Jacobi和の間の関係について

福井　邦彦

平成19年2月23日

目 次

1　イントロダクション

今回の論文では，1973 年に Muskat と Zee が書いた論文 [1] の解説をしていく．この論文では，主に Jacobi 和の間に成り立つ関係式を示している．この関係式が，Hasse の主張に対する反例となっている．まずこの章では，Jacobi 和の間の関係式とはどういうものか，Hasse の主張とは何かなどについて解説していく．

1.1　論文の概要

p を素数，ζ_p を 1 の原始 p 乗根，χ, λ を $\mathbb{F}_p$ 上の乗法的指標とする．また，この χ, λ に対して，Gauss 和 $g(\chi)$ と Jacobi 和 $J(\chi, \lambda)$ をそれぞれ

$$g(\chi) = \sum_{x=1}^{p-1} \chi(x) {\zeta_p}^x,$$

$$J(\chi, \lambda) = \sum_{a=2}^{p-1} \chi(a)\lambda(1-a)$$

で定義する．この Jacobi 和 $J(\chi, \lambda)$ と Gauss 和 $g(\chi)$ について，Davenport と Hasse が示した次のような関係式がある．

定理 1.1 (Davenport-Hasse の公式) p を奇素数，e を $p \equiv 1\ (e)$ をみたす整数，l を e の約数とする．また，χ を $\chi^e = I$ となるような乗法的指標としたとき

$$\prod_{\lambda^l = I, \lambda \neq I} J(\chi, \lambda) = \chi(l^l) \frac{g(\chi)^l}{g(\chi^l)} \tag{1.2}$$

が成り立つ．

ここで，I は自明な指標のことである．今回，この式については [2, p.477(2)] を参考にした．この関係式とノルムの関係式 $|g(\chi_m)|^2 = p$ を用いると，Gauss 和の間の関係式が導ける．そこで，Hasse は [3, p.465] で次のような主張をした．

Hasse の主張
$\mathbb{F}_p$ 上の Gauss 和に対して，Gauss 和に関して斉次であるような Gauss 和の積の間の関係式を考えると，任意の関係式はノルムの関係式 $|g(\chi_m)|^2 = p$ と Davenport Hasse の公式によって導かれる．

ここで，Hasse の主張で述べている，Gauss 和の斉次な関係式の例を紹介する．まず，Gauss 和の間の関係式を導くための式を補題として書いておく．

補題 1.3 $e = xy$，t.整数のとき

$$\prod_{k=0}^{y-1} g(\chi_{kx+t}) = \chi_{-ty}(y)g(\chi_{ty})\prod_{k=1}^{y-1} g(\chi_{kx}) \tag{1.4}$$

が成り立つ.

この関係式は [4, (0.9_1)] で紹介している．この式は Davenport-Hasse の公式から示せる式である．この関係式とノルムの関係式を用いて作れる Gauss 和の関係式の例を今から挙げていく．実際に e を定めて，それに応じて x, y を代入して，Gauss 和の間の関係式を導く．まず一つ目の例として，Davenport-Hasse の公式とノルムの式を用いて導かれる関係式の例を挙げる.

例 1.5 $e = 12$ とする．(1.4) に $x = 3, y = 4, t = 1$ を代入すると

$$g(\chi_1)g(\chi_4)g(\chi_7)g(\chi_{10}) = \chi_{-4}(4)g(\chi_4)g(\chi_3)g(\chi_6)g(\chi_9)$$

となる．両辺を $g(\chi_4)$ で割ると

$$g(\chi_1)g(\chi_7)g(\chi_{10}) = \chi_{-4}(4)g(\chi_3)g(\chi_6)g(\chi_9).$$

ここで，$9 \equiv -3\ (12), 7 \equiv -5\ (12)$ であるから，$\overline{g(\chi_3)} = g(\chi_9), \overline{g(\chi_5)} = g(\chi_7)$ である．$g(\chi_n)\overline{g(\chi_n)} = |g(\chi_n)|^2 = p$ より，

$$|g(\chi_3)|^2 = |g(\chi_5)|^2 = p$$

であるので，これを利用して書き換えると

$$g(\chi_1)g(\chi_7)g(\chi_{10}) = \chi_{-4}(4)g(\chi_5)g(\chi_6)g(\chi_7)$$

となる．両辺を $g(\chi_7)$ で割ると

$$g(\chi_1)g(\chi_{10}) = \chi_{-4}(4)g(\chi_5)g(\chi_6).$$

さらに，Davenport-Hasse の公式とノルムの式からえられる Gauss 和の間の関係式から，Jacobi 和の関係式が導ける．その例を一つ挙げる.

例 1.6 $e = 21$ とする．(1.4) に $x = 3, y = 7, t = 1$ を代入すると

$$\begin{aligned} &g(\chi_1)g(\chi_4)g(\chi_7)g(\chi_{10})g(\chi_{13})g(\chi_{16})g(\chi_{19}) \\ &\qquad = \chi_{-7}(7)g(\chi_7)g(\chi_3)g(\chi_6)g(\chi_9)g(\chi_{12})g(\chi_{15})g(\chi_{18}) \end{aligned}$$

となる．両辺を $g(\chi_7)$ で割ると

$$g(\chi_1)g(\chi_4)g(\chi_{10})g(\chi_{13})g(\chi_{16})g(\chi_{19}) \\ = \chi_{-7}(7)g(\chi_3)g(\chi_6)g(\chi_9)g(\chi_{12})g(\chi_{15})g(\chi_{18}).$$

この式に

$$\begin{cases} g(\chi_3)g(\chi_{18}) = g(\chi_2)g(\chi_{19}) \\ g(\chi_6)g(\chi_{15}) = g(\chi_5)g(\chi_{16}) \\ g(\chi_9)g(\chi_{12}) = g(\chi_8)g(\chi_{13}) \end{cases}$$

を代入すると，

$$g(\chi_1)g(\chi_4)g(\chi_{10})g(\chi_{13})g(\chi_{16})g(\chi_{19}) \\ = \chi_{-7}(7)g(\chi_2)g(\chi_5)g(\chi_8)g(\chi_{13})g(\chi_{16})g(\chi_{19})$$

となる．両辺を $g(\chi_{13})g(\chi_{16})g(\chi_{19})$ で割ると

$$g(\chi_1)g(\chi_4)g(\chi_{10}) = \chi_{-7}(7)g(\chi_2)g(\chi_5)g(\chi_8)$$

となる．さらに両辺に $\frac{g(\chi_1)^2}{g(\chi_2)g(\chi_5)g(\chi_{10})}$ をかけると

$$\frac{g(\chi_1)g(\chi_4)}{g(\chi_5)} \cdot \frac{g(\chi_1)g(\chi_1)}{g(\chi_2)} = \chi_{-7}(7)\frac{g(\chi_1)g(\chi_8)}{g(\chi_9)} \cdot \frac{g(\chi_1)g(\chi_9)}{g(\chi_{10})}$$

となる．これを Jacobi 和で書き直せば

$$J(\chi_1, \chi_4)J(\chi_1, \chi_1) = \chi_{-7}(7)J(\chi_1, \chi_8)J(\chi_1, \chi_9)$$

