Andre Weil「Basic Number Theory」

https://seasawher.hatenablog.com/

@seasawher

2018 年 11 月 12 日

Chapter I-1. Finite Fields

Theorem 1

> **引用.** each factor in the product $p(q) = \prod(q - \zeta)$ has an absolute value $> q - 1$

注意. 背理法の仮定 $n > 1$ はここで使う。

Lemma 1

> **引用.** there is a prime p and power $q = p^{\nu}$ of p such that q divides n and not N. Then one verifies at once that the order of $\alpha\beta^{\frac{n}{q}}$ is the l.c.m of N and q

注意. 有限生成 Abel 群の基本定理を使う手もあるが、ここでは本文通り示す。次を示せばよい。

命題. G は有限 Abel 群とする。G の元のうち最大の位数をもつものを α とし、その位数を N とする。任意に $\beta \in G$ をとり、β の位数を n とする。このとき、n は N を割り切る。

証明. 背理法による。n が N を割らないと仮定しよう。このとき、ある素数 p が存在して

$$\mathrm{ord}_p\, n > \mathrm{ord}_p\, N$$

が成り立つ。そこで $q = p^{\mathrm{ord}_p\, n}$ とおき、$\alpha\beta^{\frac{n}{q}}$ の位数を s、N と q の最小公倍数を l とおく。$(\alpha\beta^{\frac{n}{q}})^l = 1$ なので、s が l を割り切ることはあきらかである。

逆に、$(\alpha\beta^{\frac{n}{q}})^s = 1$ より、

$$\alpha^s = \beta^{-\frac{ns}{q}}$$

である。両辺の位数を考えて

$$\frac{N}{\gcd(s, N)} = \frac{n}{\gcd(\frac{ns}{q}, n)} = \frac{q}{\gcd(s, q)}$$

である。ゆえに

$$\mathrm{ord}_p\, n - \mathrm{ord}_p\, N = \min\{\mathrm{ord}_p\, s, \mathrm{ord}_p\, n\} - \min\{\mathrm{ord}_p\, s, \mathrm{ord}_p\, N\}$$

が成り立つ。s のオーダー $\mathrm{ord}_p\, s$ については

(1) $\mathrm{ord}_p\, s \leq \mathrm{ord}_p\, N$
(2) $\mathrm{ord}_p\, N < \mathrm{ord}_p\, s < \mathrm{ord}_p\, n$
(3) $\mathrm{ord}_p\, n \leq \mathrm{ord}_p\, s$

の三つの可能性がある。(1) は上の式の右辺が 0 になって矛盾。(2) は $\mathrm{ord}_p\, s = \mathrm{ord}_p\, n$ を導くので矛盾。したがって (3) が成り立ち、q は s を割り切る。そうすると $\alpha^s = \beta^{-\frac{ns}{q}} = 1$ より、N は s を割り切る。したがって最小公倍数の定義から、l は s を割ることがわかり、$s = l$ が言えた。l は N よりも大きいので、これは N の取り方に矛盾する。 □

Chapter I-2. The module in a locally compact field

Haar 測度の定義および基本的性質が [FANF][2] に載っている。参照のこと。

Lemma 2 直前

> **引用.** If G is discrete or compact, the first formula (applied to $X = \{0\}$, $X = G$, respectively) shows that the module is 1.

注意. Haar 測度は相対コンパクト集合の上で有限であり、空でない開集合の上で正の値をとる（[FANF][2] 命題 1-7）ことを用いる。

Lemma 2

> **引用.** Let G' be a closed subgroup of G, and λ an automorphism of G which induces on G' an automorphism λ' of G'. Put $G'' = G/G'$, and call λ'' the automorphism of G'' determined by λ modulo G'.

