数理解析研究所講究録
第583巻 1986年 106-119

格子の自己同型群と跡公式の一般化

九大教養　伊吹山知義（Tomoyoshi Ibukiyama）

§1. 問題の設定と一般論

以下の話は定符号の"2次"形式すべてに対して設定できるが、話を簡単にするため、4元数的エルミート形式のみについて述べる。Bを$\mathbb{Q}$上の定符号4元数環とし、B^nに内積を

$B^n \ni x, y$ に対し

$$(x, y) = \sum_{i=1}^{n} x_i \bar{y_i} \quad (x=(x_1,\cdots,x_n),\ y=(y_1,\cdots,y_n))$$

で入れる。これでB^nを4元数的エルミート空間とみなし、$\mathcal{L}$をB^nの$\mathcal{O}$-lattice からなるある genus とする。（但し$\mathcal{O}$はBのある極大整数環）すなわち、$M \in \mathcal{L}$とする時、

$$\mathcal{L} = \{L \subset B^n,\ 左\ \mathcal{O}\text{-lattice};\ L = M g_p \text{ for some } g_p \in G_p \text{ for all } p\},$$

$$G_p = \{g \in M_n(B_p);\ g\,{}^t\bar{g} = n(g)\cdot 1_n,\ n(g) \in \mathbb{Q}_p^{\times}\}.$$

今、$G = \{g \in M_n(B);\ g\,{}^t\bar{g} = n(g)\cdot 1_n,\ n(g) \in \mathbb{Q}_+^{\times}\}$とおくとき、$L_1 g = L_2$ $(g \in G)$ ならL_1とL_2は同じ class という。

この時，次の問題を考えたい。

問題1　$\mathcal{L}$ の類数，即ち $\#(\mathcal{L}/G)$ を求めよ。

問題2　$\mathcal{L}$ の類の完全代表系を $L_1, \cdots, L_H$ とする。

$Aut(L_i) = \{g \in G \,;\, L_i g = L_i\}$ とおくとこれは

有限群だが，どのような群か決めよ。

問題3.　K を与えられた有限群とする時，$K \cong Aut(L_i)$

となる類 L_i の個数を求めよ。

問題に対する結果等については次節以下にまわし，ここでは，問題の性格と，これを解く一般的手段について解説しよう。問題1 は，一般的解法は跡公式として良く知られている。(cf. Hashimoto[1]) しかし，問題2, 3については，言及したものをみかけない。実際この両者（1 と 2, 3）は，かなり性格が違い，通常の跡公式だけでは，2, 3 を解くには不足なのである。この事情は次の通りである。今 place $v(\neq\infty)$ に対し

$$U_v = \{g \in G_v \,;\, M_v g_v = M_v\}$$ とおく。この時

$$\#(\mathcal{L}/G) = \#\big((G_\infty \cdot \prod_{v\neq\infty} U_v)\backslash G_A/G\big)$$

であるが，今 p を fixed prime として U_p の有限指数正規部分群 V_p で $gGg^{-1}\cap V_p$ $(g \in G_A)$ がいつでも torsion free のものを選ぶ。

U_p/V_p は $\mathcal{V}\backslash G_A/G$ $(\mathcal{V} = G_\infty V_p \prod_{v\neq\infty,p} U_v)$ に作用しているが，この作用での単位表現の重複度が $\#(\mathcal{L}/G)$ と言って

もよい。言いかえると、有限群 U_p/V_p が $V\backslash G_A/G$ 上ひきおこす置換表現の推移域の個数が $\#(\mathcal{L}/G)$ であり、この置換表現の指標を与えるのが通常の跡公式である。一方、問題2.3はこの各推移域での1点の isotropy subgroup を決める問題、つまり置換表現それ自身を決める問題であり、一般に置換表現は付随する線型表現を指定してもそれだけでは決まらないので何らかの新しい道具が必要となる。(勿論、非常に幸運な場合は何もいらないことはありうるが、それはむしろ例外的であろう。) 今 $\Gamma_i = \mathrm{Aut}(L_i)$ $(i=1\sim H)$ とおく。$f(x)\in\mathbb{Z}[x]$ とする時、通常の跡公式では、

$$\sum_{i=1}^{H} \frac{\#\{\gamma\in\Gamma_i\,;(\gamma\text{の主多項式})=f\}}{\#(\Gamma_i)}$$