と書ける．

このように，Davenport-Hasse の公式とノルムの式から導かれる Gauss 和の斉次式の符号は χ で表されるが，この χ は p によらない値で，Davenport-Hasse の公式とノルムの式から導かれる式の符号は p によらず一つに定まる．Hasse の主張が正しければ，Gauss 和について斉次であるような Gauss 和の間に成り立つ任意の関係式の符号は p によらないということになる．ところが，Hasse の主張は間違っていることが確認されている．最初の反例は [2, p.489] で Yamamoto によって与えられている．Yamamoto は，(1.4) とノルムの関係式から導いた関係式の符号が p によって異なることに注目して，(1.4) によらない関係式が存在することを確認した．今から，その反例について述べる．

Koichi Yamamoto の反例

$e = 12$ とする．このとき，Davenport-Hasse の公式とノルムの式より

$$(g(\chi_2)g(\chi_5))^2 = \zeta_{12}^2(g(\chi_3)g(\chi_4))^2$$

となる．$e = 12$ であるから

$$g(\chi_2)g(\chi_5) = \mu\zeta_{12}g(\chi_3)g(\chi_4)$$

となる．ただし，$\mu = \pm 1$ である．この式の符号は p によって変化するので，この関係式は Davenport-Hasse の公式とノルムの式によって導かれた式の符号が一通りに定まる，という Hasse の主張に反している．

この反例についての説明が [2] 内に見つからなかったので，この符号 μ が p によってどのような変化をするのか，という点については結局理解できなかった．この点は，今後勉強して理解したいと思う．また，Muskat は，Hasse の主張に対して，(1.4) などの式を用いて導ける Gauss 和の関係式から，Jacobi 和の関係式を考えることでいくつかの反例を示している．今回はそれについて解説していきたいと思う．$\mathbb{F}_p$ 上の乗法的指標 $\chi_m : {\mathbb{F}_p}^{\times} \longrightarrow \mathbb{Q}(\zeta_e)$ を，$\chi_m(\gamma) = \zeta_e$ と定義する．この χ と，その Jacobi 和に対して，次のような定理が成り立つ．

Muskat の反例

定理 1.7 (J. B. Muskat 1) $p = U^2 + 7V^2 \equiv 1\ (21)$ のとき

$$\chi_{-7}(7)J(\chi_1, \chi_4) = \mu J(\chi_3, \chi_6) \tag{1.8}$$

が成り立つ．ただし，

$$\begin{cases} \mu = +1 \Leftrightarrow 3|V \\ \mu = -1 \Leftrightarrow 3|U \end{cases}$$

である．

この定理の等式は，符号 μ が p によって二通りに値をとるという点で，Hasse の主張の反例になっている．Davenport-Hasse の公式から導かれた Jacobi 和の間の関係式は，e が奇数の場合必ず一通りに決定するからである．この点については，後ほどまた説明する．$e = 21$ 以外の場合についても，Muskat はいくつか反例を挙げている．以下で紹介しておく．$e = 28$ のときは以下のような関係式が導ける．

定理 1.9 (J. B. Muskat 2) $p = X^2 + 4Y^2 \equiv 1\ (28)$ のとき

$$J(\chi_1, \chi_6) = I\sigma_3 J(\chi_1, \chi_2) \tag{1.10}$$

が成り立つ．ただし，

$$\begin{cases} I = +1 \Leftrightarrow 7 \mid Y \\ I = -1 \Leftrightarrow 7 \mid X \\ I^2 = -1 \Leftrightarrow 7 \nmid XY \end{cases}$$

である．

$e = 28$ のときも，符号 I が p によって異なる値をとる．この点で，この定理も Hasse の主張の反例であるということができる．また，$e = 39$ のときは次の式が導ける．

定理 1.11 (J. B. Muskat 3) $p \equiv 1\ (39)$ のとき

$$\sigma_2[\chi_{13}(13)J(\chi_1, \chi_{16})] = \rho\chi_{13}(13)J(\chi_1, \chi_{16}) \tag{1.12}$$

が成り立つ．ただし，

$$\begin{cases} \rho = +1 \Leftrightarrow p = A^2 + 39B^2 \\ \rho = -1 \Leftrightarrow p = 3C^2 + 13D^2 \end{cases}$$

である．

$e = 39$ のときに関しても，基本的に $e = 21, e = 28$ のときと同じ考え方で式を導ける．基本的な考え方は同じなので，本論文では，$e = 21$ のときの証明について詳しくやっていこうと思う．

2 Davenport Hasseの公式とHasseの主張

2.1 Gauss和，Jacobi和の定義

pを素数，ζ_pを1の原始p乗根，χ, λを有限体$\mathbb{F}_p$上の乗法的指標とするとき，p, χ, λに対して，Gauss和とJacobi和を次のように定義する．

定義 2.1

$$g(\chi) = \sum_{x=1}^{p-1} \chi(x)\zeta_p{}^x,$$

$$J(\chi, \lambda) = \sum_{a=2}^{p-1} \chi(a)\lambda(1-a).$$

次に，今回考える乗法的指標の定義をする．$p = ef + 1$を奇素数，γを$\mathbb{F}_p{}^\times$の生成元，$\beta = \zeta_e, \sigma_s : \beta \to \beta^s$：ガロア群$(\mathbb{Q}(\beta)/\mathbb{Q})$の元とする．ただし，$e, f \in \mathbb{Z}$である．このとき，$\chi_m : \mathbb{F}_p{}^\times \longrightarrow \mathbb{Q}(\beta)$を，$\chi_m(\gamma) = \beta^m$と定義する．$\mathbb{F}_p{}^\times$の任意の元$a$は$\gamma^d$ $(1 \leq d \leq p-1)$の形で書けて $\chi_m(a) = \beta^{md}$．$\chi_m(\gamma)^{p-1} = \beta^{m(p-1)} = \beta^{mef}$で，$ef$は偶数であるから，$\beta^{mef} = 1$である．よって，任意の$a$に対して$\chi_m(a)$は1の$p-1$乗根である．よって，乗法的指標としてwell-definedである．このχ_mに対して$\chi_m(-1)$を考えると，$(-1)^2 = 1$なので

$$\chi_m(-1) = \chi_m(\gamma^{\frac{p-1}{2}}) = \beta^{\frac{p-1}{2}} = \beta^{\frac{ef}{2}} \tag{2.2}$$

である．pが奇数であることよりefは偶数なので，eが奇数の時とe, fがともに偶数の時は$\chi_m(-1) = 1$，eが偶数，fが奇数の時は$\chi_m(-1) = -1$である．また，χ_{-m}について考えると，定義より

$$\chi_{-m}(a) = \beta^{-md} = \frac{1}{\beta^{md}} = \frac{1}{\chi_m(a)} \tag{2.3}$$

が成り立つ．つまり，$\overline{\chi_{-m}(a)} = \chi_m(a)$であるといえる．また$m \equiv n\ (e)$のとき，$\beta = \zeta_e$なので$\chi_m(a) = \beta^{md} = \beta^{nd} = \chi_n(a)$である．Jacobi和とGauss和の間には，[5, Theorem 1(d)]より次の関係が成り立つ．

