数理解析研究所講究録
630巻 1987年 14-33

Z_4の拡大環から得られるHadamard差集合

東京女子大・文理　山田美枝子 (Mieko Yamada)
東京女子大・文理　山本幸一 (Koichi Yamamoto)

§1. Hadamard 差集合.

1. 既知の結果.

<u>定理A</u> (Mann). v が2巾の非自明な (v, k, λ) ブロックデザインのパラメータは

$$v = 2^{2s},\quad k = 2^{s-1}(2^s \pm 1),\quad \lambda = 2^{s-1}(2^{s-1} \pm 1),\quad n = 2^{2s-2}$$

で与えられるものに限る. その関連行列で成分0を -1 で置き換えたものは 2^{2s} 次の正則 (regular) な Hadamard 行列である すなわち行和が一定 $\pm 2^{s-1}$ になる.

<u>定理B</u> (Turyn, 山本ら). 位数 2^{2s} のアーベル群Gの上に $(2^{2s}, 2^{s-1}(2^s-1), 2^{s-1}(2^{s-1}-1))$ 差集合があれば, Gの指数(exponent) h について $h \leqq s+1$ となる.

<u>定義</u>. 上のパラメーターを持つ差集合を, G上の<u>Hadamard差集合</u>という.

<u>定理C</u> 位数がそれぞれ 2^{2s_1}, 2^{2s_2} のアーベル群 G_1, G_2 の上

の Hadamard 差集合 D_1, D_2 があれば

$$D_1 \times D_2' \cup D_1' \times D_2$$

は直積 $G_1 \times G_2$ 上の Hadamard 差集合である. ' は余集合を示す.

<u>定理 D</u> (Turyn) 有限体 $K = GF(2^s)$ で, $K \times K$ の中で

$$(l+m,\ lm) \qquad (l \neq m)$$

なる対の集合は, 群 $K \times K$ 上の Hadamard 差集合である.

2. 定理 B から $s \geqq 2$ ならば, $v = 2^{2s}$ なる巡回 Hadamard 差集合は存在しないし, 定理 D に見るように基本アーベル群上には対応する Hadamard 差集合が存在する.

本稿では 4 位巡回群 $\mathbf{Z}_4$ s 個の直積 $\mathbf{Z}_4^s$ 上に Hadamard 差集合を構成する. それは Liebler-Mena の取扱った環 $\mathbf{Z}_4 = \mathbf{Z}/4\mathbf{Z}$ の代数拡大 $\mathfrak{R}$ の性質を用いて行われる.

3. 一般に加法群 G の群環 $\mathbf{Z}G$ の元 $\sum_{\alpha \in G} c_\alpha \alpha$ と, G 上に定義された, 値域 $\mathbf{Z}$ の函数 f : $f(\alpha) = c_\alpha$ を同一視する. たとえば G はまた G 上いたる所で 1 なる値を取る函数をも表わす. また $\mathbf{O}$ は 0 の特性函数を表わす. すなわち

$$\mathbf{O}(0) = 1, \quad \mathbf{O}(\alpha) = 0 \qquad (\alpha \neq 0).$$

G 上の 2 つの函数 f, g からその convolution 積 $f * g$ を

$$(f * g)(\alpha) = \sum_{\beta \in G} f(\beta) g(\alpha - \beta)$$

で定義する. また f の共役 $\hat{f}$ は

$$\hat{f}(\alpha) = f(-\alpha)$$

から定義されるものとする.

この記号によれば，アーベル群Gの部分集合Dが(v, k, λ)差集合であるという条件は

(1) $$D * \hat{D} = n\mathbf{O} + \lambda G$$

と書き直すことができる. むろん $n = k - \lambda$.

4. アーベル群Gの（加法的）指標μは$\mu(\alpha)$が1のv乗根で

$$\mu(\alpha+\beta) = \mu(\alpha)\mu(\beta)$$

をみたすもののことであるが，μは$f = \sum_{\alpha \in G} f(\alpha)\alpha$のとき

(2) $$\mu(f) = \sum_{\alpha \in G} f(\alpha)\mu(\alpha)$$

とおくことによって，群環$\mathbf{Z}G$上に拡張できる. そして

$$f = 0 \iff \text{“凡ての指標}\mu\text{について}\ \mu(f) = 0\text{”}.$$

指標μの全体は位数vの群で，Gの元αの特性函数l_α

$$l_\alpha(\beta) = 1 \quad (\beta = \alpha \text{ のとき}),$$
$$= 0 \quad (\beta \neq \alpha \text{ のとき})$$

は

$$l_\alpha = \frac{1}{v}\sum_{\mu \in M} \bar{\mu}(\alpha)\mu$$

となる. Mは指標群. 上式は指標の直交関係と呼ばれるものである.