が、G の共役類上の data で書きあらわせていた。我々はこれを少し拡張して、有限群 K に対して、$K\subset\Gamma_i$ なる情報を与えるような値を得たい。そのため、K の生成元を $g_1,\cdots,g_r$ とし、基本関係式を $f_1(g_1,\cdots,g_r)=\cdots=f_s(g_1,\cdots,g_r)=1$ としよう。今 Γ_i^r ($=\Gamma_i$ の r 個の直積) の元 $(\gamma_1,\cdots,\gamma_r)$ (つまり、順序つき) であって、その基本関係が $f_1,\cdots,f_s$ のものの個数を $t_i(K)$ と書くことにする。

$$M(K) = \sum_{i=1}^{H} \frac{t_i(K)}{\#(\Gamma_i)} \quad \text{とおく。}$$

$M(K)$ を求める公式は、G の元の順序をこめた r ケの組の"共役類"の data であらわされる。詳しくは次のようになる。

<u>定理</u> $$M(K) = \sum_{g \in G^r(K)/\underset{G}{\sim}} \sum_{L_G(\Lambda)} M_G(\Lambda) \prod_p c_p(g, U_p, \Lambda)$$

以下、記号を解説する。$G^r(K)$ は $G^r \ni g = (g_1, \cdots, g_r)$ で基本関係式が $f_1 = \cdots = f_s = 1$ のもの全体、$/\underset{G}{\sim}$ は、この G-共役類、すなわち $(g_1, \cdots, g_r) \to (hg_1h^{-1}, \cdots, hg_rh^{-1})$ $(h \in G)$ による G-orbit 全体をあらわす。Λ の説明のため、次の記号を導入する。$Z(g) = \{h \in M_n(B) ; hg_i = g_ih \text{ for all } i = 1 \sim r\}$, $Z_G(g) = Z(g) \cap G$。さて Λ は $Z(g)$ の $\mathbb{Z}$-order であり、

$$L_G(\Lambda) = \{\Lambda' \subset Z(g) ;\ \Lambda'_p = x_p \Lambda_p x_p^{-1} \text{ for some } x \in Z_G(g)_p \text{ for } \forall p\}.$$ また

$$M_G(\Lambda) = \sum_{k=1}^{l} \frac{1}{\#(\Lambda_k^\times \cap G)},$$ 但し $\{y_k\}_{k=1}^{l}$ を $Z_G(g) \backslash Z_G(g)_A / (\Lambda_A^\times \cap G)$ とするとき、$\Lambda_k = y_k \Lambda y_k^{-1}$ とおいた。

さて、ある $\mathbb{Z}$-order $R \subset M_n(B)$ があって $R_p \cap G_p = U_p$ と仮定しておく。$g \in G^r(K)$ に対し

$$\mathfrak{M}(g, U_p, \Lambda) = \{h \in G_p ;\ h^{-1} g_i h \in U_p \text{ for all } i = 1 \sim r,\ Z(g)_p \cap hR_p h^{-1} = a \Lambda_p a^{-1} \text{ for some } a \in Z_G(g)_p\}$$

とおき、

$C_p(g, U_p, \Lambda) = \#(Z(g)_p \backslash \mathfrak{M}_p(g, U_p, \Lambda)/U_p)$ とおく。

(注意1) この定式化はΛが少し無駄なので、$\mathrm{vol}(Z_G(g)_\Lambda / Z_G(g))$ 等で書きみかけ上Λを除いてしまうこともできるが、実際上の計算ではmeasureのとり方等で注意が必要になるので、あえてこのままにしておいた。