命題 2.4 指標χ_mについて，Gauss和とJacobi和の間に

$$J(\chi_m, \chi_n) = \frac{g(\chi_m)g(\chi_n)}{g(\chi_{m+n})} \tag{2.5}$$

という関係が成り立つ．

この式を用いると，Davenport-Hasseの公式をGauss和の積の間の関係式に直すことができる．これを利用して，Hasseの主張について考えていく．

2.2 Davenport-Hasse の公式と Hasse の主張について

まず，改めて Davenport-Hasse の公式について書いておく．

定理 2.6 (Davenport-Hasse の公式) p を奇素数，e を $p \equiv 1\ (e)$ をみたす整数，l を e の約数とする．また，χ を $\chi^e = I$ となるような乗法的指標としたとき

$$\prod_{\lambda^l = I, \lambda \neq I} J(\chi, \lambda) = \chi(l^l) \frac{g(\chi)^l}{g(\chi^l)} \tag{2.7}$$

が成り立つ．

今からこの等式が成り立つことを示す．方針としては，まず $l = 2$ の場合について，この等式が成り立つことを示す．その際，$g(\chi)^2$ を式変形して考えていく．その後は

$$g(x)^k = \chi(-1) p J(\chi, \chi) J(\chi, \chi^2) \cdots J(\chi, \chi^{k-2}) \tag{2.8}$$

を用いて一般の l で成り立つことを示していく．

証明　右辺を変形すると

$$\begin{aligned} \chi(l^l) \frac{g(\chi)^l}{g(\chi^l)} &= \frac{g(\chi)^l}{\chi^{-1}(l^l) g(\chi^l)} \\ &= \frac{g(\chi)^l}{\chi^l(l^{-1}) g(\chi^l)} \\ &= \frac{g(\chi)^l}{g_l(\chi^l)} \end{aligned}$$

となるので，

$$\prod_{\lambda^l = I, \lambda \neq I} J(\chi, \lambda) = \frac{g(\chi)^l}{g_l(\chi^l)} \tag{2.9}$$

であることを示す．まず，$l = 2$ の場合について考える．(2.9) に $l = 2$ を代入すると

$$J(\chi, \lambda) = \frac{g(\chi)^2}{g_2(\chi^2)} \quad (\chi^2 \neq I, \lambda \neq I, \lambda^2 = I) \tag{2.10}$$

だから，この式が成り立つことを示す．$g(\chi)^2$ を式変形していく．

$$\begin{aligned} g(\chi)^2 &= \sum_x \chi(x) \zeta^x \cdot \sum_y \chi(y) \zeta^y \\ &= \sum_{x,y} \chi(x) \chi(y) \zeta^{x+y} \\ &= \sum_{x,y} \chi(xy) \zeta^{x+y}. \end{aligned}$$

$x+y=t$ とおくと

$$
\begin{aligned}
g(\chi)^2 &= \sum_t \sum_{x+y=t} \chi(xy)\zeta^t \\
&= \sum_t \zeta^t \sum_{x+y=t} \chi(xy).
\end{aligned} \tag{2.11}
$$

$\sum_{x+y=t} \chi(xy)$ に関して，$t=0$ の場合と $t\neq 0$ の場合にわけて考える．まず，$t=0$ とすると

$$
\begin{aligned}
\sum_{x+y=0} \chi(xy) &= \sum_x \chi(x\cdot(-x)) \\
&= \sum_x \chi(-x^2) \\
&= \sum_x \chi(-1)\chi(x^2) \\
&= \chi(-1)\sum_x \chi^2(x).
\end{aligned}
$$

ここで，$\chi^2 \neq I$ である．自明でない指標について，その値の和をとると 0 になるので

$$
\sum_{x+y=0} \chi(xy) = 0 \tag{2.12}
$$

となる．次に $t\neq 0$ の場合について考える．$x=\frac{x't}{2}, y=\frac{y't}{2}$ とおくと

$$
x+y = \frac{x't}{2} + \frac{y't}{2} = t.
$$

$t\neq 0$ なので，両辺に $\frac{2}{t}$ をかけると

$$
x'+y'=2
$$

となる．これが x,y を $\frac{x't}{2}, \frac{y't}{2}$ で置き換えたときの和をとる範囲となるので

$$
\begin{aligned}
\sum_{x+y=t} \chi(xy) &= \sum_{x'+y'=2} \chi(\frac{x't}{2}\cdot\frac{y't}{2}) \\
&= \sum_{x'+y'=2} \chi((\frac{t}{2})^2)\chi(x'y') \\
&= \chi^2(\frac{t}{2}) \sum_{x'+y'=2} \chi(x'y')
\end{aligned} \tag{2.13}
$$

となる．(2.13) を (2.11) に代入して，さらに $\frac{t}{2} = t'$ とおくと

$$\begin{aligned} g(\chi)^2 &= \sum_t \zeta^t \cdot \chi^2(\frac{t}{2}) \sum_{x'+y'=2} \chi(x'y') \\ &= (\sum_t \chi^2(t')\zeta^{2t'})(\sum_{x'+y'=2} \chi(x'y')) \\ &= g_2(\chi^2) \sum_{x'+y'=2} \chi(x'y') \end{aligned}$$

となるから，移項すれば

$$\sum_{x'+y'=2} \chi(x'y') = \frac{g(\chi)^2}{g_2(\chi^2)} \tag{2.14}$$

となる．あとは，左辺が Jacobi 和 $J(\chi, \lambda)$ と等しくなることを示せばよい．ここで，$x'y' = z$ とおくと，x', y' の値のとり方は

$$t^2 - 2t + z = (t - x)(t - y)$$

の任意の根 t の個数と等しい．z の値のとり方は $1 + \lambda(1 - z)$ 通りなので，

$$\begin{aligned} \sum_{x'+y'=2} \chi(x'y') &= \sum_z (1 + \lambda(1 - z))\chi(z) \\ &= \sum_z \chi(z) + \chi(z)\lambda(1 - z) \end{aligned} \tag{2.15}$$

となるが，$\chi \neq 0$ なので，$\sum_z \chi(z) = 0$ である．よって，

$$\begin{aligned} \sum_{x'+y'=2} \chi(x'y') &= \sum_z \chi(z) + \chi(z)\lambda(1 - z) \\ &= \sum_z \chi(z)\lambda(1 - z) = J(\chi, \lambda). \end{aligned} \tag{2.16}$$

(2.14) と (2.16) より

$$J(\chi, \lambda) = \frac{g(\chi)^2}{g_2(\chi^2)}. \tag{2.17}$$

$l = 2$ のときに関しては以上より示せた．次に一般の場合について考える．(2.8) を式変形すると

$$\frac{g(\chi)g(\chi^{k-1})}{g(\chi^k)} \cdot \frac{g(\chi)^k}{\chi(-1)p} = \prod_{\lambda^k=I} J(\chi, \lambda)$$

となる．$\chi(-1)p = g(\chi)\overline{g(\chi)} = g(\chi)g(\overline{\chi}) = g(\chi)g(\chi^{k-1})$ であるから，

$$\frac{g(\chi)^k}{g(\chi^k)} = \prod_{\lambda^k=I} J(\chi,\lambda).$$

Hasse の主張

$\mathbb{F}_p$ 上の Gauss 和に対して，Gauss 和の積の間の関係式を考えると，任意の関係式はノルムの関係式 $|g(\chi_m)|^2 = p$ と Davenport Hasse の公式によって導かれる．

