For Tutors

MeBio　数学テキスト

ヒルベルト記号のまとめ

—まとめ—

Edited by kamei

§ 1 定義

定義 1–1 $p=\infty$, 素数 とする．$a,\ b,\ c\in\mathbb{Q}_p$ に対して，±1 の値をとるヒルベルト記号 $(a,\ b)_p$ を

$$(a,\ b)_p=1 \iff ax^2+by^2=z^2 \text{ が } \mathbb{Q}_p\times\mathbb{Q}_p\times\mathbb{Q}_p \text{ に自明でない解を持つ}$$

注：$z=0$ である非自明な解を持つ場合，$z\neq 0$ である解も持つ．これは 2 次曲線と直線の交点を考えれば分かる．もっと一般に $ax^2+by^2=z^2$ が一点でも解を持てば，代数曲線として $\mathbf{P}^1(\mathbb{Q}_p)$ と双有理同値である．

一般化やコホモロジー的に扱うには次の定義の方がよいのだろう．

定義 1–2 $F=\mathbb{Q}_p,\ K=\mathbb{Q}_p(\sqrt{b})$ とおく．

$$(a,\ b)_p=1 \iff a\in \mathrm{N}_{K/F}K^\times$$

「加藤，黒川，斎藤　数論 I」では次のように定義している．

定義 1–3 p を素数とする．$a,\ b\in\mathbb{Q}^\times$ に対し $a=p^iu,\ b=p^jv$ $(i,\ j\in\mathbb{Z},\ u,\ v\in{\mathbb{Z}_p}^\times)$ とおく．$p\neq 2$ の場合

$$(a,\ b)_p=\left(\frac{(-1)^{ij}u^iv^j}{p}\right)$$

また $p=2$ のとき

$$(a,\ b)_2=(-1)^{\frac{r^2-1}{8}}\cdot(-1)^{\frac{u-1}{2}\cdot\frac{v-1}{2}}$$

無限素点では

$$(a,\ b)_\infty=\begin{cases}1 & a>0 \text{ または } b>0 \text{ のとき}\\ -1 & a<0 \text{ かつ } b<0 \text{ のとき}\end{cases}$$

「彌永　数論」では次のように定義している．

定義 1–4 k を代数体，$k_\mathfrak{p}$ をその素点 $\mathfrak{p}$ に関する完備化とする．$k_\mathfrak{p}\ni\zeta_n$ とする．$a\in {k_\mathfrak{p}}^*$ に対し $k_\mathfrak{p}(\sqrt[n]{a})$ が不分岐 Kummer 拡大であるとき，n 巾剰余記号 $\left(\frac{a}{\mathfrak{p}}\right)\in W_n$（1 の n 乗根）を

$$\left(\frac{a}{\mathfrak{p}}\right)=\sqrt[n]{a}^{\sigma_0-1}$$

で定義する．ここで $\sigma_0=\left(\frac{k_\mathfrak{p}(\sqrt[n]{a})/k_\mathfrak{p}}{\mathfrak{p}}\right)$ は Frobenius 置換を表す．

その上で $a,\ b\in k_\mathfrak{p}$ に対し Hilbert の Norn 剰余記号を

$$\left(\frac{a,\ b}{\mathfrak{p}}\right)=\left(\frac{-1}{\mathfrak{p}}\right)^{w_\mathfrak{p}(a)w_\mathfrak{p}(b)}\left(\frac{a_0}{\mathfrak{p}}\right)^{-w_\mathfrak{p}(b)}\left(\frac{b_0}{\mathfrak{p}}\right)^{w_\mathfrak{p}(a)}$$

ただし $\mathfrak{p}$ の素元を π として $a=a_0\pi^{w_\mathfrak{p}(a)},\ b=b_0\pi^{w_\mathfrak{p}(b)}$ とおいている．

$\left(\frac{a,\ b}{\mathfrak{p}}\right)\equiv\{(-1)^{w_\mathfrak{p}(a)w_\mathfrak{p}(b)}a^{-w_\mathfrak{p}(b)}b^{w_\mathfrak{p}(a)}\}^{(\mathrm{N}\mathfrak{p}-1)/n}\pmod{\mathfrak{p}}$ であることが容易に分かる．

また Norm 剰余記号を次で定義する．

$$\left(\frac{a,\ K/k}{\mathfrak{p}}\right) = \bar{\sigma}$$

ただし右辺は $\mathfrak{g}(K/k)$ のアーベル化 $\mathfrak{g}/\mathfrak{g}'$ に値を持つ．

§ 2 基本公式

解説 2–1

(1) $(a,\ b) = (b,\ a)$

(2) $(a,\ c^2) = 1$

(3) $(a,\ -a) = 1$

(4) $(a,\ 1-a) = 1$

(5) $(a,\ bc) = (a,\ b)(a,\ c)$

解説 2–2 p を奇素数とする．$u,\ v \in \mathbb{Z}_p{}^{\times}$ とする．

(1) $(u,\ v)_p = 1$

(2) $(u,\ p)_p = \left(\frac{u}{p}\right)$ ここで $\left(\frac{u}{p}\right)$ はルジャンドル記号