(注意2) 実用上は、Kの基本関係のみではなく、$K \hookrightarrow G$ なるうめこみまで指定しておいた方がよい。つまり $\mathbb{Q}(K) \subset M_n(B)$ の $GL_n(B)$-共役類によって"G-共役類"のparametrizationが変わってきうる。公式は勿論その分だけ $G^r(K)$ を小さくしてやれば同様である。

定理の証明は[1]の跡公式と全く同様である。さて、これを用いて問題2, 3は少くとも原理的には次のようにして解ける。

1) V_p をうまくみつけて U_p/V_p の有限部分群をすべて求める。$\Gamma_i \hookrightarrow U_p/V_p$ が容易だからKの候補はこれらに限る。

2) 1)でできた群すべてについて $M(K)$ を求める。($M(K)=0$ かもしれない。)

3) 上のK全体に包含関係で順序を入れて、大きい方から順に個数を求める。即ち、$M(K) \neq 0$ なるKのうちで、極大な元K_0をとると、$\Gamma_i \cong K_0$ なるものがある。これについて $t_i(K_0)/\#(K_0)$ をK_0のみみれば計算できるので $\#\{i ; \Gamma_i \cong K_0\} = M(K_0)\#(K_0)/t_i(K_0)$ である。($t_i(K_0)$ はK_0のみによる。) 次にこのような$\{K_0\}$を除いたもののうちで極大なものに対し $M(K)$ を求め、Kを含むK_0からの寄与 $t_i(K)/\#(K_0)$ をひきさって上と同様のことをすれば $\#\{i ; \Gamma_i \cong K\}$が求まる。以下同様。

以上で最も面倒なのは $M(K)$ の計算である。これを実行するには、$G^r(K)$ の共役類のうまい paranetrization, adelic な共役類と global な共役類の比較、くしに $c_p(g, U_p, \Lambda)$ のかなり面倒な計算等、通常の跡公式と類似なことをもっと複雑な場合に実行しなければならない。完全に実行した case は以下に述べるが、しかし、たとえ部分的な情報でも、unimodular 行列の単数群等について面白いこともあるかもしれない。

§2. 代数幾何的動機と知られていた結果

この節では、この問題を考えた動機と知られていた結果について述べる。

素数 p を固定し、E を $\overline{\mathbb{F}}_p$ 上の supersingular elliptic curve とする。B の判別式を p とすると $\mathrm{End}(E)\otimes\mathbb{Q}=B$ であり、E の同型類と B の ideal類の1対1対応は Deuring によりよく知られている。また B の類数公式等、$\overbrace{\text{問題 1〜3}}^{n=1\text{での}}$ の答は Eichler によりよく知られていた。さて、$\mathcal{L}_n$ を B^n の、$\mathcal{O}^n$ を含む genus (= principal genus) とする。この時、

__Th. 1__ (Hashimoto-Ibukiyama [3], Hashimoto [2])

$\#(\mathcal{L}_n/G)$ は $n=2,3$ では具体的に与えられる。

__Th. 2__ (Ibukiyama-Katsura-Oort [4])

E^n 上の principal polarization (up to alg. equivalence), $n\geqq 2$ と $\mathcal{L}_n/G$ の元は1対1に対応する。更に $n=2$ に対して問題2, 3は代数幾何的手法で解ける。

更に、$n=2$ の時は、supersingular abelian surface の moduli と、他のある genus が関係している。$A_{2,1}$ で主偏極アーベル曲面(標数 p の閉体上)の moduli をあらわし、$A_{2,1,2}$ で level 2 structure を入れた moduli をあらわすとする。今 $A\sim E^2$ (isogeny) なるもの全体の $A_{2,1}$ での orbit を V_1 とかき level 2 で考えたものの $A_{2,1,2}$ での orbit を V_2 とかく。V_i の成分は皆 $\mathbb{P}^1$ と同型であることが知られているが、一般に V_i は既約ではない。さて、一方、$\mathcal{L}_2'$ を B^2 の non principal genus