Davenport-Hasse の公式は Jacobi 和と Gauss 和の関係式であるが，(2.5) を使うことで Gauss 和の積の間の関係式に直すことができる．Hasse の主張でいう Gauss 和の積の間の関係式は，Davenport-Hasse の公式を直したもので導ける．今回は Jacobi 和の間の関係式について考えているので，Davenport Hasse の公式によってどのように Jacobi 和の間の関係式が与えられるか，ということを考える．Davenpot-Hasse の公式を右辺に Jacobi 和が出てくるように変形する．

$$\prod_{\lambda^l=I,\lambda\neq I} J(\chi,\lambda) = \chi(l^l)\frac{g(\chi)^l}{g(\chi^l)}$$

の右辺を Gauss 和の分数の形に直すと

$$\prod_{k=1}^{l-1} J(\chi,\chi^{\frac{e}{l}}) = \chi(l^l)\frac{g(\chi)g(\chi^{l-1})}{g(\chi^l)}\frac{g(\chi)g(\chi^{l-2})}{g(\chi^{l-1})}\cdots\frac{g(\chi)g(\chi)}{g(\chi^2)}$$

となる．ここで，(2.5) を使って Jacobi 和に直すと

$$\prod_{k=1}^{l-1} J(\chi,\chi^{\frac{e}{l}}) = \chi(l^l)\prod_{k=1}^{l-1} J(\chi,\chi^{l-1}) \tag{2.18}$$

となる．このとき，χ は p に依存しない値なので，Davenport-Hasse から導ける Jacobi 和の間の関係式は p に依存しない．一方，$|g(\chi_m)|^2 = p$ について考えると，$|g(\chi)|^2 = \chi_m(-1)p$ である．先ほど書いたように，$p = ef+1$ のとき $\chi_m(-1)$ の値は e, f によって決まり，$e \equiv 0\ (2)$ かつ $f \equiv 1\ (2)$ のとき -1，それ以外のとき $+1$ となる．つまり，e が奇数のときは常に $+1$ になり，ノルムの式を使って変形しても符号の変化が起こらないことがわかる．以上から，Hasse の主張は，e が奇数のときは Davenport-Hasse から導ける Jacobi 和の間の関係式の符号は p に依存しない，ということを述べている．だから，もし Hasse の主張が正しければ，任意の Jacobi 和が p によって変化する符号をもたないということになる．なので，定理 1.7 のように p によって符号の変化

するような関係式が導けた場合，これは Hasse の主張の反例であるといえる．

実際，定理 1.7 の p の条件について具体的に考えてみる．$p = 43 \equiv 1\ (21)$ のとき，$43 = 6^2 + 7 \cdot 1^2$ とかけるので $U = 6, V = 1$ である．このときの Jacobi 和の関係式の符号は，$3|U$ であるから $\mu = -1$．また，$p = 127 \equiv 1\ (21)$ のとき，$127 = 8^2 + 7 \cdot 3^2$ とかけるので $U = 8, V = 3$ である．このときの Jacobi 和の関係式の符号は，$3|V$ であるから $\mu = +1$．一方，二次指標 χ について，$p \equiv 1\ (4)$ ならば $g(\chi) = \sqrt{p}$ であり，$p \equiv 3\ (4)$ ならば $g(\chi) = i\sqrt{p}$ である．つまり，Gauss 和の関係式は符号が異なる可能性がある．しかし，43 と 127 は共に 4 を法として 3 と合同なので，ノルムの式から得られる Gauss 和の間の関係式は，$p = 43$ の場合と $p = 127$ の場合で符号が異なるということはない．以上より，ノルムの式と Davenport-Hasse の式から得られる Jacobi 和の関係式は，p によって不変である．これは，定理 1.7 から得られる結果と違うので，定理 1.7 は Hasse の主張の反例となっている．

3　主定理の証明

3.1　主定理の証明に使う関係式

これから定理 1.7 の証明をしていく．方針としては，まず Davenport-Hasse の式から 2 つの Jacobi 和の積の間の関係式を導く．次に Jacobi 和一つ一つを，Davenport-Hasse の関係式や Jacobi 和に成り立つ関係式を使って，違う Jacobi 和との対応をさせていくことで，結果的には，$J(\chi_1, \chi_4)$ と $J(\chi_3, \chi_6)$ を含む次の 2 つの関係式を導く．具体的には

$$J(\chi_1, \chi_1)J(\chi_3, \chi_6) = \chi_6(3)J(\chi_1, \chi_3)J(\chi_1, \chi_4) \tag{3.1}$$

と

$$J(\chi_1, \chi_4)J(\chi_1, \chi_1) = \chi_6(3)\chi_{-7}(7)J(\chi_3, \chi_6)J(\chi_1, \chi_3) \tag{3.2}$$

の 2 つの式を導く．(3.2) の式を (3.1) の式で割ることで

$$J(\chi_1, \chi_4) = \mu\chi_7(7)J(\chi_3, \chi_6) \tag{3.3}$$

という Jacobi 和の間の関係式が得られる．ただし

$$\mu = \pm 1$$

である．この μ を以下では符号と呼ぶことにする．証明の中盤以降では，符号 μ の p による動向について考えていく．そのために，$\beta^{-7S}J(\chi_1, \chi_4)$ と $\sigma_2\{\beta^{-7S}J(\chi_1, \chi_4)\}$ を β^i の 1 次結合の形で表して，係数を比較することで $\beta^{-7S}J(\chi_1, \chi_4)$ を Dickson-Hurwitz 和 b を使って表す．同様に，$J(\chi_3, \chi_6)$ と $\sigma_2 J(\chi_3, \chi_6)$ を β^i の 1 次結合の形で表して，係数を比較することで $J(\chi_3, \chi_6)$ を b で表す．2 つの結果を

$$\mu\beta^{-7S}J(\chi_1, \chi_4) = J(\chi_3, \chi_6) \tag{3.4}$$

に代入すれば，μ と b の関係がわかる．また，$\beta^{-7S}J(\chi_1, \chi_4)$ のノルムを考えることで，p を b の関係がわかる．2 つの関係を照らし合わせて，符号 μ が p によって変化していることがわかれば，その関係式は Hasse の主張の否定になっている．まずは，証明に必要な等式について確認していく．$\beta = \zeta_e, \sigma_s : \beta \to \beta^s$：ガロア群 $(\mathbb{Q}(\beta)/\mathbb{Q})$ の元とする．この σ に対して Jacobi 和を対応させると

$$\sigma_s J(\chi_m, \chi_n) = J(\chi_{sm}, \chi_{sn}) \tag{3.5}$$

となる．また，一般的な Gauss 和，Jacobi 和に対して

$$J(\chi_m, \chi_n) = \frac{g(\chi_m)g(\chi_n)}{g(\chi_{m+n})} \tag{3.6}$$

が成り立つ．証明では，Davenport-Hasse から導かれた Gauss 和の積の間の式を，この式を使って Jacobi 和に変換していく．

補題 3.7 整数 m, n, r に対して

$$J(\chi_m, \chi_n)J(\chi_{m+n}, \chi_r) = J(\chi_m, \chi_r)J(\chi_{m+r}, \chi_n) \tag{3.8}$$