前出convolution積は，群環$\mathbf{Z}G$の元としての積に当る. したがって，Gの指標μについて

$$\mu(f * g) = \mu(f)\mu(g),$$

$$\mu(\hat{f}) = \overline{\mu(f)} \qquad \text{— : 共役複素数}$$

§2. $\mathbf{Z}_4$ の拡大環 $\mathfrak{R}$

5. $F = GF(2)$, $K = GF(2^s)$, $s \geqq 2$ とし，F 上の monic 原始多項式

(3) $$f(x) = x^s + c_1 x^{s-1} + \cdots + c_s$$

にたいて，係数 $c_1, \cdots, c_s$ を mod 4 で動かし，その根 ξ が

$$\xi^{2^s-1} = 1$$

を満たすようにすることができる．ξ を $\mathbf{Z}_4$ に添加して生ずる $\mathbf{Z}_4$ の代数的拡大環 $\mathbf{Z}_4(\xi)$ を $\mathfrak{R}$ で表わす．

この環 $\mathfrak{R}$ は $\mathbf{Z}_4$ 上 s 次代数的で，根基 (radical) $\mathfrak{N} = 2\mathfrak{R}$ をもち，剰余類体 $\mathfrak{R}/\mathfrak{N}$ は $K = GF(2^s)$ である．剰余類体の代表は，いわゆる Teichmüller 代表系

(4) $$\mathfrak{Z} = \{0, 1, \xi, \xi^2, \cdots, \xi^{2^s-2}\}$$

から取ることができる．$\mathfrak{Z}$ はまた $\mathfrak{R}$ の中で，方程式

$$x^{2^s} = x$$

の根であるものの全体となる．

この代表系を用いれば，$\mathfrak{R}$ の元 α が，一意的に

$$\alpha = \alpha_0 + 2\alpha_1, \qquad \alpha_0, \alpha_1 \in \mathfrak{Z}$$

と書き表わされる．

しばらく α によって定まる α_0 を $\alpha_0 = \tau(\alpha)$ と書くことに

する.

$\mathfrak{R}$ の正則元（逆元を持つもの）の全体 $\mathfrak{R}^* = \mathfrak{R} - \mathfrak{N}$ は $2^5(2^5-1)$ 位の群で，$\alpha \in \mathfrak{R}^*$ に対して

$$\alpha \longrightarrow \tau(\alpha)$$

は，$\mathfrak{R}^*$ から $\{\xi\}$ の上への準同型写像である．その核は，$\tau(\alpha) = 1$ なる α，すなわち

$$1 + 2\beta, \qquad \beta \in \mathfrak{Z}$$

の形の元，いわゆる主単数 (principal unit) の作る主単数群 $\mathcal{E}$ である．なお主単数 $1+2\beta$ においては β が $\mathfrak{R}/\mathfrak{N} = K$ の元とみなすことも便利であるから，主単数は $1+2l$, $l \in K$ の形に書くことにする．ここで

$$(1+2l)(1+2m) = 1 + 2(l+m) \qquad (l, m \in K)$$

によって，主単数群 $\mathcal{E}$ は，K の加法群と同型である．そして，$\mathfrak{R}^*$ は $\{\xi\}$ と $\mathcal{E}$ の直積である．

6. $\mathfrak{R}$ の元 $\alpha = \alpha_0 + 2\alpha_1$ に

$$\alpha^F = \alpha_0^2 + 2\alpha_1^2$$

を対応させると，F は環 $\mathfrak{R}$ の自己同型である．

これを $\mathfrak{R}$ の <u>Frobenius 自己同型</u> と呼ぶ

[証明] $(\alpha\beta)^F = \alpha^F \beta^F$ は簡単である．$\alpha = \alpha_0 + 2\alpha_1$, $\beta = \beta_0 + 2\beta_1$ ならば $\alpha\beta = \alpha_0\beta_0 + 2(\alpha_0\beta_1 + \alpha_1\beta_0)$, $\alpha_0\beta_0 \in \mathfrak{Z}$ で，

$$(\alpha\beta)^F = (\alpha_0\beta_0)^2 + 2(\alpha_0\beta_1 + \alpha_1\beta_0)^2 = \alpha_0^2\beta_0^2 + 2\alpha_0^2\beta_1^2 + 2\alpha_1^2\beta_0^2$$

$= \alpha^F \beta^F$

$(\alpha+\beta)^F = \alpha^F + \beta^F$ を確めるのに，$\tau(\alpha)$ の具体形を必要とする．

(5) $\tau(\alpha) = \alpha^{2^s}$.

(6) $\tau(\alpha+\beta) = \tau(\alpha) + \tau(\beta) + 2\alpha^{2^{s-1}}\beta^{2^{s-1}}$.

何となれば $\alpha = \alpha_0 + 2\alpha_1$ より $\alpha^{2^s} = \alpha_0^{2^s} = \alpha_0$ でこれが (5) である．

したがって

$$\tau(\alpha+\beta) = (\alpha+\beta)^{2^s} = \alpha^{2^s} + \beta^{2^s} + 2\alpha^{2^{s-1}}\beta^{2^{s-1}} = \alpha_0 + \beta_0 + 2\alpha^{2^{s-1}}\beta^{2^{s-1}},$$

$$\alpha+\beta = (\alpha_0 + \beta_0 + 2\alpha^{2^{s-1}}\beta^{2^{s-1}}) + 2(\alpha_1 + \beta_1 + \alpha^{2^{s-1}}\beta^{2^{s-1}}),$$

$$(\alpha+\beta)^F = (\alpha_0 + \beta_0 + 2\alpha^{2^{s-1}}\beta^{2^{s-1}})^2 + 2(\alpha_1 + \beta_1 + \alpha^{2^{s-1}}\beta^{2^{s-1}})^2$$

$$= (\alpha_0+\beta_0)^2 + 2(\alpha_1^2 + \beta_1^2 + \alpha^{2^s}\beta^{2^s}) = \alpha_0^2 + \beta_0^2 + 2(\alpha_1^2 + \beta_1^2)$$

$$= \alpha^F + \beta^F.$$

これから ξ と共に $\xi^F, \xi^{F^2}, \cdots, \xi^{F^{s-1}}$ が原始多項式 (3) の根となる．しかし他には根がない．(3) の根は mod $\mathfrak{P}$ では，$\xi, \xi^F, \cdots, \xi^{F^{s-1}}$ のいずれかであるから，$\xi^{2^t} + 2\beta$ が根ならば，

$$0 = f(\xi^{2^t} + 2\beta) = f(\xi^{2^t}) + 2f'(\xi^{2^t})\beta = 0,$$

$f'(\xi^{2^t})\beta = 0$ であるが，$f'(\xi^{2^t}) \neq 0$ (K において) だから，$\beta = 0$ でなければならない．