注意. G は Abel 群なので G/G' がふたたび群になり、商位相に関して演算は連続になる。G/G' が Hausdorff 空間になることは、G' が閉部分群であることから [FANF][2] 命題 1-4 により従う。

Lemma 2

> **引用.** In fact, it is well-known that one can choose Haar measures $\alpha, \alpha', \alpha''$ on G, G', G'' so as to have, for every continuous function f with compact support on G:
>
> $$\int_G f(x) d\alpha x = \int_{G''} \left(\int_{G'} f(x+y) d\alpha'(y) \right) d\alpha''(\dot{x})$$
>
> here $\dot{x}$ denotes the image of x in G''

注意. わからない。セミナーでは示さずに認めた。

Proposition 1

> **引用.** let W be a neighborhood of a such that $WX \subset U$.

注意. 後で使うことがあるので、次の補題の形で示す。なお、開近傍補題という名前は僕が勝手につけたもので、一般的なものではない。

命題. 開近傍補題
K は位相体、$U \subset K$ は開集合、$X \subset K$ はコンパクト集合で、$aX \subset U$ なる $a \in K$ があるとする。
　このとき、ある a の開近傍 W が存在して $WX \subset U$ を満たす。

証明. 積 $m\colon K \times K \to K$ による U の逆像 $m^{-1}(U) \subset K \times K$ は開集合である。積位相の定義により、

$$\{a\} \times X \subset m^{-1}(U) = \bigcup_{k \in B} (W_k \times X_k)$$

なる K の開集合 W_k, X_k がある。$x \in X$ とすれば、$(a, x) \in W_k \times X_k$ なる k が存在する。この W_k, X_k を W_x, X_x と書くことにする。そうすると

$$X \subset \bigcup_{x \in X} X_x$$

であるから、X のコンパクト性により有限個の $x_1, \ldots, x_i$ が存在して

$$X \subset \bigcup_{1 \leq s \leq i} X_{x_s}$$

が成り立つ。このとき $W = \bigcap_{1 \leq s \leq i} W_{x_s}$ とおくと有限個の共通部分であるから W は a の開近傍になっていて、

$$WX \subset \bigcap_{1 \leq s \leq i} W_{x_s} \quad \bigcup_{1 \leq s \leq i} X_{x_s} \subset U$$

となる。 □

Proposition 1

> **引用.** The function mod_K is continuous on K, and $\mathrm{mod}_K(ab) = \mathrm{mod}_K(a)\,\mathrm{mod}_K(b)$ for all $a \in K$, $b \in K$.

注意. 次のことが系として従うことに注意する。

命題. K を、離散的でない局所コンパクト (Hausdorff) 位相体とする。このとき K は第一可算である。とくに、K の位相は点列により特徴づけられる。

証明. $0 \in K$ のあるコンパクト近傍 V をとり固定する。そして $m \in \mathbb{N}$ に対し $u_m = B_{\frac{1}{m}} \cap V$ とする。mod_K の連続性により $B_{\frac{1}{m}} \subset K$ は閉集合なので、各 u_m はコンパクトである。このとき、$\{u_m\}_{m\in\mathbb{N}}$ が 0 の基本近傍系であることを示そう。

いま $0 \in K$ の開近傍 W が任意に与えられたとする。このとき

$$\bigcap_{m=1}^{\infty} (u_m \setminus W) = \emptyset$$

である。一方で $u_m \setminus W \subset V$ は閉集合であり、V はコンパクトであるので、集合族 $\{u_m \setminus W\}_{m\in\mathbb{N}}$ は有限交叉性を持たない。したがって、ある $N \in \mathbb{N}$ が存在して

$$\bigcap_{m=1}^{N} (u_m \setminus W) = u_N \setminus W = \emptyset$$

である。すなわち、$u_N \subset W$ がいえた。

□

Proposition 2

> **引用.** let W be a neighborhood of 0 such that $WV \subset V$.

証明. Int で集合の内部を表すことにする。V は 0 の近傍なので $0 \cdot V = \{0\} \subset \operatorname{Int} V$ であり、開近傍補題から

$$WV \subset \operatorname{Int} V \subset V$$

なる 0 の開近傍 W がある。 □

Proposition 2

> **引用.** As it is contained in the compact set V, it has the limit 0.