が成り立つ．

証明 (3.6) を用いると

$$(\text{左辺}) = \frac{g(\chi_m)g(\chi_n)}{g(\chi_{m+n})}\frac{g(\chi_{m+n})g(\chi_r)}{g(\chi_{m+n+r})} = \frac{g(\chi_m)g(\chi_n)g(\chi_r)}{g(\chi_{m+n+r})}.$$

$$(\text{右辺}) = \frac{g(\chi_m)g(\chi_r)}{g(\chi_{m+r})}\frac{g(\chi_{m+r})g(\chi_n)}{g(\chi_{m+n+r})} = \frac{g(\chi_m)g(\chi_n)g(\chi_r)}{g(\chi_{m+n+r})} = (\text{左辺}).$$

補題 3.9

$$J(\chi_m, \chi_n) = J(\chi_n, \chi_m) = J(\chi_{-m-n}, \chi_n) \tag{3.10}$$

が成り立つ．

証明 $J(\chi_m, \chi_n) = J(\chi_n, \chi_m)$ は明らか．(3.6) を用いると

$$J(\chi_{-m-n}, \chi_n) = \frac{g(\chi_{-m-n})g(\chi_n)}{g(\chi_{-m})}.$$

e が奇数なので $|g(\chi_m)|^2 = g(\chi_m)g(\chi_{-m}) = p$ であることに注意すると，$g(\chi_{-m}) = \frac{p}{g(\chi_m)}, g(\chi_{-m-n}) = \frac{p}{g(\chi_{m+n})}$ なので

$$\frac{g(\chi_{-m-n})g(\chi_n)}{g(\chi_{-m})} = \frac{g(\chi_m)g(\chi_n)}{g(\chi_{m+n})} = J(\chi_m, \chi_n).$$

Jacobi 和の間の関係式の変換には，主に σ とこの 2 つの式を用いる．また，[4, 0.9_1] より次の Gauss に関して斉次であるような関係式が成り立つ．

補題 3.11 $e = xy$，t:整数のとき

$$\prod_{k=0}^{y-1} g(\chi_{kx+t}) = \chi_{-ty}(y) g(\chi_{ty}) \prod_{k=1}^{y-1} g(\chi_{kx}) \tag{3.12}$$

が成り立つ.

e に応じてこの式に値を代入して，まず Gauss 和の関係式を導くことになる．$e = xy$ のとき $J_e(\chi_{ym}, \chi_{yn}) = J_x(\chi_m, \chi_n)$ が成り立つ．これは，χ^y を指標として考えると，$e = xy$ であるから $(\chi^y)^x = 1$ となることから導ける．証明中で β の係数について考える際，Dickson-Hurwitz 和に使うことになる．Dickson-Hurwitz 和の定義のためには，まずは円分数の定義の必要があるので，この 2 つについて定義しようと思う．今回，円分数と Dickson-Hurwitz 和の定義に関しては [6, p.263] を参考にした.

定義 3.13 (円分数) $p = ef + 1$：奇素数 $(e, f \in \mathbb{Z})$，γ：p の生成元とする．このとき

$$(h, k) = (h, k)_e$$

を

$$\gamma^{es+h} + 1 \equiv \gamma^{et+k} \ (p), 0 \leq h, k \leq e-1, 0 \leq s, t \leq f-1$$

の解の個数で定義する．この (h, k) を円分数という.

この (h, k) に対して，Dickson-Hurwitz 和を定義する.

定義 3.14 (Dickson-Hurwitz 和) (h, k) に対して

$$b_e(j, v) = b(j, v) = \sum_{h=0}^{e-1} (h, j - vh)$$

と定義する．この b を Dickson-Hurwitz 和という.

この b に対して，[7, (2.11)] より

$$J(\chi_n, \chi_{vn}) = (-1)^{vnf} \sum_{j=0}^{e-1} b(j, v) \beta^{nj} \tag{3.15}$$

が成り立つ.

3.2 主定理の証明

証明に必要な等式が揃ったので，今から本定理の証明をしていく．まず，定理について改めて確認をしておく．

定理 3.16 (J. B. Muskat 1) $p = U^2 + 7V^2 \equiv 1\ (21)$ のとき

$$\chi_{-7}(7)J(\chi_1, \chi_4) = \mu J(\chi_3, \chi_6) \tag{3.17}$$

が成り立つ．ただし，

$$\begin{cases} \mu = +1 \Leftrightarrow 3|V \\ \mu = -1 \Leftrightarrow 3|U \end{cases}$$

である．

証明 まず，(3.1) の式を導く．(3.8) の式に $m = 1, n = 1, r = 3$ を代入すると

$$J(\chi_1, \chi_1)J(\chi_2, \chi_3) = J(\chi_1, \chi_3)J(\chi_1, \chi_4) \tag{3.18}$$

となる．右辺に $J(\chi_1, \chi_4)$ が含まれてるので，左辺に $J(\chi_3, \chi_6)$ が出てくるような変形を考えていく。$-2 - 3 = -5 \equiv 16\ (21)$ なので

$$J(\chi_2, \chi_3) = J(\chi_2, \chi_{-5}) = J(\chi_2, \chi_{16}) = \sigma_2 J(\chi_1, \chi_8) \tag{3.19}$$

と書き直せる．次に，(3.12) の式を利用して考える．$e = 3 \times 7$ なので，まず $x = 7, y = 3, t = 1$ を代入すると

$$g(\chi_1)g(\chi_8)g(\chi_{15}) = \chi_{-3}(3)g(\chi_3)g(\chi_7)g(\chi_{14}) \tag{3.20}$$

となる．χ_3 と χ_6 の積を含む関係式がほしいので，$g(\chi_m)g(\chi_{-m}) = p$ より $g(\chi_7)g(\chi_{-7}) = g(\chi_6)g(\chi_{-6})$ であることを利用して変形すると

$$g(\chi_1)g(\chi_8)g(\chi_{15}) = \chi_{-3}(3)g(\chi_3)g(\chi_6)g(\chi_{15}). \tag{3.21}$$

(3.21) の両辺を $g(\chi_9)g(\chi_{15})$ で割れば，$\frac{g(\chi_1)g(\chi_8)}{g(\chi_9)} = \chi_{-3}(3)\frac{g(\chi_3)g(\chi_6)}{g(\chi_9)}$ なので

$$J(\chi_1, \chi_8) = \chi_{-3}(3)J(\chi_3, \chi_6). \tag{3.22}$$

(3.19) と (3.22) をまとめると

$$J(\chi_2, \chi_3) = \sigma_2 \chi_{-3}(3)J(\chi_3, \chi_6). \tag{3.23}$$

$\sigma_2\chi_{-3}(3)=\chi_{-6}(3)$，$\sigma_2 J(\chi_3,\chi_6)=J(\chi_6,\chi_{12})=J(\chi_6,\chi_{-18})=J(\chi_3,\chi_6)$ なので

$$J(\chi_2,\chi_3)=\chi_{-6}(3)J(\chi_3,\chi_6). \tag{3.24}$$

これを (3.18) に代入すれば，$\frac{1}{\chi_{-6}(3)}=\chi_6(3)$ なので

$$J(\chi_1,\chi_1)J(\chi_3,\chi_6)=\chi_6(3)J(\chi_1,\chi_3)J(\chi_1,\chi_4)$$

となり，(3.1) の式が導ける．次に (3.2) の式を導く．(3.12) の式に $x=3,y=7,t=1$ を代入すると

$$\begin{aligned}&g(\chi_1)g(\chi_4)g(\chi_7)g(\chi_{10})g(\chi_{13})g(\chi_{16})g(\chi_{19})\\&\qquad=\chi_{-7}(7)g(\chi_7)g(\chi_3)g(\chi_6)g(\chi_9)g(\chi_{12})g(\chi_{15})g(\chi_{18}).\end{aligned}$$