(3) $(p,\ p)_p = (p,\ -1)_p = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \pmod 4 \text{ のとき} \\ -1 & p \equiv 3 \pmod 4 \text{ のとき} \end{cases}$

解説 2–3 $u,\ v \in \mathbb{Z}_2{}^{\times}$ とする．

(1) $(u,\ v)_2 = (-1)^{\frac{u-1}{2}\cdot\frac{v-1}{2}} = \begin{cases} 1 & u \equiv 1 \pmod 4 \text{ または } v \equiv 1 \pmod 4 \text{ のとき} \\ -1 & u \equiv v \equiv 3 \pmod 4 \text{ のとき} \end{cases}$

(2) $(u,\ 2)_2 = \left(\frac{2}{u}\right) = (-1)^{\frac{u^2-1}{8}} \begin{cases} 1 & u \equiv 1,\ 7 \pmod 8 \text{ のとき} \\ -1 & u \equiv 3,\ 5 \pmod 8 \text{ のとき} \end{cases}$

(3) $(2,\ 2)_2 = (2,\ -1)_2 = \left(\frac{-1}{2}\right) = 1$

解説 2–4

(1) $(u,\ v)_\infty = \begin{cases} 1 & u > 0 \text{ または } v > 0 \text{ のとき} \\ -1 & u < 0 \text{ かつ } v < 0 \text{ のとき} \end{cases}$

問題 2–5 $(ax^2 + by^2,\ -ab) = (a,\ b)$

解答

これは 2 次形式 $f(x,\ y) = ax^2 + by^2$ に関する不変量 $e(f)$ のことである．二次形式の基底の変換で示すことが出来るが，次のような解法を考えてみた．

$$(ax^2 + by^2,\ -ab) = (-ab,\ ax^2 + by^2) = (-ab,\ ax^2)\left(-ab,\ 1 - \left(-\frac{by^2}{ax^2}\right)\right)$$

ここで $(-ab,\ ax^2) = (-ab,\ a) = (-a,\ a)(b,\ a) = (a,\ b)$.

また $\left(-ab,\ 1-\left(-\dfrac{by^2}{ax^2}\right)\right)=\left(\left(-\dfrac{by^2}{ax^2}\right),\ 1-\left(-\dfrac{by^2}{ax^2}\right)\right)=1$
以上より証明できた.

定理 2–6 $\prod_v (a,\ b)_v = 1$

§ 3 2 次形式

解説 3–1

(1) $p \neq 2$ とし $q=p^f$ とする．有限体 $\mathbb{F}_q$ 上の 2 変数非退化 2 次形式 ax^2+by^2 は ${\mathbb{F}_q}^\times$ のすべての元を表現する.

(2) $p \neq 2$ とし $q=p^f$ とする．有限体 $\mathbb{F}_q$ 上の 3 変数非退化 2 次形式 $ax^2+by^2+cz^2$ は $\mathbb{F}_q$ のすべての元を表現する.

解説 3–2 f を $k=\mathbb{Q}_p$ 上の階数 n の非退化 2 次形式とする.

(1) $n=2$ の場合，f が 0 を表す $\iff$ $d(f) \equiv -1 \pmod{k^{\times 2}}$.

(2) $n=3$ の場合，f が 0 を表す $\iff$ $(-1,\ d(f)) = e(f)$

(3) $n=4$ の場合，f が 0 を表す $\iff$ $d(f) \neq 1$ または $d(f)=1,\ e(f)=(-1,\ -1)$

(4) $n=5$ の場合，すべての 2 次形式は 0 を表す.

解説 3–3 f を $k=\mathbb{Q}_p$ 上の階数 n の非退化 2 次形式とする．$a \in k^\times/k^{\times 2}$ をとる.

(1) $n=1$ の場合，f が a を表す $\iff$ $a \equiv d \pmod{k^{\times 2}}$.

(2) $n=2$ の場合，f が a を表す $\iff$ $(a,\ d(f)) = e(f)$

(3) $n=3$ の場合，f が a を表す $\iff$ $a \neq -d(f)$ または $a \equiv d(f),\ e(f)=(-1,\ -d)$

(4) $n=4$ の場合，すべての 2 次形式は a を表す.

解説 3–4 $p \neq 2$, $\mathbb{Q}_p$ 上の階数 n の非退化 2 次形式の類の数は

(1) $n=1$ の場合，4.

(2) $n=2$ の場合，7.

(3) $n \geqq 3$ の場合，8.

解説 3–5 $\mathbb{Q}_2$ 上の階数 n の非退化 2 次形式の類の数は

(1) $n=1$ の場合，8.

(2) $n=2$ の場合，15.

(3) $n \geqq 3$ の場合，16.