

整数表現に関する問題

数理解析研究所 吉田知行 (Tomoyuki Yoshida)

整数表現に関連した問題として、組合せ論への応用と有限群のガロタンフェック環に関する話題を述べた。

1. 有限射影平面

最近ハイマンの O_{11} が位数 10 の射影平面は存在しないということ証明したと報告してこの方面の研究者に大きな衝撃を与えた。位数 10 というのはきわめて特殊な場合であるが、これが解ければ一般の基本予想も解けるだろうと言われるほど重要な場合である。また J.G. Thompson がさえ解けなかに、それをこの難問である。さらに、位数 10 の射影平面は点の個数が 111 個しかない、このような射影平面の非存在は原理的には (つまり超高速の計算機があれば) 解けるはずの問題である。 O_{11} の証明は残念ながら間違、これをというが、彼のこれまでの研究発表から見て証明の方針は見当がつかう。

定義. P を有限集合, $\mathcal{L}$ を P の部分集合族とする. (P の元を点, $\mathcal{L}$ の元を直線という.) 次が成立する時, $(P, \mathcal{L})$ を 有限射影平面 という.

(P.1) 相異なる 2 点を通る直線はただ 1 本だけ存在する.

(P.2) 相異なる 2 直線の交点はただ 1 点だけ.

(P.3) 退化しない 4 角形が存在する.

$(P, \mathcal{L})$ が有限射影平面なら, ある自然数 $n > 1$ があって,

(i) 各直線は $n+1$ 個の点から成る.

(ii) 各点は丁度 $n+1$ 本の直線に含まれる.

(iii) $|P| = |\mathcal{L}| = n^2 + n + 1$. (= n とおく.)

この n を $(P, \mathcal{L})$ の 位数 という.

例. 普通の射影平面 $PG(2, q) = \mathbb{F}_q^3 - \{0\} / \sim$ は上の公理を満たす. 位数は q に等しい.

基本予想. 有限射影平面の位数は素数巾である.

$A = (a_{p, \ell})_{p \in P, \ell \in \mathcal{L}}$ を $(P, \mathcal{L})$ の結合行列とする:

$$a_{p, \ell} = \begin{cases} 1 & p \in \ell \\ 0 & p \notin \ell \end{cases}$$

$J \in$, この成分も 1 の $n \times n$ 行列とする, $I \in$ は単位行列とする, このとき, 次の容易に得られる,

$$(*) \quad A^t A = nI + J,$$

逆にこの行列方程式が (0,1) 行列 A を解に持てば, A はある射影平面の結合行列である.

$$x = (x_1, \dots, x_n), \quad y := xA = (y_1, \dots, y_n) \text{ をとれば,}$$

(*) より,

$$\sum y_i^2 = n \sum x_i^2 + \left(\sum x_i \right)^2$$

だから, (*) は 2 次形式の問題ととらえることもできる.

定理 (BRC, Bruck-Ryser-Chowla, 1950)

位数 n の射影平面が存在したと仮定し, $v = n^2 + n + 1$ とあ

く, このとき,

$$(**) \quad nx^2 + (-1)^{(v-1)/2} y^2 = z^2$$

は $(0, 0, 0)$ 以外の有理整数解をもつ.

整数論によ, z , これは次のようにも書ける:

$$n = p_1 \cdots p_t n'^2 \quad (p_1, \dots, p_t \text{ は相異なる素数}), \quad n \equiv 1, 2$$

$$(\text{mod } 4) \text{ なら, } p_i = 2 \text{ または } p_i \equiv 1 (\text{mod } 4) \quad (\forall i).$$

$n \equiv 0, 3 (\text{mod } 4)$ のとき, $v \equiv 1 (\text{mod } 4)$ となり, BRC 方程式 (**) は $(0, 1, 1)$ を解にもつ. 逆に次のこともわか, z

いる (ホールの本の §10.3) .

行列方程式 (*) が $M_n(\mathbb{Q})$ に解をもつ

$\Leftrightarrow$ BRC 方程式 (**) が自明でない解をもつ .

例. $n=6$ とする有限射影平面は存在しない. しかし, $n=10, 12, 15, 18, 20, 24, 26, 28, \dots$ は BRC によ, 2 も消えない. これらのパラメータを消す方法は現在のところまったく考えられない.

