする．また，W は $W_{s,d}$ の部分集合とする．このとき，以下の条件を満たす $\mathbb{Z}$-係数の半代数的集合 $\mathcal{B}(W) \subset K^n$ が存在する．

$$S(f_1, \ldots, f_s) \in W \quad \Longleftrightarrow \quad (y_1, \ldots, y_n) \in \mathcal{B}(W)$$

ただし，S は y_1,..., y_n を定数と考え，f を x の多項式とみなして定義する．

証明. $m_1 \geqq \cdots \geqq m_s$ と仮定してよい．

非負整数が降順に並んだ有限列全体の集合を A とし，A に辞書式順序を以下のように定義する．$K = (k_1 \geqq k_2 \geqq \cdots \geqq k_s)$, $L = (l_1 \geqq l_2 \geqq \cdots \geqq l_t)$ とし，$k_1 = l_1$,..., $k_{r-1} = l_{r-1}$, $k_r > l_r$ ($\exists r \in \mathbb{N}$) であるとき $K > L$ であると定義する．すると，A は整列集合になるので，超限帰納法が使える．

$M := (m_1, \ldots, m_s) \in A$ に関する超限帰納法で証明する．

M が A の極小元の場合は，$m_1 = \cdots = m_s = 0$ で，$f_i = h_{i,0}(y_1, \ldots, y_n)$ だから，連立不等式 $S(h_{1,0}, \ldots, h_{s,0}) \in W$ によって定まる半代数的集合を $\mathcal{B}(W)$ とすればよい．

$M > \min A$ の場合を考える．$\deg_x f_1 \geqq \cdots \geqq \deg_x f_s$ と仮定してよい．$M > \min A$ だから $\deg_x f_1 \geqq 1$ である．f_i 達は $\mathbb{Z}$-係数多項式だから，補題 13.2 を適用することができる．補題 13.2 の写像 $\varphi : W_{2s,d} \longrightarrow W_{s,d}$ を取り，$W' = \varphi^{-1}(W)$ とおく．すると，$S(f_1, \ldots, f_s) \in W$ と，$S(f_1', f_2, \ldots, f_s, r_1, \ldots, r_s) \in W'$ は同値となる．$(\deg_x f_1', \deg f_2, \ldots, \deg_x f_s, \deg_x r_1, \ldots, \deg_x r_s)$ を降順に並べ替えた順列 L は A の中で M より小さいから，帰納法の仮定によって，

$$S(f_1', \ldots, r_s) \in W' \quad \Longleftrightarrow \quad (y_1, \ldots, y_n) \in \mathcal{B}(W')$$

を満たす半代数的集合 $\mathcal{B}(W')$ が存在する．そこで，$\mathcal{B}(W) = \mathcal{B}(W')$ とおけばよい． □

定理 14.2.(Tarski-Seidenberg の定理) K は実閉体とし，L は順序体であって K の拡大体であるとする．正射影 $\pi_L : L^{n+r} \to L^n$ を $\pi_L(a_1, \ldots, a_{n+r}) = (a_1, \ldots, a_n)$ で定める．

(1) A が K^{n+r} の内の $\mathbb{Z}$-係数の半代数的集合ならば，$\pi_K(A)$ も K^n 内の $\mathbb{Z}$-係数の半代数的集合である．

(2) A は K^{n+r} の内の K-係数の半代数的集合であるとする．すると，ある $m_1, \ldots, m_n \in \mathbb{N}$ と，ある n 変数多項式 $g_{i,j} \in K[x_1, \ldots, x_n]$ および不等号または等号 $*_{i,j} \in \{>, =\}$ をうまく選べば，

$$\pi_L(A \otimes_K L) = \bigcup_{i=1}^{n} \bigcap_{j=1}^{m_i} \left\{ (a_1, \ldots, a_n) \in L^n \;\middle|\; g_{i,j}(a_1, \ldots, a_n) *_{i,j} 0 \right\}$$

が成り立つ．言い替えれば，$\pi_L(A \otimes_K L) = \pi_K(A) \otimes_K L$ が成り立つ．

(3) A が K^{n+r} の内の K-係数の半代数的集合ならば，$\pi_K(A)$ も K^n 内の K-係数の半代数的集合である．

証明. (1) $r = 1$ の場合を考える．$\pi_K(x, y_1, \ldots, y_n) = (y_1, \ldots, y_n)$ と仮定しておく．ある f_1,..., $f_s \in \mathbb{Z}[x, y_1, \ldots, y_n]$ と，ε_1,..., $\varepsilon_s \in E = \{-1, 0, +1\}$ によって，

$$A = \left\{ (x, y_1, \ldots, y_n) \in K^{n+1} \;\middle|\; \operatorname{sign}(f_i(x, y_1, \ldots, y_n)) = \varepsilon_i \ (i = 1, \ldots, s) \right\}$$