証明. 帰納的に、$\forall n\ r^n \in V$ であることに注意する。V における 0 の開近傍 A が与えられたとする。$A^c = V \setminus A$ は V の閉集合なのでコンパクト。よって mod_K の連続性により、$\mathrm{mod}_K(A^c) \subset \mathbb{R}$ はコンパクト、とくに閉である。したがって

$$0 < a < \inf_{x \in A^c} \mathrm{mod}_K(x)$$

なる実数 $a \in \mathbb{R}$ がある。このとき $V \cap B_a \subset A$ である。ゆえに、V において $\{V \cap B_m\}_{m>0}$ は 0 の基本近傍系をなす。したがって、$r^n \to 0$ である。 □

Proposition 2

> **引用.** Call X the closure of $V - (rV)$; clearly X is compact, and 0 is not in X;

証明. $X = \overline{V \setminus rV} = \overline{V \cap (rV)^c} \subset V \cap \overline{(rV)^c}$ であるから、X は V の閉集合。よって X はコンパクト。$0 \in X$ と仮定しよう。すると点列 $\{x_n\} \subset V \setminus rV$ であって、$x_n \to 0$ であるものがある。このとき

$$x_n \in V \quad r^{-1}x_n \in V^c$$

よって積の連続性により $0 = \lim(r^{-1}x_n) \in \overline{V^c}$ である。ここで $\operatorname{Int} V \subset V$ により $V^c \subset (\operatorname{Int} V)^c$ だから、$\overline{V^c} \subset (\operatorname{Int} V)^c$ となり $0 \in (\operatorname{Int} V)^c$ となって矛盾。ゆえに、X は 0 を含まない。 □

Corollary 1 of Proposition 2

> **引用.** The sets B_m, for $m > 0$, make up a fundamental sysytem of neighborhoods of 0 in K.

注意. 局所コンパクト Hausdorff 空間において、各点でコンパクトな近傍の全体は基本近傍系をなす ([内田][1]Thm24.1) ことに注意する。

Corollary 2 of Proposition 2

> **引用.** For $a \in K$, $\lim_{n\to+\infty} a^n = 0$ if and only if $\mathrm{mod}_K(a) < 1$.

証明. $\Rightarrow$ は連続性によりあきらか。$\Leftarrow$ は、Cor.1 より $\{B_m\}$ が 0 の基本近傍系であることを使えばあきらか。 □

Corollary 3 of Proposition 2

> **引用.** A discrete subfield of K is finite.

注意. 一般に位相空間 X の部分集合 Y について、$Y \subset X$ が離散部分集合 (空間) であるとは、Y に X の部分集合として相対位相を入れたとき、その位相が Y の離散位相であることをいう。このとき $Y \subset X$ が閉であるとは限らない。

本文には「Therefore L is a discrete subset of the compact set B_1, hence finite」と書いてあるが、一般にコンパクト集合の離散部分集合は有限とは限らない。反例は $I = [0, 1]$, $A = \{\frac{1}{n} \mid n \in \mathbb{Z}_{\geq 1}\}$ により与えられる。

「コンパクト集合の離散閉部分集合は有限集合」なら正しい。通常、離散部分集合と言われるものは閉でもあることが多いので、本文にはこう書いてあるのだろう。

証明. L は離散体であるので、$x \in L \setminus \{0\}$ について本文にある論法で $\mathrm{mod}_K(x) = 1$ がいえる。よって $L \subset B_1$ である。一般に、(Hausdorff) 位相群の局所コンパクト部分群は閉 ([FANF][2]Prop1.6) なので、$L \subset K$ は閉であり、したがって L はコンパクト離散集

合であることになる。よって L は有限集合。 □

Theorem 3

> **引用.** Hence there exists a neighborhood W of 0 in V, and a neighborhood of 0 in K which we may assume to be of the form B_ε with $\varepsilon > 0$, such that $B_\varepsilon W \subset V \setminus f(S)$