この式に

$$\begin{cases} g(\chi_3)g(\chi_{18})=g(\chi_2)g(\chi_{19})\\ g(\chi_6)g(\chi_{15})=g(\chi_5)g(\chi_{16})\\ g(\chi_9)g(\chi_{12})=g(\chi_8)g(\chi_{13})\end{cases}$$

を代入して，さらに両辺に $\frac{g(\chi_1)^2}{g(\chi_2)g(\chi_5)g(\chi_{10})}$ をかけると

$$\frac{g(\chi_1)g(\chi_4)}{g(\chi_5)}\cdot\frac{g(\chi_1)g(\chi_1)}{g(\chi_2)}=\chi_{-7}(7)\frac{g(\chi_1)g(\chi_8)}{g(\chi_9)}\cdot\frac{g(\chi_1)g(\chi_9)}{g(\chi_{10})} \tag{3.25}$$

となる．これを Jacobi 和に直して，(3.22) を代入すると

$$J(\chi_1,\chi_4)J(\chi_1,\chi_1)=\chi_{-3}(3)\chi_{-7}(7)J(\chi_3,\chi_6)J(\chi_1,\chi_9). \tag{3.26}$$

あとは，$J(\chi_1,\chi_3)$ と $J(\chi_1,\chi_9)$ の関係式がわかればよい．

$$g(\chi_6)g(\chi_{15})=g(\chi_5)g(\chi_{16})=p$$

を用いて (3.21) の式を変化させて，両辺を $g(\chi_8)g(\chi_{16})$ で割れば，Jacobi 和の関係式 $J(\chi_1,\chi_{15})=\chi_{-3}(3)J(\chi_3,\chi_5)$ が導ける．さらに，$-1-15=-16\equiv 5\ (21)$ なので，$J(\chi_1,\chi_5)=J(\chi_1,\chi_{15})$ がいえて，

$$J(\chi_1,\chi_5)=\chi_{-3}(3)J(\chi_3,\chi_5) \tag{3.27}$$

である．また，$3\equiv 45\ (21)$ なので

$$J(\chi_3,\chi_5)=\sigma_5 J(\chi_1,\chi_9) \tag{3.28}$$

となる．(3.28) を (3.27) に代入すれば

$$J(\chi_1, \chi_5) = \chi_{-3}(3)\sigma_5 J(\chi_1, \chi_9). \tag{3.29}$$

この結果を利用して，$J(\chi_1, \chi_3)$ と $J(\chi_1, \chi_9)$ の関係を導く．$-1-3 = -4 \equiv 17\ (21), 1 \equiv 85\ (21)$ より

$$J(\chi_1, \chi_3) = J(\chi_1, \chi_{-4}) = J(\chi_{17}, \chi_{85}) = \sigma_{17} J(\chi_1, \chi_5). \tag{3.30}$$

(3.30) の式に (3.29) の式を代入すると

$$J(\chi_1, \chi_3) = \sigma_{17}(\chi_{-3}(3)\sigma_5 J(\chi_1, \chi_9)).$$

$\sigma_{17}\chi_{-3}(3) = \chi_{-51}(3) = \chi_{-9}(3)$ となることに注意して χ を外に出すと，$85 \equiv 1\ (21)$ なので，σ_{85} はそのまま消せて，結果として

$$J(\chi_1, \chi_3) = \chi_{-9}(3) J(\chi_1, \chi_9) \tag{3.31}$$

となる．(3.26) の式に代入すれば $\frac{\chi_{-3}(3)}{\chi_{-9}(3)} = \chi_6(3)$ より

$$J(\chi_1, \chi_4) J(\chi_1, \chi_1) = \chi_6(3)\chi_{-7}(7) J(\chi_3, \chi_6) J(\chi_1, \chi_3)$$

となり，(3.2) の式が導ける．あとは，(3.2) の式を (3.1) の式で割れば

$$(J(\chi_1, \chi_4))^2 = (\chi_7(7) J(\chi_3, \chi_6))^2 \tag{3.32}$$

となり，目標としていた式

$$J(\chi_1, \chi_4) = \mu \chi_7(7) J(\chi_3, \chi_6) \tag{3.33}$$

が導けた．ただし符号 μ については

$$\mu = \pm 1$$

である．ここまでは，Davenport-Hasse とノルムの関係式により容易に導ける．ここから，符号について考える．

$p = U^2 + 7V^2$ と分解するとき，$3|V \Rightarrow \mu = +1, 3|U \Rightarrow \mu = -1$ となることを示す．Hasse の主張を正しいとすると，$e = 21$ のとき，μ が p によらないということは先ほど確認した．しかし，結論からいうと，この関係式の μ は p によって動くので，この点で，今回の関係式は Hasse の主張の反例になっている．今から，この μ について考

える．ここで S を $\gamma^S = 7$ で定義する．χ の定義より，この S に対して $\chi_m(7) = \beta^{mS}$ が成り立つ．ここから使う 3 つの等式をあげておく．

$$\sigma_2 J(\chi_3, \chi_6) = J(\chi_3, \chi_6), \tag{3.34}$$

$$\mu\beta^{-7S} J(\chi_1, \chi_4) = J(\chi_3, \chi_6), \tag{3.35}$$

$$\sigma_2\{\beta^{-7S} J(\chi_1, \chi_4)\} = \beta^{-7S} J(\chi_1, \chi_4). \tag{3.36}$$

(3.34) は，(3.24) の式を示すときに確認した．(3.35) は今示した (3.33) を S を用いて書き直したものである．(3.36) は (3.34) に (3.35) を代入して得られる．(3.34)，(3.36) より $J(\chi_3, \chi_6)$ と $\beta^{-7S} J(\chi_1, \chi_4)$ は σ_2 で不変である．上の 3 つの式を用いて μ について考える．まず，(3.15) を利用して，Jacobi 和を Dickson-Hurwitz 和と β に変換して，β の 1 次結合の形で表す．次に (3.34) と (3.36) に代入して，両辺の係数を比較することで，Dickson-Hurwitz 和の間に成り立つ関係式を求める．得られた式を使って $\beta^{-7S} J(\chi_1, \chi_4)$ を簡略化すると，Dickson-Hurwitz 和を使って定義される U, V を用いて

$$\beta^{-7S} J(\chi_1, \chi_4) = U + V\sqrt{-7}$$

という形で表すことができ，このノルムを考えれば

$$p = U^2 + 7V^2$$

と p と Dickson-Hurwitz 和の関係がわかる．$J(\chi_3, \chi_6)$ も同様にして $A + B\sqrt{-7}$ という形でかけるので，(3.35) に結果を代入して係数を比較すれば，μ と Dickson-Hurwitz 和との関係がわかるので，これと $p = U^2 + 7V^2$ を照らし合わせれば，p と μ との関係性が導ける．Jacobi 和が $\mathbb{Q}(\sqrt{-7})$ の元であることからこのように解くことができる．σ_2 の不変体は 2 次体である．これが $\mathbb{Q}(\sqrt{-7})$ であることを確認するために 1 つ元を構成しておく．

$$\begin{cases} x = \beta + \beta^2 + \beta^4 + \beta^8 + \beta^{11} + \beta^{16} \\ y = \beta^5 + \beta^{10} + \beta^{13} + \beta^{17} + \beta^{19} + \beta^{20} \end{cases}$$

