ワイルと数の幾何

今野秀二

2016年1月23日

§1　ヒルベルトはミンコウスキの死後ワイル，シュパイザーと協力し彼の全集を編集しているが，その序文で数の幾何をミンコウスキーの最も重要な研究であると述べています．そのミンコウスキーは1896年，数の幾何に関する著書 Geometrie der Zahlen （以後 [GZ] で表す）を出版していて，ワイルの数の幾何研究はこの本が出発点になっている．

ミンコウスキはこの本の序文に「エルミートの数の幾何に関する定理とヂリクレの2次形式の簡約化が関係する」という趣旨のことを簡単に述べている．でも本文のなかにこの事に相当することは書かれていない．ヒルベルトはこれについて，（ミンコウスキの死後）シュパイザーとこの本の再版をしたとき，その序文に「この本の後半が出ていない」と書いている．ワイルの数の研究はこの出版されなかった後半部分の再現がモチベーションになっていたようで，以下ワイルが論文の中で述べていることを追いながら再現して見ることにする．

まず実 n 次元空間を $E=\mathbf{R}^n$ とし，x をその点（またはヴェクトル）とする．ミンコウスキーは E 上の連続関数 $f(x)$ が (i) $f(x)\geq 0,\ =0 \rightleftarrows x=0$, (ii) $f(tx)=|t|f(x)$ $(t\in\mathbf{R})$, (iii) $f(x+y)\leq f(x)+f(y)$ の3条件を満たすとき，これをゲージ関数と呼んだ．これは距離関数を一般化したもので例えば，正定値の2次形式やエルミート形式 $q(x)$ に対し，$f(x)=q(x)^{1/2}$ とすればゲージ関数が得られる．このような f に対して $\mathfrak{K}=\{x\in E\mid f(x)<1\}$ と置くと，これは原点対称で有界な凸領域になる．そこでこの体積を V と表そう．

一方，E の格子点からなる加群 $L=\mathbf{Z}^n$ に対し $M=\min_{0\neq x\in L} f(x)$ と定義する．ミンコウスキーの定理は凸体と格子点を結びつけるもので

$$M^n\cdot V\leq 2^n \tag{1}$$

と表される（[GZ] 30 章）．[GZ] ではこの定理を更に精密化して主定理

$$M_1 \cdots M_n \cdot V \leq 2^n \tag{2}$$

を導いている（51 章）．ここで $\{M_i\}$ は，まず $M_1 = M$ とし $f(d_1) = M_1$ なる $d_1 \in L$ をとる（以下 $x_1, \cdots, x_k \in E$ で張られる部分空間を $[x_1, \cdots, x_k]$ で表す）．$\{M_1, \cdots, M_{k-1}\}$, $\{d_1, \cdots, d_{k-1}\}$, $(f(d_i) = M_i)$ まで求まったとき，$d \notin [d_1, \cdots, d_{k-1}]$ なる $d \in L$ について $f(d)$ の最小値を $M_k = f(d_k)$ とする．このとき $M_1 \leq \cdots \leq M_n$ である．

さて，上記エルミートの数の幾何の話は正定値 2 次形式 $q(x)$ に対し，$M = \min_{0 \neq x \in L} q(x)$ がある定数を超えないという定理である．ヂリクレの方は 3 変数の 2 次形式の類数計算での簡約化理論 (reduction theory) である．これに関しワイルは「ミンコウスキーは [GZ] で 2 次形式を含む一般のゲージ関数について，エルミートとヂリクレのアイデアを結びつけようとしていた，だが何故か途中でやめてしまった」と述べている．実際，ミンコウスキー は 1905 年になって，論文 Diskontinuitats bereich fur arithmetische Aquivalenz ([D] で表す）で 2 次形式の簡約化を発表しているが，その方法は [GZ] とは別の方法であった．（この論文には不備があり，後にビーベルバッハ，シューアが完成させている）．ワイルの数の幾何研究のモチベーションは [GZ] の考えを発展させるという点にあり，彼はマーラーの方法を改良し，ゲージ関数の簡約化を進めその特別な場合として正定値エルミート形式および四元数体での簡約化を展開している．