また Frobenius 自己同型で不変なものは Z_4 の元に限る．

$\alpha = \alpha_0 + 2\alpha_1$, $\alpha^F = \alpha_0^2 + 2\alpha_1^2$ ならば $\alpha_0^2 = \alpha_0$, $\alpha_1^2 = \alpha_1$ で Teichmüller 系 (4) の元だから，$\alpha_0 = 0$ 又は 1，$\alpha_1 = 0$ 又は 1．よって $\alpha = 0, 1, 2, 3$ のいずれかとなる．

ゆえに $\mathfrak{R}$ の自己同型は Frobenius 自己同型 F の巾だけで，$\mathfrak{R}$ の自己同型群は F の生成する s 位巡回群となる．

7. $\mathfrak{R}$ の元 α の相対トレース $S_{\mathfrak{R}/\mathbf{Z}_4}\alpha$ を

$$S_{\mathfrak{R}/\mathbf{Z}_4}\alpha = \alpha + \alpha^F + \alpha^{F^2} + \cdots + \alpha^{F^{s-1}}$$

で定義すると，値は $\mathbf{Z}_4$ に属して，むろん

$$S_{\mathfrak{R}/\mathbf{Z}_4}(\alpha+\beta) = S_{\mathfrak{R}/\mathbf{Z}_4}\alpha + S_{\mathfrak{R}/\mathbf{Z}_4}\beta.$$

これは F 上 K の元 a の相対トレース

$$S_{K/F}\, a = a + a^F + a^{F^2} + \cdots + a^{F^{s-1}}$$

と類似であるが，$\alpha = \alpha_0 + 2\alpha_1$ とすると α_0 を K の元とみて，

$$S_{\mathfrak{R}/\mathbf{Z}_4}\alpha \equiv S_{K/F}\,\alpha_0 \qquad (\mathrm{mod}\ \mathfrak{R})$$

§3. $\mathfrak{R}$ の加法的指標，乗法的指標，Gauss の和および Jacobi の和．

8. K を F 上のベクトル空間とみて

$$f(x, y) = S_{K/F}\, xy$$

は非退化双一次形式である．非退化とは

凡ての $a \in K$ について $S_{K/F}(ba) = 0 \implies b = 0$

の意味で，その真であることは $S_{K/F}(c) = 1$ なる $c \in K$ が存在することから分る．もしすべての c について $S_{K/F}(c) = 0$ ならば，

$$c + c^2 + c^4 + \cdots + c^{2^{s-1}} = 0$$

で，2^{s-1} 次の多項式 $x^{2^{s-1}} + x^{2^{s-2}} + \cdots + x^2 + x$ が 2^s 個の根を持つこと

となって矛盾する.

したがって K から F への '1次函数' g は, ある b につき,

$$g(a) = S_{K/F}(ba) \qquad (a \in K)$$

の形に書かれる. したがってまた, 加法群 K の加法的指標は

$$(7) \qquad \lambda(a) = (-1)^{S_{K/F}(la)} \qquad (a \in K)$$

の形である. この指標を λ_l で表わすことにする.

次に $\mathfrak{R}$ から, 基礎環 $\mathbf{Z}_4$ への1次函数 g は, ある β につき

$$g(\alpha) = S_{\mathfrak{R}/\mathbf{Z}_4}(\beta\alpha) \qquad (\alpha \in \mathfrak{R})$$

の形をしている.

実際 $S_{\mathfrak{R}/\mathbf{Z}_4}(\beta\alpha)$ が1次函数であるのは明白だが, なお

凡ての α について $S_{\mathfrak{R}/\mathbf{Z}_4}(\beta\alpha) = 0 \Longrightarrow \beta = 0$.

何となれば $\alpha = \alpha_0 + 2\alpha_1$, $\beta = \beta_0 + 2\beta_1$ のとき

$$S_{\mathfrak{R}/\mathbf{Z}_4}(\beta\alpha) = S_{K/F}(\beta_0\alpha_0) = 0$$

がすべての α_0 について成立ち $\beta_0 = 0$. よって $\beta = 2\beta_1$ だが

$S_{\mathfrak{R}/\mathbf{Z}_4}(2\beta_1\alpha) = 0$, $S_{\mathfrak{R}/\mathbf{Z}_4}(\beta_1\alpha) = 0$ がすべての α について成立つ

ので $\beta_1 = 0$, 結局 $\beta = 0$ となる.

したがってまた, $\mathfrak{R}$ の加法的指標は, ある β について

$$(8) \qquad \lambda(\alpha) = \mathbf{i}^{S_{\mathfrak{R}/\mathbf{Z}_4}(\beta\alpha)} \qquad (\mathbf{i} = \sqrt{-1})$$

の形をしていることが分る. 上の指標は λ_β と書くことにする. たとえば

$$\lambda_l(a) = \lambda_1(la) \qquad (l, a \in K),$$

$$\lambda_\beta(\alpha)=\lambda_1(\beta\alpha) \qquad (\alpha,\beta\in\mathfrak{R})$$

が成立し，指標の直交関係から

$$(9) \qquad \sum_{\ell\in K}(-1)^{S_{K/F}(\ell a)}=2^s \qquad (a=0 \text{ のとき}),$$
$$=0 \qquad (a\neq 0 \text{ のとき}).$$

$$(10) \qquad \sum_{\beta\in\mathfrak{R}} i^{S_{\mathfrak{R}/Z_4}(\beta\alpha)}=2^{2s} \qquad (\alpha=0 \text{ のとき}),$$
$$=0 \qquad (\alpha\neq 0 \text{ のとき})$$

を得る.