とする．x, y は σ_2 で不変．$x + y = 1, xy = 2$ なので，この x, y は $t^2 - t + 2 = 0$ の解になっている．方程式を解くと $t = \frac{1 \pm \sqrt{-7}}{2}$ なので，$x, y \in \mathbb{Q}(\sqrt{-7})$．$\beta^{21} - 1$ を因数分解すると $\beta^{21} - 1 = (\beta - 1)(\beta^{14} + \beta^7 + 1) = 0$．$\beta \neq 1$ より $1 + \beta^7 + \beta^{14} = 0$ だから

$$\begin{aligned} x + y =& \beta(1 + \beta^7) + \beta^2(1 + \beta^{14}) + \beta^3(\beta^7 + \beta^{14}) \\ & + \beta^4(1 + \beta^7) + \beta^5(1 + \beta^{14}) + \beta^6(\beta^7 + \beta^{14}) \\ =& -(\beta^{15} + \beta^9 + \beta^3 + \beta^{18} + \beta^{12} + \beta^6). \end{aligned}$$

$\gamma = \beta^3$ とおくと，γ は 1 の原始 7 乗根だから，$1 + \gamma + \cdots + \gamma^6 = 0$．よって

$$x + y = -(\gamma + \gamma^2 + \cdots + \gamma^6) = 1.$$

また

$$xy = 6 + (\beta + \beta^2 + \cdots + \beta^{20}) + 2(\beta^7 + \beta^{14}) + (\beta^3 + \beta^6 \cdots + \beta^{18}).$$

$1 + \beta + \beta^2 + \cdots + \beta^{20} = 0, 1 + \beta^7 + \beta^{14} = 0, 1 + \beta^3 + \beta^6 \cdots + \beta^{18} = 0$ なので

$$xy = 6 - 1 - 2 - 1 = 2.$$

x, y を解にもつ t の方程式は $t^2 - t + 2 = 0$．これを解くと $t = \frac{1 \pm \sqrt{-7}}{2}$．よって，$x$ は $\mathbb{Q}(\sqrt{-7})$ の元であることがわかる．今のように，実際の元を考えれば，$\beta^{-7S} J(\chi_1, \chi_4)$ と $J(\chi_3, \chi_6)$ がともに $\mathbb{Q}(\sqrt{-7})$ の元であることはすぐにわかる．ここからは,「具体的にどのような形に書けるか」について考えていく．Dickson-Hurwitz 和 b に対して

$$J(\chi_n, \chi_{vn}) = (-1)^{vnf} \sum_{j=0}^{e-1} b(j, v) \beta^{nj} \tag{3.37}$$

が成り立つ．これについては [7, (2.11)] に詳しく書いてある．$n = 1, v = 4$ とすると

$$J(\chi_1, \chi_4) = \sum_{j=0}^{20} b(j, 4) \beta^j$$

なので，$j - 7S = i, v_i = b(i + 7S, 4)$ をおくと

$$\beta^{-7S} J(\chi_1, \chi_4) = \sum_{j=0}^{20} b(j, 4) \beta^{j-7S} = \sum_{i=0}^{20} b(i + 7S, 4) \beta^i = \sum_{i=0}^{20} v_i \beta^i. \tag{3.38}$$

b について，[6, (2.7)] より

$$b(i, v) = b(j, e - v - 1) \tag{3.39}$$

が成り立つ．また，[9, Lemma.1] より

$$b(j, v) = b(\overline{v} j, \overline{v}) \tag{3.40}$$

が成り立つ．$\bar{4} = 16$ なので，(3.40) の式を使って

$$b(i, 4) = b(\overline{4} i, \overline{4}) = b(16i, 16).$$

さらに (3.39) の式を使うと

$$b(16i, 16) = b(16i, 21 - 16 - 1) = b(16i, 4).$$

よって

$$v_i = v_{16i}.$$

さらにこの i に $16i$ を改めて代入して考えれば

$$v_{16i} = v_{16\cdot 16i} = v_{4\cdot 4\cdot \bar{4}i} = v_{4i}.$$

以上より

$$v_i = v_{4i} = v_{16i} \tag{3.41}$$

がわかる．$i = 1, 2, 3, 5, 9, 10$ を代入すると

$$\begin{cases} v_1 = v_4 = v_{16} \\ v_2 = v_8 = v_{11} \\ v_3 = v_{12} = v_6 \\ v_5 = v_{20} = v_{17} \\ v_9 = v_{15} = v_{18} \\ v_{10} = v_{19} = v_{13} \end{cases} \tag{3.42}$$

であることがわかるので，これを使って式を変形すると

$$\begin{aligned} \sum_{i=0}^{20} v_i\beta^i = v_0 &+ v_1(\beta + \beta^4 + \beta^{16}) + v_2(\beta^2 + \beta^8 + \beta^{11}) \\ &+ v_3(\beta^3 + \beta^6 + \beta^{12}) + v_5(\beta^5 + \beta^{17} + \beta^{20}) + v_7\beta^7 \\ &+ v_9(\beta^9 + \beta^{15} + \beta^{18}) + v_{10}(\beta^{10} + \beta^{13} + \beta^{19}) + v_{14}\beta^{14}. \end{aligned} \tag{3.43}$$

次に，β の次数を下げるように式変形をする．

$$\begin{cases} 1 + \beta^7 + \beta^{14} = 0 \\ 1 + \beta^3 + \cdots + \beta^{18} = 0 \end{cases}$$

を利用して各係数を $1, \beta + \beta^4 - \beta^9, \beta^2, \beta^7, \beta^8 + \beta^{11}$ の 5 つの基底の 1 次結合の形に書き直すと

$$\begin{aligned} \beta + \beta^4 + \beta^{16} &= \beta + \beta^4 + \beta^2(-1 - \beta^7) \\ &= (\beta + \beta^4 - \beta^9) - \beta^2, \end{aligned}$$

$$
\begin{aligned}
\beta^3+\beta^6+\beta^{12} &= -1-\beta^9-\beta^{15}-\beta^{18}\\
&= -1-\beta^9-\beta(-1-\beta^7)-\beta^4(-1-\beta^7)\\
&= -1+(\beta+\beta^4-\beta^9)+(\beta^8+\beta^{11}),\\
\beta^5+\beta^{17}+\beta^{20} &= \beta^2(-1-\beta^6-\beta^9-\beta^{12})\\
&= -\beta^2-\beta^8-\beta^{11}-\beta^{14}\\
&= 1-\beta^2+\beta^7-(\beta^8+\beta^{11}),\\
\beta^9+\beta^{15}+\beta^{18} &= \beta^9+\beta(-1-\beta^7)+\beta^4(-1-\beta^7)\\
&= -(\beta+\beta^4-\beta^9)-(\beta^8+\beta^{11}),\\
\beta^{10}+\beta^{13}+\beta^{19} &= \beta(-1-\beta^3-\beta^6-\beta^{15})\\
&= -\beta-\beta^4-\beta^7-\beta^2(-1-\beta^7)\\
&= -(\beta+\beta^4-\beta^9)+\beta^2-\beta^7,\\
\beta^{14} &= -1-\beta^7
\end{aligned}
$$