定義. $(P, \mathcal{L})$: 位数 n の射影平面, $v := n^2 + n + 1 = |P|$.

$$I := \{(p, \ell) \in P \times \mathcal{L} \mid p \in \ell\} \subseteq P \times \mathcal{L}.$$

$$V := \mathbb{Z}[I] \quad : I \text{ を基底とする自由アーベル群.}$$

$\sigma, \tau \in \text{End}_{\mathbb{Z}}(V)$ を次で定義する.

$$\sigma: (p, \ell) \mapsto \sum_{\ell \in \mathcal{L}, \ell \neq \ell} (p, \ell)$$

$$\tau: (p, \ell) \mapsto \sum_{m \in \mathcal{L}: p \in m \neq \ell} (p, m)$$

σ と τ で生成された $\text{End}_{\mathbb{Z}}(V)$ の部分環 H を $(P, \mathcal{L})$ の Hecke 環 という.

H はアーベル群として基底 $\{1, \sigma, \tau, \sigma\tau, \tau\sigma, \sigma\tau\sigma\}$ を持つ自由アーベル群であり, 次の基本関係式をもつ:

$$\begin{cases} \sigma^2 = n + (n-1)\sigma \\ \tau^2 = n + (n-1)\tau \\ \tau\sigma = \sigma\tau \end{cases}$$

例. $n = q = \text{素数}$ のとき, H は A_2 型 $Weyl$ 群の Hecke 環に同型である. つまり, $G = GL_3(q)$, $B = \text{Borel} = \{\text{下三角行列}\}$ としたとき,

$$H \cong \mathbb{Z}[B \backslash G / B] \cong \text{End}_{\mathbb{Z}G}(\mathbb{Z}[G/B]).$$

以下 Hecke 環 H と $\mathbb{Z}$ の上の標準加群 V の性質をあげておく.

- ① V は忠実な H -加群.
- ② V 上の内積が, $\langle (p, \ell), (q, m) \rangle := \delta_{pq} \delta_{\ell m}$ で定義され, σ と τ はこの内積に関して自己随伴: $\langle x, \sigma y \rangle = \langle \sigma x, y \rangle$ 等.
- ③ $\sigma \mapsto \sigma, \tau \mapsto \tau$ は H の逆自己同型を与える.
- ④ $H_{\mathbb{Q}} := \mathbb{Q} \otimes_{\mathbb{Z}} H$ は半単純で, $\mathbb{Q} \oplus \mathbb{Q} \oplus M_2(\mathbb{Q})$ に同型. $H_{\mathbb{Q}}$ は 3 個の既約表現をもつ:

$$\text{ind} : \sigma \mapsto n, \tau \mapsto n$$

$$\text{st} : \sigma \mapsto -1, \tau \mapsto -1 \quad (\text{Steinberg 表現})$$

$$f : \sigma \mapsto \begin{pmatrix} -1 & 1 \\ 0 & n \end{pmatrix}, \tau \mapsto \begin{pmatrix} n & 0 \\ n & -1 \end{pmatrix}$$

⑤ $V_{\mathbb{Q}} := \mathbb{Q} \otimes_{\mathbb{Z}} V$. このとき, 上の既約表現に対応しを部分空間 $V_{\mathbb{Q}}^{\text{ind}}, V_{\mathbb{Q}}^{\text{st}}, V_{\mathbb{Q}}^+$ をとると,

$$V_{\mathbb{Q}}^{\text{ind}} = \mathbb{Q} L \quad L := \sum_{(P, \ell) \in I} (P, \ell) \in V$$

$$\dim V_{\mathbb{Q}}^{\text{st}} = n^3$$

$$V_{\mathbb{Q}} = V_{\mathbb{Q}}^{\text{ind}} \perp V_{\mathbb{Q}}^{\text{st}} \perp V_{\mathbb{Q}}^+$$

$$\dim V_{\mathbb{Q}}^+ = 2n^2 + 2n.$$

O_{tt} はこのような $H_{\mathbb{Q}}, V_{\mathbb{Q}}$ の研究によって BRC の定理の意味ある証明を得た. つまり $H_{\mathbb{Q}}$ の作用の方から $V_{\mathbb{Q}}$ に入る非退化対称二次形式の判別式 ^{α} を求め, 一方基底 I から計算される判別式は 1 なのを, $\alpha \in \mathbb{Q}^{*2}$ を得る. これから BRC が従う. 彼の方針は $\mathbb{Q}$ でなくとも適用できると思われる.