とする。即ち、 $\mathcal{L}_2'$ は、 $q \neq p$ の時 $L_q = O_q^2 g_q \ (g_q \in G_q)$、で、$L_p$ は B_p^2 の (unique) indecomposable maximal O_p-lattice となる O-lattice L の集合である。この時、

<u>Th. 3.</u> (Katsura-Oort [5])

$$\#(V_1 \text{ の成分}) = \#(\mathcal{L}_2'/G)$$

(なお、右辺の具体的値は以前から [3] でわかっていた。)
更に、$V_2 \to V_1$ によって各成分上で、$\mathbb{P}^1$ 上の Galois covering でやはり $\mathbb{P}^1$ になるものが得られ、このそれぞれの Galois 群が、$\mathrm{Aut}(L_i)/\pm 1$ になっている。(L_i は $\mathcal{L}_2'/G$ の代表)
Katsura-Oort は更に、$\mathcal{L}_2'$ に対する問題 2, 3 の解答を、小さな p (29 以下位) について代数幾何的に求めた。ここで使用された方法をよくみると、実質上、<u>通常の</u>跡公式から得られる情報を代数幾何的手法で得ていることになり、結局、雑に言って「線型表現」のみで決められる場合のみ答が得られていることになる。我々は任意の p につき次節で解く。なお、$\mathrm{Aut}(L_i)/\pm 1$ は $\mathrm{Aut}(\mathbb{P}^1)$ の部分群でかつ $p \geq 7$ なら tame covering である事等から、彼等によって $\mathbb{Z}/n$ $(n = 1, 2, 3)$, D_{2n} $(n = 2, 3, 4, 5, 6)$, A_4, S_4, A_5 のいずれかであることが指適されている。これも純粋に整数論的に示せ、D_8, D_{10} はないこともわかる。

§3. 主定理と数値例.

主定理 $\mathcal{L}_2'$を前節の通りとする。$L_1, \cdots, L_H$を$\mathcal{L}_2'/G$の代表とする。有限群Kに対して

$$\#(K) = \#\{i \,;\, \mathrm{Aut}(L_i)/\pm 1 \cong K\}$$

と書くことにする。Bの判別式p（素数）を7以上とすれば、$\#(K) \neq 0$ なるKは、$\{1\}$, $\mathbb{Z}/2$, $\mathbb{Z}/3$, $(\mathbb{Z}/2)^2$, S_3, A_4, S_4, A_5, D_{12}（位数12のdihedral）のどれかであり、具体的には次で与えられる。但し$h(-d)$は$\mathbb{Q}(\sqrt{-d})$の類数とする。

$$\#(A_5) = \begin{cases} 1 & p \equiv 2, 3\ (5) \\ 0 & \text{otherwise}, \end{cases} \qquad \#(S_4) = \begin{cases} 1, & p \equiv 3, 5\ (8) \\ 0, & \text{otherwise} \end{cases}$$

$$\#(D_{12}) = \begin{cases} 1 & p \equiv 5\ (12) \\ 0 & \text{otherwise} \end{cases}$$

$$\#(A_4) = \begin{cases} \dfrac{h(-2p)}{4} - \#(A_5) & \cdots\ p \equiv 1, 7 \mod. 8 \\[2ex] \dfrac{h(-2p) - 2}{4} - \#(A_5) & \cdots\ p \equiv 3, 5 \mod. 8 \end{cases}$$

$$\#((\mathbb{Z}/2)^2) = \begin{cases} \dfrac{h(-p)}{4} - \#(D_{12}) & \cdots\ p \equiv 1 \mod. 8 \\[2ex] \dfrac{h(-p) - 1}{2} & \cdots\ p \equiv 3 \mod. 8 \\[2ex] \dfrac{h(-p) - 2}{4} - \#(D_{12}) & \cdots\ p \equiv 5 \mod. 8 \\[2ex] 0 & \cdots\ p \equiv 7 \mod. 8 \end{cases}$$