注意. $f(S)$ はコンパクトなので、$f(S) \subset V$ は閉集合。スカラー倍 $K \times V \to V$ は連続なので、$V - f(S)$ の逆像は $(0,0)$ を含む開集合である。よって積位相の定義により、

$$UW \subset V - f(S)$$

なる 0 の開近傍 $U \subset K$ と $W \subset V$ とがある。B_m は 0 の基本近傍系なので、示すべきことがいえる。

Corollary 2 of Theorem 3

> **引用.** If V is a locally compact topological vector-space over K, then V has a finite dimension d over K, and $\mathrm{mod}_V(a) = \mathrm{mod}_K(a)^d$ for every $a \in K$.

注意.

(1) μ を K の Haar 測度とするとき、K^d の直積測度 μ^d もまた Haar 測度となることに注意する。本文には Fubini's Theorem とあるが、この部分の意図は不明。示すべき等式は直積測度の定義から従う。

(2) $\mathrm{mod}_K \colon K \to \mathbb{R}$ の連続性を示す議論をそのまま繰り返すことにより、$\mathrm{mod}_V \colon K \to \mathbb{R}$ の連続性がいえる。これを用いなければ

$$\lim_{n\to\infty} a^n = 0 \;\Rightarrow\; \mathrm{mod}_V(a) < 1$$

が言えないのにも関わらず、本文には注意がないので注意しておく。

Corollary 2 of Theorem 3 直後

> **引用.** Fubini's theorem shows at once that every subspace of V of dimension $n' < n$ is of measure 0.

注意. 次を示せばよい。

命題. K は離散的でない局所コンパクト位相体であるとする。$n \geq 1$ は自然数、V は n 次元左位相ベクトル空間。とくに V は局所コンパクトである。このとき次が成り立つ。

(1) $n' < n$ なる $n' \in \mathbb{Z}$ について、V の n' 次元部分空間の V 上の測度は 0

(2) K-線形写像 $A\colon V \to V$ について $\mathrm{mod}_V A$ を定義できる。A が同型 (つまり同相) なら既に述べられたように定め、A が同型でなければ (送った先がゼロ集合なので)$\mathrm{mod}_V A = 0$ で定める。

証明. (1) があきらかでないと感じるかもしれない。(1) を示すには、積測度の定義により、K 上の Haar 測度 α に対して $\alpha(\{0\}) = 0$ を示せばよい。

$0 < \mathrm{mod}_K(r) < 1$ なる $r \in K$ をとる。$B(n) = r^n B_1$ とおくと

$$\alpha(B(n)) = \alpha(r^n B_1) = \mathrm{mod}_K(r)^n \alpha(B_1)$$
$$B(n) = B_{\mathrm{mod}_K(r)^n} \subset B(n-1) \subset \cdots \subset B(0) = B_1$$

が成り立つ。つまり、$B(n)$ は下降列であり、共通部分の測度は 0 である。ゆえに $\alpha(B_1) < \infty$ により、[伊藤][3]Thm6.2 から

$$\alpha(\{0\}) = \alpha(\bigcap_{n\geq 1} B(n)) = \inf_{n\geq 1} \alpha(B(n)) = 0$$

がいえた。 □

Corollary 3 of Theorem 3

> **引用.** for types (b) and (c), it follows from a straightforward application of Fubini's theorem, just as in classical analysis (where one proves the theorem for the case $K = \mathbb{R}$)