9. $\mathfrak{R}^*$ の指標 χ は，取る値が 1 の $2(2^s-1)$ 乗根で

$$\chi(\alpha\beta)=\chi(\alpha)\chi(\beta) \qquad (\alpha,\beta\in\mathfrak{R}^*)$$

をみたすものである．それらは乗法を自然的に定義するとき，$\mathfrak{R}^*$ と同型な，指標群 X を構成する．

$\mathfrak{R}^*$ の指標 χ は $\alpha\in\mathfrak{R}$ については $\chi(\alpha)=0$ と定義してしまって，$\mathfrak{R}$ 全体で定義されたものと見ることにする．これを $\mathfrak{R}$ の指標，または加法的指標と区別するために，$\mathfrak{R}$ の乗法的指標と呼ぶ．

$$\chi_0(\alpha)=1 \qquad (\alpha\in\mathfrak{R}^*)$$

なるものが単位指標 χ_0 である．

本稿では χ の取る値が実数である，つまり ± 1 である指標を取り扱かう．これら<u>実指標</u>は，$\mathfrak{R}^*$ の部分群 $\{\xi\}$ 上では値 1 を取り，結局主単数群 $\mathfrak{E}$ の指標であるに過ぎない．すなわち，

$$\chi((1+2a)\xi^m)=\chi(1+2a).$$

χ は主単数群 $\mathfrak{E}$ 上の指標である. $\psi(a)=\chi(1+2a)$ とおけば ψ は K の加法群の指標で **8** に示したように $\psi(a)=(-1)^{S_{K/F}(la)}$ ならしめる $l\in K$ がある. その l によって

$$\chi=\chi_l$$

と書くことにする. すなわち

$$\chi_l((1+2a)\xi^m)=(-1)^{S_{K/F}(la)}$$

またむろん

$$\chi_l\chi_m=\chi_{l+m}$$

で, 実指標の乗法群と K の加法群が同型である.

10. $\mathfrak{R}$ の指標 χ から, **4**, (2) の線に沿って, 和

$$G(\chi)=\lambda_1(\chi)=\sum_{\alpha\in\mathfrak{R}^*}\chi(\alpha)\lambda_1(\alpha)$$

を作り, これを χ に属する <u>Gauss の和</u> と呼ぶ.

<u>定理 1.</u> χ が実指標 χ_l, $l\neq 0$ ならば

$$G(\chi_l)=2^s\mathbf{i}^{S_{\mathfrak{R}/Z_4}l^{2^s}}$$

[証明] $$\lambda_1(\chi_l)=\sum_{m=0}^{2^s-2}\sum_{a\in K}(-1)^{S_{K/F}(la)}\mathbf{i}^{S_{\mathfrak{R}/Z_4}((1+2a)\xi^m)}$$

$$=\sum_{m=0}^{2^s-2}\mathbf{i}^{S_{\mathfrak{R}/Z_4}\xi^m}\sum_{a\in K}(-1)^{S_{K/F}(l+\xi^m)a}$$

内側の和は (9) によって $l+\xi^m\equiv 0 \pmod{\mathfrak{R}}$ なる m についてのみ, 値 2^s を取り, 他では 0 となる. そのような ξ^m はちょうど $\tau(l)$ で, (5) から $\xi^m=l^{2^s}$. したがって

$$G(\chi_l)=\lambda_1(\chi_l)=2^s\mathbf{i}^{S_{\mathfrak{R}/Z_4}l^{2^s}}.$$

11. 実指標 χ_ℓ の間の convolution 積が必要である.

<u>定理 2.</u> $\chi_0 * \chi_0 = (2^{2s} - 2^s)\mathbf{1} - 2^s \chi_0$.

$\ell \neq 0$ ならば $\chi_0 * \chi_\ell = 0$,

$$\chi_\ell * \chi_\ell = \chi_\ell(-1)\left(2^{2s}\mathbf{0} - 2^s(\mathbf{1} - \chi_0)\right).$$

$\ell, m, \ell + m \neq 0$ ならば $\chi_\ell * \chi_m = \chi_{\ell m}(-1)\, 2^s \chi_{\ell+m}$.

ここに $\mathbf{1}$ は到るところ 1 を取る函数である.

[証明] $\alpha \in \mathfrak{R}^*$ ならば

$$(\chi_0 * \chi_0)(\alpha) = \sum_{\beta \in \mathfrak{R}} \chi_0(\beta)\chi_0(\alpha - \beta) = \sum_{\beta \in \mathfrak{R}} \chi_0(\alpha\beta)\,\chi_0(\alpha - \alpha\beta)$$

$$= \sum_{\beta \in \mathfrak{R}} \chi_0(\beta)\,\chi_0(1 - \beta) = \sum_{\beta - 1 \in \mathfrak{R}^*} \chi_0(\beta) = \sum_{\beta \in \mathfrak{R}} \chi_0(\beta) - \sum_{\beta - 1 \in \mathfrak{R}} \chi_0(\beta)$$

$$= \sum_{\beta \in \mathfrak{R}^*} \chi_0(\beta) - \sum_{\beta \in \mathcal{E}} \chi_0(\beta) = \#\mathfrak{R}^* - \#\mathcal{E} = 2^{2s} - 2^{s+1}.$$

$\alpha \in \mathfrak{R}$ ならば

$$(\chi_0 * \chi_0)(\alpha) = \sum_{\beta \in \mathfrak{R}^*} \chi_0(\beta)\,\chi_0(\alpha - \beta) = \#\mathfrak{R}^* = 2^{2s} - 2^s.$$

これより $\chi_0 * \chi_0 = (2^{2s} - 2^s)\mathbf{1} - 2^s \chi_0$ を得る.