$$\#(S_3) = \begin{cases} h(-3p) - \#(A_5) - \#(D_{12}) & \cdots\ p \equiv 1 \ (8) \\ \dfrac{h(-3p)}{2} - \#(A_5) - \#(D_{12}) - 1 & \cdots\ p \equiv 5 \ (8) \\ \dfrac{h(-3p)}{4} - \#(A_5) - \#(S_4) & \cdots\ p \equiv 3, 7 \ (8) \end{cases}$$

$$\#(\mathbb{Z}/2) = -\frac{3}{2}\#((\mathbb{Z}/2)^2) - \#(S_3) - \frac{1}{2}\#(A_4) - \frac{3}{4}\#(S_4)$$

$$-\frac{7}{6}\#(D_{12}) - \frac{1}{2}\#(A_5) + \begin{cases} \dfrac{5(p-1)}{48} & \cdots\ p \equiv 1 \ (4) \\ \dfrac{p+1}{16} & \cdots\ p \equiv 3 \ (4) \end{cases}$$

$$\#(\mathbb{Z}/3) = -\frac{1}{2}\#(S_3) - \#(A_4) - \frac{1}{2}\#(S_4) - \frac{1}{4}\#(D_{12}) - \frac{1}{2}\#(A_5)$$

$$+ \begin{cases} \dfrac{p-1}{12} & \cdots\ p \equiv 1 \ (3) \\ \dfrac{p+1}{24} & \cdots\ p \equiv 2 \ (3) \end{cases}$$

$$\#(\{1\}) = \frac{p^2-1}{2880} - \frac{1}{2}\#(\mathbb{Z}/2) - \frac{1}{3}\#(\mathbb{Z}/3) - \frac{1}{4}\#((\mathbb{Z}/2)^2)$$

$$-\frac{1}{6}\#(S_3) - \frac{1}{12}\#(A_4) - \frac{1}{24}\#(S_4) - \frac{1}{12}\#(D_{12})$$

$$-\frac{1}{60}\#(A_5).$$

数値例

$\{Aut(L_i)/\pm 1\}$ は. $p=7$ は A_5, $p=11$ は S_4, $p=13$ は $\{S_4, A_5\}$

$p=17$ は $\{D_{12}, A_5\}$, $p=19$ は $\{A_4, S_4\}$, $p=23$ は $\{S_3, A_5\}$

以下は数が増えるので表にする。(右の数字は個数)

$p \backslash K$	$\{1\}$	$\mathbb{Z}/2$	$\mathbb{Z}/3$	$(\mathbb{Z}/2)^2$	S_3	A_4	S_4	D_{12}	A_5
29	0	0	0	0	1	0	1	1	0
31	0	0	0	0	1	2	0	0	0
37	0	0	0	0	2	1	1	0	1
41	0	0	0	1	1	1	0	1	0
43	0	0	1	0	1	1	1	0	1
47	0	1	0	0	1	1	0	0	1
53	0	1	0	0	2	0	1	1	1
59	0	1	1	1	0	1	1	0	0
61	0	0	1	1	3	2	1	0	0
67	0	1	2	0	1	2	1	0	1
71	0	2	1	0	2	1	0	0	0
73	0	1	1	1	3	3	0	0	1
79	0	1	3	0	3	2	0	0	0
83	1	1	1	1	1	1	1	0	1
89	0	3	1	2	1	2	0	1	0
97	0	3	2	1	3	4	0	0	1

§4. 証明のスケッチ

$G_p^* = \{ g \in M_2(B_p) \,;\, g\begin{pmatrix}0&1\\1&0\end{pmatrix}{}^t\bar{g} = n(g)\begin{pmatrix}0&1\\1&0\end{pmatrix},\ n(g)\in \mathcal{O}_p^\times\}$ と G_p を同型な群にとりかえると，π を $\mathcal{O}_p$ の素元として，

$$U_p \cong \begin{pmatrix} \mathcal{O}_p, & \pi^{-1}\mathcal{O}_p \\ \pi \mathcal{O}_p, & \mathcal{O}_p\end{pmatrix}^\times \cap G_p^*$$