注意. (c) のケースだけ証明する。座標の入れ替え行列を適当に掛けることにより、A は 2 次行列と単位元の直和だと思うことができるので、A を 2 次行列だとしても一般性を失わない。そこである $c \in K$ があり

$$A = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$$

であると仮定する。あるコンパクト集合 $X \subset K$ をとる。このとき

$$\mu^{\otimes 2}(A(X^2)) = \int_{K^2} 1_{A(X^2)}(x,y)\, d\mu \otimes \mu(x,y)$$

Fubini の定理により

$$\begin{aligned} &= \int_K \int_K 1_{A(X^2)}(x,y)\, d\mu(x)\, d\mu(y) \\ &= \int_K \mu\{x \in K \mid (x,y) \in A(X^2)\}\, d\mu(y) \\ &= \int_K \mu\{x \in K \mid x = s + ct,\ y = t \quad s,t \in X\}\, d\mu(y) \\ &= \int_X \mu\{s + cy \mid s \in X\}\, d\mu(y) \end{aligned}$$

Haar 測度の不変性により

$$\begin{aligned} &= \int_X \mu(X)\, d\mu(y) \\ &= \mu^{\otimes 2}(X) \end{aligned}$$

であることから、示したいことが言えた。

Proposition 3

> **引用.** The function mod_K induces on $K^\times$ an open homomorphism of $K^\times$ onto a closed subgroup Γ of $\mathbb{R}_+^\times$.

注意. $\mathrm{mod}_K\colon K^\times \to \mathbb{R}_{>0}$ が開写像というのと、$\mathrm{mod}_K\colon K^\times \to \Gamma$ が開写像ということは違うので注意すること。(後者が正しい)

証明. $\Gamma' = \Gamma\{0\}$ とする。$m > 0$ をとると、

$$[0, m] \cap \Gamma' = \mathrm{mod}_K(B_m)$$

である。B_m はコンパクトなので、$[0, m] \cap \Gamma'$ もコンパクト。

$\Gamma' \subset \mathbb{R}_{\geq 0}$ が閉であることを示そう。点列 $\{a_n\} \subset \Gamma'$ と $a \in \mathbb{R}_{\geq 0}$ があり、$a_n \to a$ であったと仮定する。$\{a_n\}$ は Cauchy 列なので有界であり、$a_n \subset [0, M]$ なる $M > 0$ が存在する。ゆえに $\{a_n\} \subset [0, M] \cap \Gamma'$ であり、$[0, M] \cap \Gamma'$ はコンパクトなので $a \in \Gamma'$ でなくてはならない。よって、$\Gamma' \subset \mathbb{R}_{\geq 0}$ は閉。

ゆえに $\Gamma = \Gamma' \cap \mathbb{R}_{>0}$ より、$\Gamma \subset \mathbb{R}_{>0}$ も閉である。いま $U = \ker(\mathrm{mod}_K)$ により $U \subset K^\times$ を定める。

$\mathrm{mod}_K\colon K^\times \to \Gamma$ が開写像であることを示したいので、$1 \in K^\times$ の $K^\times$ における近傍 V と V の mod_K による像 V' に対して、V' が 1 の Γ における近傍であることをいいたい。背理法による。$1 \notin \mathrm{Int}\, V'$、つまり $1 \in \overline{\Gamma \setminus V'}$ と仮定する。

このとき点列 $\{\gamma_n\} \subset \Gamma \setminus V'$ であって、$\gamma_n \to 1$ であるものがある。$\gamma_n \subset \Gamma$ なので

$$\gamma_n = \mathrm{mod}_K(a_n)$$

なる $a_n \in K^\times$ が存在する。

$\mathrm{mod}_K \subset \mathbb{R}$ は Cauchy 列なので有界であり、したがって B_m のコンパクト性により、部分列をとれば $a_{n'} \to a$ なる $a \in K$ があるようにできる。mod_K の連続性により $\mathrm{mod}_K(a) = 1$ なので $a \in U$ である。UV は U の近傍であるので

$$n \geq N \to a_n \in UV$$

なる自然数 N が存在する。したがって

$$n \geq N \to \gamma_n \in \mathrm{mod}_K(V) = V'$$

となり矛盾。よって $1 \in \mathrm{Int}\, V'$ である。 □

Theorem 4

> **引用.** If (3) is valid for $A = 1$, then the image Γ of $K^\times$ under mod_K is discrete in $\mathbb{R}_+^\times$.