§2 より詳しく見るため正定値 2 次形式を

$$q(x) = {}^t x Q x = \sum_{x \in L} q_{ij} x_i x_j \qquad (q_{ij} = q_{ji} \in \mathbf{R}) \tag{3}$$

と表し，P で n 次の実正定値 2 次形式の全体を表すことにする．ここで x は $x_1, \cdots, x_n$ を成分にもつ列ベクトル，$Q = (q_{ij})$ は退化しない実対称行列である．この $q \in P$ は $\{q_{ij}\}$ $(1 \leq i \leq j \leq n)$ を座標にもつ $\mathbf{R}^N$ $(N = n(n+1)/2)$ の点と見なして $P \subset \mathbf{R}^N$ と考える．以下 q は Q と同一視しよう．

P には $(Q, g) \to Q \cdot g = {}^t g Q g$ $(Q \in P,\ g \in GL_n(\mathbf{R}))$ で線形群 $GL_n(\mathbf{R})$ が作用している．とくに行列式が ± 1 の n 次整数係数行列からなる部分群を $\Gamma = GL_n(\mathbf{Z})$ とすれば，この Γ も P に作用しているが，2 つの 2 次形式 $q(x) = {}^t x Q x$ と $q_1(x) = {}^t x Q_1 x$ があある $\gamma \in \Gamma$ で移り合うとき，つまり $Q_1 = {}^t \gamma Q \gamma$ なるとき同値と定義する．問題は P をこの同値で分けたときその代表系はどんな集合になるか，あるいは P における Γ の基本領域を求めることである．

そのために，各 $k \in \{1,2,\cdots,n\}$ について，X_k は整数ベクトル $x=(x_1,\cdots,x_n) \in \mathbf{Z}^n$ で $\{x_k,\cdots,x_n\}$ の公約数が 1 であるものの全体とする．このとき $q \in P$ が簡約 (reduced) とは各 $k=1,\cdots,n$ について

$$q(x)=\sum_{x\in L} q_{ij}x_ix_j \geq q_{kk}, \qquad x \in X_k \tag{4}$$

を満たすことと定義する．以後簡約な $q \in P$ の全体を Z と表そう．

このとき，任意の正値2次形式は簡約な2次形式に同値になることが知られている．すなわち，任意の $q(x)={}^txQx \in P$ に対し，ある $\gamma \in GL_n(\mathbf{Z})$ があり ${}^t\gamma Q\gamma \in Z$ とできる．

ここで集合 Z だが，(4) は点 q の座標 q_{ij} を変数と見れば，x_ix_j を係数とする1次不等式で，各々は $\mathbf{R}^N$ の半空間を定めるから，Z は無限個の超平面で囲まれた凸の多面体になっていることが分かる．ミンコウスキーは [D] で Z について以上のことのほか次の (I), (II) を主張している．すなわち

(I) Z を定義する不等式 (4) は有限個の不等式で間に合うこと

(II) Z の点 Q に対し ${}^t\gamma Q\gamma \in Z$ なる $\gamma \in \Gamma$ は有限個しかないこと．

(II) の証明は完全だったが，(I) に関してワイルは問題点を指摘しそれを正し，さらにそのアイデアを発展させている．

まず $q^{(0)}$ が Z の境界点であるとは，ある $x=(x_1,\cdots,x_n) \in X_k$ について

$$q^0(x)=\sum q^0_{ij}x_ix_j = q^0_{kk}. \tag{5}$$

を満たしていることであるから，(I) の証明には簡約な $q^{(0)}$ に対し (5) を満たす $x \in X_k$ が有限個しかないことをいえばよい．そのため $q(x)$ をヤコビ変換して

$$q(x)=r_1z_1^2+\cdots+r_nz_n^2, \quad z_i=x_i+\sum_{j>i} x_j\beta_{ji} \quad (i \leq i \leq n) \tag{6}$$

と表す．このとき $r_i \leq q_{ii}$ $(1 \leq i \leq n)$ は容易に分かるが，さらに q が簡約のとき q に依存しないある定数 λ_n があり

$$\lambda_n \cdot q_{11}\cdots q_{nn} \leq r_1\cdots r_n = \det(q_{ii}) \tag{7}$$