と書ける場合に証明すれば十分である．ε_1,..., ε_s を縦に並べた列ベクトルを ε とする．$A \in W_{s,d}$ で A の少なくとも 1 つの列ベクトルが ε と一致するような A 全体の集合を W とする．このとき，$\pi_K(A) = \mathcal{B}(W)$ であり，補題 14.1 より，これは K^n 内の $\mathbb{Z}$-係数の半代数的集合である．

$r \geqq 2$ の場合は，$\pi_i : K^{n+i} \longrightarrow K^{n+i-1}$ ($i = 1, \ldots, r$) を $\pi_i(a_1, \ldots, a_{n+i}) = (a_1, \ldots, a_{n+i-1})$ で定まる正射影とし，$\pi_K = \pi_1 \circ \pi_2 \circ \cdots \circ \pi_r$ と分解して考えれば，$r = 1$ の場合に帰着される．

(2) $A = \bigcup_{i=1}^{l} \bigcap_{j=1}^{k_i} \left\{ (b_1, \ldots, b_{n+r}) \in K^{n+r} \;\middle|\; f_{i,j}(b_1, \ldots, b_{n+r}) *'_{i,j} 0 \right\}$

($f_{i,j}(x_1, \ldots, x_{n+r}) \in K[x_1, \ldots, x_{n+r}]$, $*'_{i,n} \in \{>, =\}$) と表わせたとする．すべての $f_{i,j}(x_1, \ldots, x_{n+1})$

$(1 \leqq j \leqq k_i,\ 1 \leqq i \leqq l)$ に現れるすべての項の係数を適当な順序で 1 列に並べて $c_1,\ldots,\ c_N$ とし，$f_{i,j}$ に現れる係数 c_k を不定元 x_{n+r+k} $(1 \leqq k \leqq N)$ で置き換えてできる多項式を $F_{i,j}(x_1,\ldots,\ x_{n+r+N})$ とする．$F_{i,j}$ の各項の係数は 1 か 0 なので，$F_{i,j} \in \mathbb{Z}[x_1,\ldots,\ x_{n+r+N}]$ である．

$$\tilde{A} = \bigcup_{i=1}^{l} \bigcap_{j=1}^{k_i} \left\{(b_1,\ldots,b_{n+r+N}) \in K^{n+r+N} \;\middle|\; F_{i,j}(b_1,\ldots,b_{n+r+N}) *'_{i,j} 0\right\}$$

とおく．$\tilde{\pi}\colon L^{n+r+N} \to L^{N+n}$ を

$$\tilde{\pi}(a_1,\ldots,a_{n+r+N}) = (a_1,\ldots,a_n,a_{n+r+1},\ldots,a_{n+r+N})$$

で定める．(1) より，ある $n \in \mathbb{N}$ と $m_1,\ldots,\ m_n \in \mathbb{N}$ と，ある $G_{i,j} \in K[x_1,\ldots,\ x_{n+N}]$ および $*_{i,j} \in \{>, =\}$ をうまく選べば，

$$\tilde{\pi}(\tilde{A}) = \bigcup_{i=1}^{n} \bigcap_{j=1}^{m_i} \left\{(a_1,\ldots,a_{n+N}) \in K^{n+N} \;\middle|\; G_{i,j}(a_1,\ldots,a_{n+N}) *_{i,j} 0\right\}$$

となる．そこで，$x_{n+r+1},\ldots,\ x_{n+r+N}$ に $c_1,\ldots,\ c_N$ を代入して

$$g_{i,j}(x_1,\ldots,\ x_n) := G_{i,j}(x_1,\ldots,\ x_n,\ c_1,\ldots,\ c_N)$$

とおき，

$$A_L = \bigcup_{i=1}^{n} \bigcap_{j=1}^{m_i} \left\{(a_1,\ldots,a_n) \in L^n \;\middle|\; g_{i,j}(a_1,\ldots,a_n) *_{i,j} 0\right\}$$

とおけば，$\pi_L(A \otimes_K L) = A_L$ となる．

(3) は (2) で $L = K$ とした場合からわかる． □

定理 14.3.(Artin-Lang の定理) K と L は実閉体で L は K の拡大体であるとする．また，$A \subset K^n$ は K-係数の半代数的集合であるとする．このとき，もし $A \otimes_K L \neq \phi$ ならば $A \neq \phi$ である．