証明. $U = \mathrm{mod}_K^{-1}[0,1)$ とする。このとき $1+U \subset K^\times$ であることはあきらか。$\mathrm{mod}_K\colon K^\times \to \Gamma$ は開写像なので、$\mathrm{mod}_K(1+U) \subset \Gamma$ は開。したがって、ある $\mathbb{R}$ の開集合 V が存在して

$$\mathrm{mod}_K(1+U) = \Gamma \cap V \subset [0,1]$$

が成り立つ。とくに、1 を含む $\mathbb{R}$ の開区間 I が存在して

$$\{1\} \subset \Gamma \cap I \subset [0,1]$$

が成立する。

ここで $\{1\} \subset \Gamma$ が開集合でない、つまり任意の 1 を含む $\mathbb{R}$ の開区間 J に対して、$\{1\} \neq \Gamma \cap J$ と仮定する。このとき $1 \in \Gamma$ は Γ の集積点であり、ある $\{a_n\} \subset K^\times$ が存在して

$$\mathrm{mod}_k(a_n) \neq 1$$

$$\mathrm{mod}_K(a_n) \to 1$$

を満たす。このとき各 n に対して $\mathrm{mod}_K(a_n) > 1$ または $\mathrm{mod}_K(a_n) < 1$ のいずれかであるが、必要なら a_n^{-1} を考えることにより、$\forall n\ \mathrm{mod}_K(a_n) > 1$ としてよい。

I は $1 \in \mathbb{R}$ の開近傍なので

$$n \geq N \to \mathrm{mod}_K(a_n) \in I$$

なる $N \in \mathbb{Z}$ が存在する。このとき

$$n \geq N \to \mathrm{mod}_K(a_n) \in I \cap \Gamma \subset [0,1]$$

であるので矛盾。よって $\{1\} \subset \Gamma$ は開集合であり、任意の $a \in \Gamma$ について左からの積 $a\colon \Gamma \to \Gamma$ は同相なので $\Gamma \subset \mathbb{R}$ は離散集合。 □

Chapter I-3. Classification of locally compact fields

Lemma 3

引用. $f(m^k) = kf(m)$, $f(mn) \leq f(m) + f(n)$, $f(m+n) \leq a + \sup(f(m), f(n))$.

証明. いずれも場合分けすればわかる。

(1)

$$\begin{aligned} f(m^k) &= \begin{cases} 0 & (F(m) \leq 1) \\ k \log F(m) & (F(m) > 1) \end{cases} \\ &= kf(m) \end{aligned}$$

(2)

$$f(m) + f(n) - f(mn) = \begin{cases} 0 & (1 \leq \min(F(m), F(n)) \ ) \\ -\log F(n) & (F(m)^{-1} \leq F(n) \leq 1 \leq F(m) \ ) \\ \log F(m) & (F(n) \leq F(m)^{-1} \leq 1 \leq F(m) \ ) \\ \text{omitted} & \\ 0 & (\max(F(m), F(n)) \leq 1) \end{cases}$$

(3) $F(m) \geq F(n)$ としても一般性を失わない。

$$\begin{aligned} F(m+n) &\leq \sup(0, \log(AF(m))) \\ &\leq \sup(0, \log A + \log(F(m)) \end{aligned}$$

であるから、

$$f(m+n) - f(m) \leq \begin{cases} \log A & (\max(A^{-1}, 1) \leq F(m) \ ) \\ 0 & (F(m) \leq \min(A^{-1}, 1) \ ) \\ -\log F(m) & (1 \leq F(m) \leq A^{-1}) \\ \log A + \log F(m) & (A^{-1} \leq F(m) \leq 1) \end{cases}$$

が成り立つ。それぞれの場合に a で上から抑えられることは明らか。よって示せた。

□

Lemma 3

> **引用.** In this inequality, replace m by m^k, this does not change.....Now replace n by n^k, for $k \to +\infty$, we get.....