同様にして, $\alpha \in \mathfrak{R}^*$ ならば

$$(\chi_\ell * \chi_0)(\alpha) = \sum_{\beta \in \mathfrak{R}} \chi_\ell(\beta)\,\chi_0(\alpha - \beta) = \sum_{\beta \in \mathfrak{R}} \chi_\ell(\alpha\beta)\,\chi_0(\alpha - \alpha\beta)$$

$$= \chi_\ell(\alpha) \sum_{\beta \in \mathfrak{R}} \chi_\ell(\beta)\,\chi_0(1 - \beta) = \chi_\ell(\alpha) \sum_{\beta - 1 \in \mathfrak{R}^*} \chi_\ell(\beta) = \chi_\ell(\alpha)\left(\sum_{\beta \in \mathfrak{R}} \chi_\ell(\beta) - \sum_{\beta \in \mathcal{E}} \chi_\ell(\beta)\right)$$

$$= 0 - 0 = 0.$$

$\alpha \in \mathfrak{R}$ ならば

$$(\chi_\ell * \chi_0)(\alpha) = \sum_{\beta \in \mathfrak{R}^*} \chi_\ell(\beta)\,\chi_0(\alpha - \beta) = \sum_{\beta \in \mathfrak{R}^*} \chi_\ell(\beta) = 0.$$

したがって $\chi_\ell * \chi_0 = 0$ を得る

また，$\alpha\in\mathfrak{R}^*$ ならば

$$(\chi_\ell * \chi_\ell)(\alpha)=\sum_{\beta\in\mathfrak{R}}\chi_\ell(\alpha\beta)\chi_\ell(\alpha-\alpha\beta)=\sum_{\beta\in\mathfrak{R}^*}\chi_\ell(\beta)\chi_\ell(1-\beta)$$

$$=\sum_{\beta\in\mathfrak{R}^*}\chi_\ell\left(\frac{1-\beta}{\beta}\right)=\sum_{\beta\in\mathfrak{R}^*}\chi_\ell\left(-1+\frac{1}{\beta}\right)=\sum_{\beta\in\mathfrak{R}^*}\chi_\ell(-1+\beta)$$

$$=\sum_{\beta\in\mathfrak{R}}\chi_\ell(\beta)-\sum_{\beta\in\mathfrak{R}}\chi_\ell(-1+\beta)=0-0=0.$$

$\alpha\in\mathfrak{R}$ ならば，$\alpha=2a$，$a\in K$ とおいて，$a\neq 0$ の時には

$$(\chi_\ell * \chi_\ell)(2a)=\sum_{\beta\in\mathfrak{R}^*}\chi_\ell(\beta)\chi_\ell(2-\beta)=\sum_{\beta\in\mathfrak{R}^*}\chi_\ell\left(-1+\frac{2}{\beta}\right)$$

$$=\sum_{\beta\in\mathfrak{R}^*}\chi_\ell(-1+2\beta)=\sum_{\beta\in\mathfrak{R}}\chi_\ell(\beta)-\sum_{\beta\in\mathfrak{R}}\chi_\ell(-1+2\beta)=-\chi_\ell(-1)\#\mathfrak{R}$$

$$=-\chi_\ell(-1)2^s.$$

$\alpha=0$ については

$$(\chi_\ell * \chi_\ell)(0)=\sum_{\beta\in\mathfrak{R}^*}\chi_\ell(\beta)\chi_\ell(-\beta)=\chi_\ell(-1)\#\mathfrak{R}^*=\chi_\ell(-1)(2^{2s}-2^s).$$

したがって

$$\chi_\ell * \chi_\ell=\chi_\ell(-1)\left((2^{2s}-2^s)\mathbf{0}-2^s(\mathbf{1}-\chi_0)\right)$$

を得る．

最後に $\chi_\ell * \chi_m$ については，$\alpha\in\mathfrak{R}^*$ ならば

$$(\chi_\ell * \chi_m)(\alpha)=\sum_{\beta\in\mathfrak{R}}\chi_\ell(\alpha\beta)\chi_m(\alpha-\alpha\beta)=\chi_{\ell+m}(\alpha)\sum_{\beta\in\mathfrak{R}}\chi_\ell(\beta)\chi_m(1-\beta).$$

$\alpha\in\mathfrak{R}$ ならば，

$$(\chi_\ell * \chi_m)(\alpha)=\sum_{\beta\in\mathfrak{R}}\chi_\ell(\beta)\chi_m(\alpha-\beta)=\chi_m(-1)\sum_{\beta\in\mathfrak{R}}\chi_\ell(\beta)\chi_m(\beta)$$

$$=\chi_m(-1)\sum_{\beta\in\mathfrak{R}}\chi_{\ell+m}(\beta)=0.$$

したがって

$$\chi_\ell * \chi_m = J(\chi_\ell, \chi_m)\, \chi_{\ell+m},$$

$$J(\chi_\ell, \chi_m) = \sum_{\alpha \in \mathfrak{R}} \chi_\ell(\alpha)\, \chi_m(1-\alpha).$$