R を剰余標数 p の離散付値環 (商体は標数 p), $F := R/J(R)$ (標数 p の体) とする. O_{tt} による基本予想解決のプログラム (?) は概略次のようなものとなる.

- (1) H_R ($:= R \otimes H$) や H_F の (直) 既約表現を定める.
- (2) V_R ($:= R \otimes V$) や V_F の (直交) 直和分解 (または Witt 群のような適当なケロタンティック群での分解)
- (3) V_R, V_F の不変量 (二次形式の判別式など) の計算.

この方針でうまく行く保障はまったくないが, 標数 p として p を割る素数をとるのがよさそうである. この場合 H_R

は Gorenstein order (即ち, H_R 自身が, H_R -lattice
 のカテゴリ-で入射的) をし, $p \mid n$ のときはさらに遺伝的
 (すなわち左イデアルが射影的) で直既約 H_R -lattice は
 4 個しかないことがわかる. ($p \nmid n$ のときの H_R は有限表現
 型が示しぬ).

次に注意すべきなのは 2 次形式 $\langle, \rangle : V_R \times V_R \rightarrow R$ を
 H_R 上の非退化エルミート形式 $[\cdot, \cdot] : V_R \times V_R \rightarrow H_K$ に拡張
 してあるのがよい.

(K は R の商の体)

$(p, \ell), (z, m) \in I$ に対し, $[(p, \ell), (z, m)] \in H_K$ を

1	if $p = z, \ell = m$
σ/n	if $p \neq z, \ell = m$
τ/n	if $p = z, \ell \neq m$
$\sigma\tau/n^2$	if $p \in \ell - m, z \in \ell \cap m,$
$\tau\sigma/n^2$	if $p \in \ell \cap m, z \in m - \ell$
$\sigma\tau\sigma/n^3$	if $p \in \ell - m, z \in m - \ell$

で定義する. このとき, $u, v \in V_R$ に対し,

$$[h u, h' v] = h [u, v] \overline{h'} \quad h, h' \in H_R$$

ここで, $h \mapsto \overline{h}$ は $\alpha \mapsto \alpha^{-1}$ を動かさないう H_R の逆自己同型.

こうすると問題は H_R 上のエルミート形式の分類というお
 ピエーションになる.

以上述べたと同様のことは、 $\mathbb{Z}$ と一般の対称テンサインにも考えられる。また強正則グラフ、距離正則グラフ（ $\mathbb{Z}$ と一般の association scheme）については Hecke 環が可換なので射影平面の場合より話は簡単になる、だが簡単と言っても最後に帰着される Hecke 環上の加群と二次形式の問題は整数論がからんで来ると解きにくいことも多い。最も簡単な強正則グラフの場合、問題は実二次体（とるこの整数環）上のエルミート加群の分類になるが、これもなかなかしい（Ott の論文の § 2）

§ 2. いさゝか Hecke 環の作用.

G を有限群, H をその部分群とする. このとき,

$$(H \times H) \cdot (H \times H) := \sum_{z \in H \backslash G / H} |(H \times H, z H \times H) / H| \cdot (H \times H)$$

(ここで z は $H \backslash G / H$ の完全代表系上を動く) とすることにより,

$\mathbb{Z}[H \backslash G / H]$ は Hecke 環と呼ばれる環になる. この環は自己準同型環 $\text{End}_{\mathbb{Z}G}(\mathbb{Z}[G/H])$ に同型である:

$$(H \times H): gH \mapsto \sum_{h \in H \times H / H} gh$$

次に $H_{\mathbb{Z}G}$ は permutation $\mathbb{Z}G$ 加群のなすカテゴリーとする. これは $\mathbb{Z}G$ 加群のカテゴリー $\mathcal{M}_{\mathbb{Z}G}$ の full subcategory で, abelian で $\mathbb{Z}$ は $\mathbb{Z}$ が additive である.