注意. 本文では何故か 2 回に分けているが、m、n を同時に m^k、n^k で置き換えたほうが見通しがよい。

Chapter I-4. Structure of p-fields

Theorem 6

> **引用.** Clearly every relatively compact subset of K which is closed under multiplication is contained in R;

証明. もし mod の値が 1 より大きい元を持てば、どんな部分列も収束しないような点列が作れてしまうため、コンパクト性に反する。 □

Theorem 6

> **引用.** let γ be the largest element of Γ which is < 1, and let $\pi \in K^\times$ be such that $\mathrm{mod}_K(\pi) = \gamma$. Clearly γ generates Γ;

証明. 背理法で示す。$\beta \in \Gamma \setminus \langle\gamma\rangle$ とする。必要なら逆数を考えることにより $\beta < 1$ と仮定してよい。γ の最大性により $\beta \leq \gamma$ である。よって $\beta\gamma^{-1} \leq 1$ となるが、仮定により $\beta\gamma^{-1} < 1$ である。したがって再び $\beta\gamma^{-1} \leq \gamma$ であることが判る。以下帰納的に、任意の n について $\beta\gamma^{-n} < 1$ となる。これは矛盾。 □

Theorem 6

> **引用.** as R is compact, $K = R/P$ is finite.

注意. 次の補題が成り立つことを認めればあきらか。

補題. 位相群 G, H があり $H \subset G$ とする。このとき次は同値。

(1) 位相空間 G/H は離散的

(2)　$H \subset_{\text{open}} G$

証明. [FANF][2] 命題 1-4(iv) を参照のこと。 □

Corollary 2 of Theorem 6

> **引用.** Let ξ be an element of P, other than 0; put $n = \text{ord}(\xi)$, and let A be a full set of representatives of the classes modulo P^n in R. Then, for all $v \in \mathbb{Z}$, every $x \in P^{nv}$ can be expressed in one and only one way in the form
>
> $$x = \sum_{i=v}^{+\infty} a_i \xi^i$$
>
> with $a_i \in A$ for all $i \geq v$.

証明. 本文通り $v = 0$ としてよい。$x \in R$ が与えられたとき、A の定義により

$$x \equiv a_0 \pmod{P^n}$$

なる $a_0 \in A$ がある。このとき $(x - a_0)/\xi \in R$ なのでさらに

$$\frac{x - a_0}{\xi} \equiv a_1 \pmod{P^n}$$

なる $a_0 \in A$ がある。したがって帰納的に次の式をみたす A の元 a_{N+1} がとれることがわかる。

$$\frac{x - \sum_{i=0}^{N} a_i \xi^i}{\xi^{N+1}} \equiv a_{N+1} \pmod{P^n}$$

以上により

$$x = \sum_{i=v}^{+\infty} a_i \xi^i$$

が成り立つ。

一意性を示そう。背理法による。すべては同じでない $a_i, b_i \in A$ が存在して

$$\sum_{i=v}^{+\infty} a_i \xi^i = \sum_{i=v}^{+\infty} b_i \xi^i$$

が成り立ったとする。このとき

$$\sum_{i=v}^{+\infty}(a_i - b_i)\xi^i = 0$$

が成り立つ。いま $a_i - b_i \neq 0$ なる最小の i を j とおく。すると

$$a_j - b_j = -\sum_{i>j}^{+\infty}(a_i - b_i)\xi^{i-j}$$

であるが、右辺は P^n の元であるのでこれは A の定義に反する。よって矛盾。

□

Corollary 4 of Theorem 6

> **引用.** Every automorphism of K (as a topological field) maps R onto R, P onto P, and has the module 1

証明. $f\colon K \to K$ を位相体としての同型とする。このとき $f(R) \subset R$ であることだけ示せば十分だが、R のコンパクト部分環としての最大性からこれはあきらか。 □

Corollary 5 of Theorem 6

> **引用.** and K' a division algebra over K.