ここに現われた量 $J(\chi_\ell, \chi_m)$ が，χ_ℓ と χ_m に関する<u>Jacobiの和</u>である．

このままではこれ以上変形ができないが，定理1を援用して

$$\lambda_1(\chi_\ell * \chi_m) = \lambda_1(\chi_\ell)\lambda_1(\chi_m) = G(\chi_\ell)G(\chi_m) = 2^{2s}\, i^{S_{\mathfrak{R}/\mathbb{Z}_4}(\ell^{2^s} + m^{2^s})}$$

$$= J(\chi_\ell, \chi_m)\, G(\chi_{\ell+m}) = 2^s\, i^{S_{\mathfrak{R}/\mathbb{Z}_4}(\ell+m)^{2^s}}\, J(\chi_\ell, \chi_m),$$

$$J(\chi_\ell, \chi_m) = 2^s\, i^{S_{\mathfrak{R}/\mathbb{Z}_4}(\ell^{2^s} + m^{2^s} - (\ell+m)^{2^s})}$$

i の肩にあるものは，(6) から

$$(\ell+m)^{2^s} = \ell^{2^s} + m^{2^s} + 2\ell^{2^{s-1}} m^{2^{s-1}}$$

だから

$$J(\chi_\ell, \chi_m) = 2^s (-1)^{S_{K/F}(\ell m)^{2^{s-1}}} = 2^s (-1)^{S_{K/F}\, \ell m} = 2^s \chi_{\ell m}(-1)$$

で，$\chi_\ell * \chi_m = 2^s \chi_{\ell m}(-1)\, \chi_{\ell+m}$ が得られ，定理2の凡ての式が証明された．

§4. $\mathfrak{R}^*/\{\xi\}$ の coset の合併から生ずる Hadamard 差集合

12. われわれが最初に気づいたのは次の

<u>定理 3</u>　$\mathfrak{R}^*$の指数 2 の部分群は $\mathfrak{R}$ 上の Hadamard 差集合である.

であるが，ここではもっと一般的な定理 4，5 を述べ，その特別な場合として考える.

$\mathfrak{R}^*/\{\xi\}$ の coset $E_a=\{(1+2a)\xi^m\}$ を 2^{s-1} 個合併した集合 $\mathfrak{D}=\bigcup_{a\in A}E_a$，$\#A=2^{s-1}$ が $\mathfrak{R}$ 上の Hadamard 差集合であることは，

$$E_a=\sum_{m=0}^{2^s-2}(1+2a)\xi^m\ ,\quad \mathfrak{D}=\sum_{a\in A}E_a$$

について (1) から

$$(11)\qquad \mathfrak{D}*\hat{\mathfrak{D}}=2^{2s-2}\mathbf{0}+2^{s-1}(2^{s-1}-1)\mathbf{1}$$

であるが，

$$E_a=2^{-s}\sum_{\ell\in K}\chi_\ell(a)\chi_\ell=2^{-s}\sum_{\ell\in K}(-1)^{S_{K/F}\ell a}\chi_\ell$$

だから

$$\mathfrak{D}=\sum_{\ell\in K}\omega_\ell\chi_\ell\ ,\quad \omega_\ell=\sum_{a\in A}(-1)^{S_{K/F}\ell a}$$

により，次のように変形される.

$$\mathfrak{D}*\hat{\mathfrak{D}}=2^{-2s}(\omega_0\chi_0+\sum{}'\omega_\ell\chi_\ell)*(\omega_0\chi_0+\sum{}'\omega_\ell\hat{\chi}_\ell)\qquad\left(\sum{}'=\sum_{\ell\neq 0}\ \text{の意}\right)$$

$$=2^{-2s}\Big(\omega_0^2\chi_0*\chi_0+\sum{}'\omega_\ell^2\chi_\ell*\hat{\chi}_\ell+\sum_{\ell}{}'\sum_{m}{}'\omega_\ell\omega_m\chi_\ell*\hat{\chi}_m\Big)$$

ここで最初の 2 項は定理 2 によって

$$2^{-2s}\Big(\omega_0^2\big(2^s(2^s-1)\mathbf{0}+2^s(2^s-1)(\mathbf{1}-\mathbf{0})-2^s\chi_0\big)$$
$$+\Big(\sum{}'\omega_\ell^2\Big)\big(2^s(2^s-1)\mathbf{0}-2^s(\mathbf{1}-\mathbf{0})+2^s\chi_0\big)\Big)$$

$$=2^{-2s}\Big(\big(\omega_0^2+\sum{}'\omega_\ell^2\big)2^s(2^s-1)\mathbf{0}+\big(2^s(2^s-1)\omega_0^2-2^s\sum{}'\omega_\ell^2\big)(\mathbf{1}-\mathbf{0})+\big(\omega_0^2-\sum{}'\omega_\ell^2\big)2^s\chi_0\Big)$$

ここで $D*\hat{D}$ における $\mathbf{0}$ の係数は $\#D=2^{s-1}(2^s-1)$ だから

$$\omega_0^2+\sum{}'\omega_\ell^2=2^{2s-1},\quad \omega_0=2^{s-1}\quad より\quad \sum{}'\omega_\ell^2=2^{2s-2}.$$

したがって結局上式は

$$2^{s-1}(2^s-1)\mathbf{0}+2^{s-2}(2^s-2)(\mathbf{1}-\mathbf{0})=2^{2s-2}\mathbf{0}+2^{s-1}(2^{s-1}-1)\mathbf{1}$$