証明. n に関する帰納法で証明する．$n = 0$ ならば $K^0 = L^0 = \{0\}$ だから，$A \otimes_K L \neq \phi$ ならば $A = \{0\} \neq \phi$ である．

$n \geqq 1$ とし，$n-1$ まで定理は正しいと仮定する．$\pi_L\colon L^n \to L^{n-1}$ は正射影で，$\pi = \pi_L|_K\colon K^n \to K^{n-1}$ はその K^n への制限とする．$A \otimes_K L \neq \phi$ ならば $\pi_L(A \otimes_K L) \neq \phi$ である．Tarski-Seidenberg の定理より $\pi_L(A \otimes_K L) = \pi(A) \otimes_K L$ が成り立つ．すると，帰納法の仮定から $\pi(A) \neq \phi$ である．よって，$A \neq \phi$ である． □

定理 14.4.(Artin の定理) $f_1(x_1,\ldots,\ x_n)$, $f_2(x_1,\ldots,\ x_n)$ は互いに素な実数係数多項式で，$f(x_1,\ldots,x_n) = \dfrac{f_2(x_1,\ldots,x_n)}{f_1(x_1,\ldots,x_n)}$ とする．さらに，$f_1(a_1,\ldots,\ a_n) \neq 0$ であるような任意の有理数の組 $(a_1,\ldots,\ a_n)$ に対して $f(a_1,\ldots,\ a_n) \geqq 0$ が成り立つと仮定する．すると，ある自然数 r と，ある実数係数有理関数 $g_1(x_1,\ldots,\ x_n),\ \ldots,\ g_r(x_1,\ldots,\ x_n)$ が存在して，

$$f(x_1,\ldots,x_n) = \sum_{i=1}^{r} g_i(x_1,\ldots,x_n)^2$$

と書ける．さらに，$f_1,\ f_2$ が有理数係数多項式ならば，$g_1,\ldots,\ g_r$ を整数係数有理関数として選ぶことができる．

証明. 有理関数体 $K := \mathbb{R}(x_1,\ldots,\ x_n)$ は，$-1 \notin \Sigma(K)$ を満たすので実体である．

$f_0 := ff_1^2 = f_1f_2 \in K[x_1,\ldots,\ x_n]$ を考える．多項式の連続性から任意の $(a_1,\ldots,\ a_n) \in \mathbb{R}^n$ に対して $f_0(a_1,\ldots,\ a_n) \geqq 0$ である．もし，$f_0 = g_1^2 + \cdots + g_r^2$ $(\exists g_i \in K)$ が証明できれは，$f = (g_1/f_1)^2 + \cdots + (g_r/f_1)^2$ となるので，最初から f は多項式であると仮定してよい．

$f \notin \Sigma(K)$ と仮定して矛盾を導こう．定理 11.1 より，K の代数拡大体であるような実閉体 K^* で，K^* 上の順序で $f < 0$ となるようなものが存在する．定理 10.5(2) より，ある $h \in K^*$ により，$f = -h^2$ と書ける．

$$F(t_0,t_1,\ldots,t_n) := t_0^2 f(t_1,\ldots,t_n) + 1 \in \mathbb{R}[t_0,t_1,\ldots,t_n]$$
$$A := \left\{(a_0,a_1,\ldots,a_n) \in \mathbb{R}^{n+1} \;\middle|\; F(a_0,\ldots,\ a_n) = 0\right\}$$

とおく．$K^*(t_0,\ldots,t_n)$ においては，$F(1/h,x_1,\ldots,x_n)=0$ であるから，$A\otimes_K K^*\neq\phi$ である．Artin-Lang の定理より，$A\neq\phi$ となる．つまり，ある $a_0,\ldots,a_n\in\mathbb{R}$ が存在して，$a_0^2f(a_1,\ldots,a_n)+1=0$ となる．これより，$f(a_1,\ldots,a_n)<0$ となり，仮定に矛盾する．

f が $\mathbb{Z}$-係数の場合には，上の証明で $\mathbb{R}$ の部分を $\mathbb{Q}$ と書き換えれば，$f\in\Sigma\left(\mathbb{Q}(x_1,\ldots,x_n)\right)$ がわかる．$\mathbb{Q}(x_1,\ldots,x_n)$ の元は，整数係数多項式の商で表せる． □