を証明する．この不等式を部分空間に制限して

$$\lambda_k \cdot q_{kk} \leq r_k \quad (1 \leq k \leq n) \tag{8}$$

が得られ，これと $r_i \leq q_{ii}$ から $|z_i|$ が有界であること，さらに $|x_i|$ の有界を導いている．

不等式 (7) がこの証明の鍵であるが，ワイルはミンコウスキー [GD] のなかの (2) の考えとマーラーの定理を精密化することで証明している．実はミンコウスキーも値は粗いけれども（さらに証明に難点もあるが）不等式 (7) を発見しているので，ワイルは (7) をミンコウスキーの到達点と評価しています．ミンコウスキーの不等式とも呼ばれている．

さて，ワイルはここで

(1) Z は有限個の超平面で囲まれたピラミッド形をしている

(2) 変換 $\gamma \in \Gamma$ による Z の像を Z_γ とすれば $Z_\gamma = Z_{\gamma\varepsilon}$ ここで $\varepsilon = (\varepsilon_1, \cdots, \varepsilon_n)$ $(\varepsilon_j = \pm 1)$ は $x = (x_1, \cdots, x_n) \to \varepsilon x = (\varepsilon_1 x_1, \cdots, \varepsilon_n x_n)$ なる変換である

(3) $J \subset \Gamma$ は $\{\varepsilon\}$ から生成される位数 2^n の部分群とすれば $\{Z_\gamma | \gamma \in \Gamma/J\}$ は境界以外で重複せず，かつ P を隙間なく覆っている

(4) Γ は有限生成である

を証明している．Z が Γ/J の P における基本領域であることとその構造を表している．

ワイルは (7) を一般のゲージ関数に対して考えている．

§3 L の $\mathbf{Z}$ 基 $\{s_1, \cdots, s_n\}$ がゲージ関数 f に関し簡約とは，各 $k = 1, \cdots, n$ および任意の $x = (x_1, \cdots, x_n) \in X_k$ に対して

$$f(x_1 s_1 + \cdots + x_n s_n) \geq f(s_k) \tag{9}$$

の成り立つことと定義する．さらに標準基 $\{e_i\}$ が f に関し簡約のとき f は簡約という（e_i は第 i 成分が 1 他は 0 を成分に持つベクトル）．例えば $f = q^{1/2}$ $(q \in P)$ のときは f の簡約は 2 次形式の簡約と一致する．

L の基で f に関して簡約なものを求めるには以下のようにするとよい．まず L の $\mathbf{Z}$ 基となりうる $s \in L$ で $f(s)$ が最小のものを s_1 とし，$N_1 = f(s_1)$ とする．$\{s_1, \cdots, s_{k-1}\}$, $\{N_1, \cdots, N_{k-1}\}$ まで求まったら $\{s_1, \cdots, s_{k-1}, s\}$ が L の $\mathbf{Z}$ 基の構成要素となる $s \in L$ で $f(s)$ が最小のものを s_k とし $N_k = f(s_k)$ とする．こうして求めた $\{N_i\}$ は $N_1 \leq N_2 \leq \cdots \leq N_n$ かつ $M_k \leq N_k$ で，$\{s_i\}$ は簡約な基になっている．2 次形式の場合 $N_k = q_{kk}$ である．このとき f に依存しないある定数 θ_k および μ_n があり（マーラーの定理）

$$N_k \leq \theta_k M_k \tag{10}$$

$$N_1 \cdots N_n \cdot V \leq \mu_n \tag{11}$$

が分かる．ここでワイルはゲージ関数 f として，虚 2 次体上の正定値エルミート形式 と正定値ハミルトンの 4 元数形式の平方根を取ると，その体積は判別式の低数倍がとなるか

ら，２次形式の場合の $r_1 \cdots r_n$ に相当する量が現れて (7) および (8) に相当する式が得られる．こうして，これらの形式に対しても (1)-(4) の成り立つことを導いている．

(1) Theory of reduction for arithmetical equivalence. (1940)
Gesammelte Abhandlungen Bd III

(2) Theory of reduction for arithmetical equivalence II. (1942)
Gesammelte Abhandlungen Bd IV

(3) On geometry of numbers. (1942)
Gesammelte Abhandlungen Bd IV

(4) Fundamental domains for lattice groups in division algebra I, II. (1945)
Gesammelte Abhandlungen Bd IV