となる。これが(11)の右辺に等しいので，(11)を成立させるには残余項に当る部分が

$$2^{-2s}\sum_{\ell}{}'\sum_{m}{}'\omega_\ell\omega_m\hat{\chi}_\ell*\chi_m=0$$
$$\ell\neq m$$

であることが必要十分である。定理2より，上式

$$=2^{-2s}\sum{}'\sum{}'\omega_\ell\omega_m\chi_\ell*\hat{\chi}_m=2^{-s}\sum{}'\sum{}'\omega_\ell\omega_m(-1)^{S_{K/F}\ell m}\chi_m(-1)\chi_{\ell+m}$$

$$=2^{-s}\sum_{k}{}'\Big(\sum_{\substack{\ell\neq0\\ \ell\neq k}}(-1)^{S_{K/F}k\ell}\omega_\ell\omega_{k+\ell}\Big)\chi_k$$

で，χ_k $(k\in K)$ は一次独立であるから(11)の成立條件は

$$\sum_{\ell\neq0,\ell\neq k}(-1)^{S_{K/F}k\ell}\omega_\ell\omega_{k+\ell}=0.$$

<u>定理4</u>. D が Hadamard 差集合であるための必要十分條件は

$$\omega_\ell=\sum_{a\in A}(-1)^{S_{K/F}\ell a}$$

に対して

$$\sum_{\ell\neq0,\ell\neq k}(-1)^{S_{K/F}k\ell}\omega_\ell\omega_{k+\ell}=0\qquad(k\neq0)$$

が成立つことである。

注意. $S_{K/F}k=1$ ならば，結論の式は自動的に成立する。ゆえに上の條件は，

$S_{K/F}k=0$, $k\neq 0$ のとき $(l, l+k)$, $l\neq 0$, $l\neq k$ なる対に対する和

$$\sum_{\text{pair}}(-1)^{S_{K/F}kl}\omega_l\omega_{l+k}=0$$

と書くこともできる.

系として定理3が証明される. 事実 $\mathfrak{K}^*$ の指数2の部分群は, Kの指数2の部分群Aから $\{(1+2a)\xi^m;\ a\in A, 0\leqq m\leqq 2^s-2\}$ となっている. $a\in A$ に $(-1)^{S_{K/F}la}$ を対応させたものは, Aの一つの指標で, 和 $\omega_l=\sum_{a\in A}(-1)^{S_{K/F}la}$ は, 上の指標がAの単位指標でなければ $\omega_l=0$, また単位指標ならば $=2^{s-1}$ となる. 単位指標を与える l は, 凡ての $a\in A$ に対して $S_{K/F}la=0$ ならしめる l, すなわち, Aの'直交補空間'の元 l で, そのような l は唯1個しかない. したがって定理4に述べる条件が成立して, Dは Hadamard 差集合になる.

13. 次に convolution 積に関する公式, 定理1, 定理2に依らないでDが Hadamard 差集合になるための条件を求めておく. その代りに使う原理は, $\mathfrak{K}$ の凡ての加法的指標 λ_β について

$$\left.\begin{aligned}\lambda_\beta(D*\hat{D})&=2^{2s-2} && (\beta\neq 0)\\ &=2^{2s-2}(2^s-1)^2 && (\beta=0)\end{aligned}\right\}$$

が成立つことである. 左辺は

$$\lambda_\beta(\mathfrak{D})\overline{\lambda_\beta(\mathfrak{D})}$$

で $\beta=0$ の時は自明だから $\beta\neq 0$ とするとき $\lambda_\beta(\mathfrak{D})\overline{\lambda_\beta(\mathfrak{D})}=2^{2s-2}$ をしらべる.

さて $\lambda_\beta(\mathfrak{D})=\sum_{a\in A}\sum_{m=0}^{2^s-2} i^{S_{R/Z_4}\beta(1+2a)\xi^m}$ は Gauss の数体 $\mathbf{Q}(i)$ の整数で，イデアルとしては

$$(\lambda_\beta(\mathfrak{D}))(\overline{\lambda_\beta(\mathfrak{D})})=2^{2s-2}$$

であるが，$\mathbf{Q}(i)$ で素数 2 は分岐して $2=(1+i)^2$，$(1+i)$ は $\mathbf{Z}[i]$ における 2 の素因数である．したがってイデアルとしては

$$(\lambda_\beta(\mathfrak{D}))=(1+i)^{2s-2}=(2^{s-1})$$

したがって $\lambda_\beta(\mathfrak{D})=2^{s-1}v_\beta$ とおくと v_β は $\mathbf{Z}[i]$ の単数より，$\pm i$ になる．

14. さらに変形してゆくために $a\in K$ に対して

$$z_a=\lambda_1(E_a)=\sum_{m=0}^{2^s-2} i^{S_{R/Z_4}(1+2a)\xi^m}$$

とおく．

まず $\beta\in E_b$ ならば $\lambda_\beta(E_a)=z_{a+b}$，$\lambda_{2\beta}(E_a)=-1$ であることを証明しておく．

事実 $\beta=(1+2b)\xi^u$ ならば

$$\lambda_\beta(E_a)=\sum_{m=0}^{2^s-2} i^{S_{R/Z_4}\beta(1+2a)\xi^m}=\sum_{m=0}^{2^s-2} i^{S_{R/Z_4}(1+2a)(1+2b)\xi^{m+u}}$$
$$=\sum_{m=0}^{2^s-2} i^{S_{R/Z_4}(1+2a+2b)\xi^m}=\lambda_1(E_{a+b})=z_{a+b}.$$

同様に $\lambda_{2\beta}(E_a)=\lambda_2(E_{a+b})$ であるが，一般に $\lambda_2(E_a)=-1$ である：

$$\lambda_2(E_a)=\sum_{m=0}^{2^s-2}(-1)^{S_{K/F}(1+2a)\xi^m}=\sum_{m=0}^{2^s-1}(-1)^{S_{K/F}\xi^m}=-1$$

特に $\lambda_{2\beta}(\mathfrak{D})=-2^{s-1}$ で，**13.** に述べた条件 $\lambda_{2\beta}(\mathfrak{D})/2^{s-1}$ が単数

である' が満足される.