であり，

$$V_p = \begin{pmatrix} 1+\pi \mathcal{O}_p, & \mathcal{O}_p \\ \pi^2 \mathcal{O}_p, & 1+\pi \mathcal{O}_p\end{pmatrix}\cap G_p^*$$

とおけば，U_p 内で normal で，かつ $p \geqq 7$ なら V_p には G の元の G_A-共役からくる torsion element は存在しない。よって

$\Gamma_i \hookrightarrow U_p/V_p$ (injective) だが，

<u>Lemma</u> $U_p/V_p \cong SL_2(\mathbb{F}_{p^2})$

一方，通常の跡公式より $\Gamma_i/\pm1$ の元の位数は高々 6 であり また，$PSL_2(\bar{\mathbb{F}}_p)$ の位数が p と素な群は，巡回群，多面体群，2面体群のみだから群の候補はかなり減る。更に，

<u>Lemma</u> D_8, D_{10} はあらわれない。

これは $\mathbb{Q}(\bar{D}_8), \mathbb{Q}(\bar{D}_{10})$ ($\bar{D}_8, \bar{D}_{10}$ は $G/\pm1$ の G へのもちあげ) がそれぞれ $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{5})$ 上の多元環として類数が1なこと，及び簡単な local theory によりわかる。さて，S_4, A_5, D_{12} の個数は通常の跡公式から求まるが，それ以外はもはや無理である。そこで，たとえば $K=\{\pm1, \pm i, \pm j, \pm k\}$ (quaternion gp) に対して，$M(K)$ を計算する。$g=(a,b)\in G^2$, $a^2=b^2=-1$, $ab=-ba$ なる元に対して $Z_G(g) = K_0^\times \cup y K_0^\times$

(K_0はある虚2次体)となり、gのG共役類は、K_0でparametrizeされる。$c_g(g, U_g, \Lambda) \neq 0$ for some Λ なるG_g共役類を皆調べることにより、$M(K)$は$K_0 = \mathbb{Q}(\sqrt{-p})$ or $\mathbb{Q}(\sqrt{-2p})$の時の共役類のみ寄与があることがわかる。$M_G(\Lambda)$は、この時$h(-p)$及び$h(-2p)$にかなり近い。(実際はわりと微妙な点があるが。)これが、主定理に類数のあらわれる理由である。$K/\pm 1 \cong S_3$の時は、Kは判別式$3\cdot\infty$の定符号4元数環のmaximal orderの単数群になり、やはり虚2次体でparametrizeされ、$M(K)$には$\mathbb{Q}(\sqrt{-3p})$のもののみ寄与する。これから$h(-3p)$がでる。

<u>問題</u>　虚2次体の類数が現われる理由を代数幾何的に説明せよ。

更に、主定理全部が代数幾何的に示せれば面白いのであろう。

(注意) 主定理では、Bの判別式が素数の時のみ述べたが、$\mathcal{L}$があるpでindecomposableなB^2のmaximal latticeからなるgenusなら、Bの判別式が一般でも、問題2.3はexplicitに解けている。($\mathcal{L}$が$\forall p$でdecomposableでBの判別式一般の時は、勿論原理的には同様だが、実行していない。)

文献

[1] K. Hashimoto, On Brandt matrices associated with the positive definite quaternion hermitian forms, J. Fac. Sci. Univ. Tokyo (1980) 227-245

[2] K. Hashimoto, Class numbers of positive definite ternary quaternion hermitian forms, Proc. Japan Acad Vol. 59 Ser. A (1983) 449-494

[3] K. Hashimoto & T. Ibukiyama, On class numbers of positive definite binary quaternion hermitian forms, (I), (II), (III), J. Fac. Sci. Univ. Tokyo (1980) 549-601, (1982) 695-699, (1983) 393-401

[4] T. Ibukiyama, T. Katsura, F. Oort, Supersingular curves of genus two and class numbers, to appear in Comp. Math.

[5] T. Katsura and F. Oort, Families of supersingular abelian surfaces, preprint.