もし $H_{\mathbb{Z}G}$ からアーベル群のカテゴリーへの関手 F があ

は、各 $H \leq G$ に対し、 $F(\mathbb{Z}[G/H])$ は自然に (右) $\mathbb{Z}[H \backslash G/H]$ 加群となる。良く知られた例は、 G 加群 V に対し、

$$V^H := \{v \in V \mid v \cdot g = v \quad \forall g \in H\}$$

が $\mathbb{Z}[H \backslash G/H]$ 加群になることである。この作用は関手 $\mathbb{Z}X \mapsto \text{Map}_G(X, V)$ から従う。Hecke 環の作用をこのようにとらえる論文がいくつか出ている。

S/R を可換環の有限次加群 A 拡大、この加群 A を G とする。 $R = S^G$ である。(このような拡大の例としては、付数体の有限次加群 L/K に対し、 R と S を L と K 、 L の整数環とすれば、 L/K が不分岐のとき、 S/R が加群 A 拡大になる)。このとき、

定理. (Roggenkamp-Scott, Ford など) $\forall H \leq G$ に対し、 $\mathcal{L}(S^H)$, $\text{Pic}(S^H)$, $B_r(S^H)$, $\mathcal{C}(L^H)$ は $\mathbb{Z}[H \backslash G/H]$ 加群である。これは関手 $H_{\mathbb{Z}G} \rightarrow \underline{\text{Ab}} : \mathbb{Z}[H \backslash G] \mapsto \mathcal{L}(S^H), \text{Pic}(S^H), B_r(S^H), \mathcal{C}(L^H)$ から得られる。($\mathcal{C}(L^H)$ は付数体の場合の類群)。

この定理の証明には本質的なのは、トレースとカノールと transfer と呼ばれる写像が存在しこれを用いる Mackey 分解をみることである。

さて、このような Hecke 環の作用と、有限群の置換表現の理論を組み合わせよう。

L/K を代数体のガロア群, G をガロア群, $p \neq 2$ を素数,
 H を G の $(2, 2)$ 型の部分群, $H_0, \dots, H_g$ を H の位数 2 の部
 分群とする. $\mathbb{Z}_p$ を p 進整数環とする. このとき, 次の同型
 がある.

$$\mathbb{Z}_p G \oplus (\mathbb{Z}_p[G/H])^{(g)} \cong \bigoplus_{i=0}^{g-1} \mathbb{Z}_p[G/H_i].$$

この同型に上の関手を作用させると, 例えば,

$$C(K)_p \oplus (C(K^H))_p^{(g)} \cong \bigoplus_{i=0}^{g-1} (C(K^{H_i}))_p$$

を得る. ここで $C(K)_p$ は類群の Sylow p 群, 位数 2 とすると
 良く知られた類数の関係が得られる.

同様に ζ -関数の間の等式がある:

$$\zeta_K(s) \zeta_{L^H(s)}^2 = \prod_{i=0}^{g-1} \zeta_{L^{H_i}}(s)$$

Wieferich の位数公式も同じ形をもちうるが, これも同じ
 方法で証明される: $A \leq \text{Aut}(G)$, $(|A|, |G|) = 1$, $A \cong (\mathbb{Z}/2\mathbb{Z})^g$,
 2 は素数のとき,

$$|C_G(A)| = |G|^{-g} \prod_{1 \neq B \leq A} |C_G(B)|.$$

§3. 置換加群の同型と induction 定理.

一般には, 有限 G 集合 X, Y が $\mathbb{Z}X \cong \mathbb{Z}Y$ ($\mathbb{Z}G$ 加群と

(2) であつても, $X \cong Y$ とは言えない. 有限 G 集合のカテゴリの直和と直積に関する Grothendieck 環を Burnside 環といい, $\Omega(G)$ で表わす. 有限生成 $\mathbb{Z}G$ 加群のカテゴリの直和とテンソル積に関する Grothendieck 環を表現環といい $\alpha(G)$ で表わす. 自然な環準同型 $f: \Omega(G) \rightarrow \alpha(\mathbb{Z}G)$: $[X] \mapsto [\mathbb{Z}X]$ がある.

定理 (Dress) $f: \Omega(G) \rightarrow \alpha(G)$ が単射

$\Leftrightarrow$ (*) ある素数 p と正規 p -部分群 P に對し,

G/P が巡回群.

したが, $\mathbb{Z}G$ が (*) を満たさないなら, ある有限 G 集合 X と Y が存在して, $X \neq Y$ だが $\mathbb{Z}X \cong \mathbb{Z}Y$ となる. この事実が前節の考えを右用してよい.