<u>定理5</u>. $\mathfrak{D}$ が $\mathfrak{R}$ 上の Hadamard差集合であるための必要十分條件は

$$z_a=\sum_{m=0}^{2^s-2} i^{S_{\mathfrak{R}/Z_4}(1+2a)\xi^m}$$

に対して, $b\in K$ につき

$$\sum_{a\in A+b} z_a = 2^{s-1}v_b\ ,\quad v_b\in\{\pm 1, \pm i\}$$

が成立つことである.

<u>系</u> として A が群の場合には, $A+b=A$ またはある c について $A+c$ で,

$$\sum_{a\in A} z_a=\sum_{m=0}^{2^s-2} i^{S_{\mathfrak{R}/Z_4}\xi^m}\sum_{a\in A}(-1)^{S_{K/F}a\xi^m}$$

だが、内側の和は **12** に示したように ξ^m が A の直交補空間の元の時だけ 2^{s-1} になり他では $=0$. したがって

$$\sum_{a\in A} z_a = 2^{s-1} i^{S_{\mathfrak{R}/Z_4}\xi^m},\quad m \text{ は } S_{K/F}(\xi^m a)=0\ (a\in A) \text{ なる値.}$$

また $\sum_{a\in A+c} z_a$ については, $A\cup(A+c)=K$ で $\sum_{a\in K} z_a=0$ より, $\sum_{a\in A+c} z_a = -\sum_{a\in A} z_a = -2^{s-1} i^{S_{\mathfrak{R}/Z_4}\xi^m}$ となって, 定理5の條件が満足されて, $\mathfrak{D}$ が Hadamard 差集合になる.

<u>例</u>. $s=3$. $f(x)=x^3+2x^2+x+3$. coset E_a の表.

E_{000}	E_{100}	E_{010}	E_{001}	E_{110}	E_{011}	E_{111}	E_{101}
100	300	120	102	320	122	322	302
010	030	012	230	032	232	212	210
001	003	021	023	223	203	201	021
132	312	110	310	330	332	112	130
233	211	011	031	033	213	231	013
331	113	133	131	311	333	111	313
121	323	321	101	123	301	103	303

$100=1,\ 010=\xi,\ 001=\xi^2$ で $xyz = x+y\xi+z\xi^2$ の意味である.

$z_{000}=-3+2i$, $z_{100}=-3-2i$, $z_{010}=1-2i$, $z_{001}=1-2i$, $z_{110}=1+2i$, $z_{011}=1-2i$, $z_{111}=1+2i$, $z_{101}=1+2i$.

$A=\{0,\xi^a,\xi^b,\xi^c\}$ を (a,b,c) で表わして, 定理5の條件をチェックすると, 次の19個の差集合が出来る.

0,1,3. 0,1,5. 0,1,6 0,2,3. 0,2,5. 0,2,6 0,3,4. 0,4,5. 0,4,6. 1,2,4

1,3,5. 1,3,6. 1,5,6. 2,3,5. 2,3,6. 2,5,6. 3,4,5. 3,4,6. 4,5,6

これらを平行移動とFrobenius自己同型で移すと次の4個になる.

No.1 1,2,4 ; No.2 0,1,3 ; No.3 1,5,6 ;

No.4 0,1,5.

以上の中 No.1, No.2, No.3 は群で, No.4 は非群である.

そのHall不変数は次のようになる.

	0	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	64
No.1, No.2, No.3	7	0	0	0	336	0	3584	0	31836	0	3584	0	336	0	0	0	28
No.4	0	0	0	0	0	112	2492	9352	15869	9184	2492	168	42	0	0	0	0

したがって群と非群は差集合として非同型である. (この2種類はHadamard行列として非同型である.)

群 No.1, No.2, No.3 から生ずる差集合の自己同型群を求めると, それぞれ位数 672, 224, 224 の群である. さらに第2のものは, 中心の位数が2, 第3のものは中心の位数が1. したがって, これらの差集合は凡て非同型であることが分る.

同様のことを $s=4$ について行なうと，195 個の差集合が得られる．平行移動と Frobenius 自己同型で，それらは 18 個に分れる．うち 5 個は群，13 個は非群である．これらは凡て非同型であろうと信ぜられるが，おのおのの自己同型群を計算するのには莫大な時間が必要である．

15. 最後にひと言．定理 5 に述べた方法が簡単で，しかも有効であるのに，定理 4 を先に挙げたのは，そちらの方がより基本的であるからである．事実，定理 4 の方法はいわゆる distance-regular digraph にもそのままあてはまる．

文献

[1] H. B. Mann, Addition Theorems, New York 1965

[2] K. Yamamoto, Pacific J. 13 (1963), 337–352.

[3] R. J. Turyn, Pacific J. 15 (1965), 319–346.

[4] R. A. Liebler and R. A. Mena, preprint.