注意. K' の K 上の拡大次数が有限という仮定を付け加える必要があるように思う。

Proposition 4

> **引用.** we see that the elements of R' of the form $\sum_{i=0}^{e-1} a_i \pi'^i$, with $a_i \in A$ for $0 \leq i \leq e-1$, make up a full set of representatives A' of the classes modulo P' in R'.

証明. $x \in R'$ が与えられたとする。このとき

$$\exists a_i \in A \quad x = \sum_{i=0}^{\infty} a_i \pi'^i$$

が成り立つ。したがって $y = \sum_{i=0}^{e-1} a_i \pi'^i \in R'$ とおけば $x - y \in P'^e$ である。ゆえに、$\left\{ \sum_{i=0}^{e-1} a_i \pi'^i \;\middle|\; a_i \in A \right\}$ の写像 $R' \to R'/P'^e$ による像は全体ということが判る。

また、すべては同じでないある $a_i \in A$, $b_i \in A$ が存在して

$$\sum_{i=0}^{e-1} (a_i - b_i) \pi'^i \in P'^e$$

が成り立ったと仮定する。ここで $a_i - b_i \neq 0$ が成り立つ最小の i を j とおくと

$$a_j - b_j + \sum_{i>j}^{e-1} (a_i - b_i) \pi'^{i-j} \in P'^{e-j}$$

であるので、A が R'/P' の完全代表系であったことに矛盾。 □

Proposition 4

> **引用.** This shows that $K' = K(\pi')$, and, for $v = 0$, it shows that $R' = R[\pi']$.

証明. $R' = R[\pi']$ であること: $v = 0$ の場合についての、本文における直前の議論により

$$\forall x \in R' \; \exists (\alpha_i) \in R \text{ s.t. } x = \sum_{i=0}^{e-1} \alpha_i \pi'^i$$

がわかるので $R' = R[\pi']$ が結論できる。

$K' = K(\pi')$ であること: 商体を考えることにより

$$K' = \operatorname{Frac} R' = K(\pi')$$

がわかる。 □

Corollary 1 of Proposition 4

> **引用.** they have the same module, so that the modular degree of K over K' is 1.

証明. K' と K は位相体として同型なので、それぞれの最大コンパクト部分環 R' と R も同型である。したがってその剰余体 k' と k も同型であり、ともに有限体だから $\#k' = \#k$ である。 □

Corollary 1 of Proposition 4

> **引用.** the degree of K over K' must be p or 1.

証明. 係数環が DVR(離散付置環) なので、アイゼンシュタインの判定法から。 □

Corollary 1 of Proposition 4

> **引用.** As $\mathrm{ord}_K(\pi) = 1$, π is not in K^p, so that $K \neq K'$.

証明. もし $\pi \in K^p$ ならば $\pi = \tau^p$ なる $\tau \in K$ がある。(R, P) を K の最大コンパクト部分局所環とすると、このとき $\tau \in P$ である。したがって $1 = \mathrm{ord}_K(\pi) = p\,\mathrm{ord}_K(\tau) \geq p$ となり矛盾。 □

Corollary 2 of Proposition 4

> **引用.** it is well-known, and easily proved, that, if K' is purely inseparable of degree $\leq p^n$ over K, it must be contained in $K^{p^{-n}}$.

証明. $x \in K'$ が与えられたとき、x の K 上の最小多項式は $X^{p^m} - a$ $(a \in K)$ という形である。ここで、次元についての仮定から $m \leq n$ であるので、したがってすべての $x \in K'$ について $x^{p^n} \in K$ である。よって $K' \subset K^{p^{-n}}$ がわかる。 □

参考文献

[1] 内田伏一『集合と位相』(裳華房, 1986)

[2] Dinakar Ramakrishnan, Robert J.Valenza『Fourier Analysis on Number Fields』(Springer, 1999)

[3] 伊藤清三『ルベーグ積分入門』(裳華房, 1963)