L/K は代数体の有限次ガロア拡大, G をそのガロア群とする. X と Y を有限 G 集合で $\mathbb{Z}X \cong \mathbb{Z}Y$ なるものとする. このとき $\text{Map}_G(X, L)$ は中間体の直和である (実際, $X \cong G/H_1 + \dots \Rightarrow \text{Map}_G(X, L) \cong L^{H_1} \times \dots$). しかも $\mathbb{Z}X \cong \mathbb{Z}Y$ より, $\text{Map}_G(X, L) \cong \text{Map}_G(Y, L)$ (K 多元環として) が得られる. よく K 類群をとると,

$$\mathcal{C}(\text{Map}_G(X, L)) \cong \mathcal{C}(\text{Map}_G(Y, L)).$$

同様の同型が, ブラウアー群 Br , ピカール群 Pic , 単素群 U さらに高次のコホモロジー群についても得られる.

と、(*) を満たさない群 G が与えられたとき、 $X \neq Y$ だが $\mathbb{Z}X \cong \mathbb{Z}Y$ となる有限 G 集合 X, Y を求めたい。このために Burnside 環の中等元公式が使えろ。

定理. G は有限群、 μ は G の部分群束の Möbius 関数とする。

(i) $\mathbb{Q} \otimes_{\mathbb{Z}} \Omega(G)$ の原始中等元は、

$$e_{G,H} := \frac{1}{|N_G(H)|} \sum_{D \leq H} |D| \mu(D, H) [G/D]$$

の形をしている。ここで $H \leq G$ なら、 H と H' が共役 $\Leftrightarrow e_{G,H} = e_{G,H'}$ 。したがって、 $\mathbb{Q} \otimes \Omega(G)$ の原始中等元 $\longleftrightarrow G$ の部分群の共役類。

(ii) p は素数、 $\mathbb{Z}_{(p)} := \{a/b \in \mathbb{Q} \mid a \in \mathbb{Z}, b \in \mathbb{Z} - p\mathbb{Z}\} \subseteq \mathbb{Q}$ とおく。このとき、 $\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \Omega(G)$ の原始中等元は、

$$e_{G,H}^p = \sum_{(K): O^p(K) \sim H} e_{G,K}$$

の形をしている。ここで、 $O^p(K) = \langle p\text{-element of } K \rangle$ 、 (K) は G の部分群の共役類で $O^p(K)$ と H が共役なものを選ぶ。

この公式は Gluck, 吉田によっても得られる。次が目標の定理である。

定理. G を有限群, H をその部分群とする.

(i) p を素数 p に対し $H/O_p(H)$ は巡回群となる.

ここで $O_p(H)$ は最大の正規 p 部分群.

$$|G| \cdot e_{G,H} = [X] - [Y]$$

をたす G 集合 X, Y をとる, このとき $\mathbb{Z}X \cong \mathbb{Z}Y$.

(ii) p を素数とし, $H/O_p(H)$ は巡回群でなく, $O^p(H) = H$

(即ち H は指数 p の正規部分群をもたない) とする.

$$|G| \cdot e_{G,H}^p = [X] - [Y]$$

をたす G 集合 X, Y をとる, このとき $\mathbb{Z}_{(p)}X \cong \mathbb{Z}_{(p)}Y$.

証明の概略. Dress による induction 定理 (後述) によれば,

は,

$$|G| \cdot 1_G = \sum_i a_i [\text{Ind}_{H_i}^G(M_i)], \quad \text{in } \mathbb{Z}G$$

ここで $a_i \in \mathbb{Z}$, $H_i \leq G$, $H_i/O_{p_i}(H_i)$ は巡回群 (p_i は素数), M_i は $\mathbb{Z}H_i$ 加群, とする. Frobenius の相互律より

$$f(e_{G,H}) [\text{Ind}_{H_i}^G(M_i)]$$

$$= \text{Ind}_{H_i}^G(f(\text{Res}_{H_i}^G(e_{G,H})) \cdot [M_i])$$

しかし H の共役は H_i に入らなうので, $\text{Res}_{H_i}^G(e_{G,H}) = 0$. よ

$$, \quad f(e_{G,H}) [\text{Ind}_{H_i}^G(M_i)] = 0 \quad \therefore |G| f(e_{G,H}) = 0.$$

これは $[\mathbb{Z}X] = [\mathbb{Z}Y]$, 即ち $\mathbb{Z}X \cong \mathbb{Z}Y$ を意味する.

(ii) も同様に証明される.

5.4. 文献紹介.

有限群と order の整数表現の概説は Reiner による [1] と [2] がくわしい. [2] は introduction に 11 個の問題点があり, この方面で重要な問題点がわかるのがありがたい. また [2] はやさしく書かれていて読みやすい. 文献のリストは [1] と [3] に多数の, 2 つある. [3] は歴史的文献も含んでいる. [3] は各分野 (2 次形式, 代数的整数論, 虚数乗法論, トポロジー, 結晶理論) において整数表現がどのように現れられているかを紹介している. 整数表現全般については, [4] ~ [7] も役に立つ. [5] は新しい情報も含んでいる. この続巻もまもなく出版されるという.

K 理論との関係では [8], [9], [10] がある.

有限幾何については [11], [12].

13 の Hecke action については [13] ~ [16].

Burnside 環については [17], [18], [19]. 中身元公式の induction 定理への応用については [20]. [22] は読みにくいがきわめて含蓄に富んでいる.

相対 Grothendieck 環については [23], [24]. Lam と Reiner の一連の論文はこの方面の問題点を明らかにしている.

References

1. I. Reiner, A survey of integral representation theory,
Bull. A. M. S. 76 (1970), 159-227.
2. I. Reiner, Topics in integral representation theory,
Springer Lecture Notes 744 (1979), 1-143.
3. W. H. Gustafson, Remarks on the history and applications
of integral representations, Springer Lecture Notes 882
(1980), 1-36.
4. C.W.Curtis-I.Reiner, Representation theory of finite
groups and associative algebras, Interscience, New York, 1962.
5. C.W.Curtis-I.Reiner, Methods of representation theory I,
Interscience, New York, 1981.
6. I.Reiner, Maximal order, Academic Press, London, 1975.
7. K.Roggenkamp, Lattices over orders I,II, Springer Lecture
Notes 115 (1970) and 142 (1970).
8. H.Bass, Algebraic K-theory, Benjamin, New York, 1968.
9. Milnor, Introduction to algebraic K-theory, Princeton, 1971.
10. R.Swan-E.Evans, K-theory of finite groups and orders,
Springer Lecture Notes 149 (1970).
11. U.Ott, Some remarks on representation theory in finite
geometry, Springer Lecture Notes, 893 (1981).
12. M.Hall, Combinatorial theory, Blaisdell, 1967.

13. T. Yoshida, On G-functor II : Hecke operators and G-functors,
J. Math. Soc. Japan, 35 (1983), 179-190.
14. D. Husemoller, Burnside ring of a Galois group and the
relations between zeta functions of intermediate fields,
Proc. Symp. in Pure Math., 37 (1980), 603-610.
15. K. Roggenkamp-L. Scott, Hecke action on Picard groups,
J. Pure Appl. Algebra 26 (1982), 85-100.
16. T.J.Ford, Hecke actions on Brauer groups, J. Pure Appl.
Algebra 33 (1984), 11-17.
17. C. Walter, Brauer's class number relation, Acta Arith.
35 (1979), 33-40.
18. R. Perlis, On the class numbers of arithmetically
equivalent fields, J. Number theory 10 (1978), 488-509.
19. D. Gluck, Idempotent formula for the Burnside algebra
with applications to the p-subgroup simplicial complex,
Illinois J. Math. 25 (1981), 63-67.
20. T. Yoshida, Idempotents of Burnside rings and Dress
induction theorem, J. Algebra 80 (1983), 90-105.
21. T. tom Dieck, Transformation groups and representation
theory, Lectur Notes in Math. 766, Springer, Berlin, 1979.
22. A. Dress, Contributions to the theory of induced
representations, Springer Lecture Notes 342 (1973), 183-240.

23. A.Dress, On relative Grothendieck rings, Springer Lecture Notes 488 (1974), 79-131.
24. T.Y.Lam-I.Reiner, Restriction maps on relative Grothendieck rings, J.Algebra, 14 (1970), 260-298.