となる．結果をまとめると，

$$
\text{(3.44)}\qquad
\begin{cases}
\beta+\beta^4+\beta^{16} = (\beta+\beta^4-\beta^9)-\beta^2\\
\beta^3+\beta^6+\beta^{12} = -1+(\beta+\beta^4-\beta^9)+(\beta^8+\beta^{11})\\
\beta^5+\beta^{17}+\beta^{20} = 1-\beta^2+\beta^7-(\beta^8+\beta^{11})\\
\beta^9+\beta^{15}+\beta^{18} = -(\beta+\beta^4-\beta^9)-(\beta^8+\beta^{11})\\
\beta^{10}+\beta^{13}+\beta^{19} = -(\beta+\beta^4-\beta^9)+\beta^2-\beta^7\\
\beta^{14} = -1-\beta^7
\end{cases}
$$

と書ける．これを (3.43) に代入して整理すると

$$
\begin{aligned}
\beta^{-7S}J(\chi_1,\chi_4) &= v_0+v_5-v_3-v_{14}+(v_1+v_3-v_9-v_{10})(\beta+\beta^4-\beta^9)\\
&\quad+(v_2+v_{10}-v_1-v_5)\beta^2+(v_5+v_7-v_{10}-v_{14})\beta^7\\
&\quad+(v_2+v_3-v_5-v_9)(\beta^8+\beta^{11}).
\end{aligned}
\qquad\text{(3.45)}
$$

次に，(3.43) の両辺に σ_2 を対応させる．v_i は σ で不変なので

$$
\begin{aligned}
\sigma_2\{\beta^{-7S}J(\chi_1,\chi_4)\} &= v_0+v_1\sigma_2(\beta+\beta^4+\beta^{16})\\
&\quad+v_2\sigma_2(\beta^2+\beta^8+\beta^{11})+v_3\sigma_2(\beta^3+\beta^6+\beta^{12})\\
&\quad+v_5\sigma_2(\beta^5+\beta^{17}+v_7\sigma_2\beta^7+v_9\sigma_2(\beta^9+\beta^{15}+\beta^{18})\\
&\quad+v_{10}\sigma_2(\beta^{10}+\beta^{13}+\beta^{19})+v_{14}\sigma_2\beta^{14}.
\end{aligned}
\qquad\text{(3.46)}
$$

β を含む項を σ_2 で変換した結果は以下の通り.

$$\begin{aligned}
\sigma_2\{\beta+\beta^4+\beta^{16}\} &= \beta^2+(\beta^8+\beta^{11}),\\
\sigma_2\{\beta^2+\beta^8+\beta^{11}\} &= \beta+\beta^4+\beta^{16} = (\beta+\beta^4-\beta^9)-\beta_2,\\
\sigma_2\{\beta^3+\beta^6+\beta^{12}\} &= \beta^3+\beta^6+\beta^{12} = -1+(\beta+\beta^4-\beta^9)+(\beta^8+\beta^{11}),\\
\sigma_2\{\beta^5+\beta^{17}+\beta^{20}\} &= \beta^{10}+\beta^{13}+\beta^{19} = -(\beta+\beta^4-\beta^9)+\beta^2-\beta^7,\\
\sigma_2\{\beta^7\} &= \beta^{14} = -1-\beta^7,\\
\sigma_2\{\beta^9+\beta^{15}+\beta^{18}\} &= \beta^9+\beta^{15}+\beta^{18} = -(\beta+\beta^4-\beta^9)-(\beta^8+\beta^{11}),\\
\sigma_2\{\beta^{10}+\beta^{13}+\beta^{19}\} &= \beta^5+\beta^{17}+\beta^{20} = 1-\beta^2+\beta^7-(\beta^8+\beta^{11}),\\
\sigma_2\{\beta^{14}\} &= \beta^7.
\end{aligned}$$

簡単のためまとめて書くと

$$\text{(3.47)}\qquad \begin{cases}
\sigma_2\{\beta+\beta^4+\beta^{16}\} = \beta^2+(\beta^8+\beta^{11})\\
\sigma_2\{\beta^2+\beta^8+\beta^{11}\} = (\beta+\beta^4-\beta^9)-\beta_2\\
\sigma_2\{\beta^3+\beta^6+\beta^{12}\} = -1+(\beta+\beta^4-\beta^9)+(\beta^8+\beta^{11})\\
\sigma_2\{\beta^5+\beta^{17}+\beta^{20}\} = -(\beta+\beta^4-\beta^9)+\beta^2-\beta^7\\
\sigma_2\{\beta^7\} = \beta^{14} = -1-\beta^7\\
\sigma_2\{\beta^9+\beta^{15}+\beta^{18}\} = -(\beta+\beta^4-\beta^9)-(\beta^8+\beta^{11})\\
\sigma_2\{\beta^{10}+\beta^{13}+\beta^{19}\} = 1-\beta^2+\beta^7-(\beta^8+\beta^{11})\\
\sigma_2\{\beta^{14}\} = \beta^7
\end{cases}$$

となる．これらを (3.46) に代入して，1 次結合の形にまとめると，

$$\text{(3.48)}\qquad \begin{aligned}
&\sigma_2\{\beta^{-7S}J(\chi_1,\chi_4)\}\\
&\quad = v_0+v_{10}-v_3-v_7+(v_2+v_3-v_5-v_9)(\beta+\beta^4-\beta^9)\\
&\qquad +(v_1+v_5-v_2-v_{10})\beta^2+(v_{10}+v_{14}-v_5-v_7)\beta^7\\
&\qquad +(v_1+v_3-v_9-v_{10})(\beta^8+\beta^{11}).
\end{aligned}$$

(3.36) より $\beta^{-7S}J(\chi_1,\chi_4) = \sigma_2\{\beta^{-7S}J(\chi_1,\chi_4)\}$ で，$\{1,\beta,\beta_2,\cdots,\beta_{11}\}$ は $\mathbb{Q}(\beta)/\mathbb{Q}$ の基底なので，(3.45) と (3.48) の係数を比較して v_i の関係式を導く．1 の係数を比較すると

$$v_0+v_5-v_3-v_{14} = v_0+v_{10}-v_3-v_7$$

なので,

$$v_{10}-v_5 = v_7-v_{14}.$$

β の係数を比較すると

$$v_1 + v_3 - v_9 - v_{10} = v_2 + v_3 - v_5 - v_9$$

なので,

$$v_1 - v_2 = v_{10} - v_5.$$

β^2 の係数を比較すると

$$v_2 + v_{10} - v_1 - v_5 = v_1 + v_5 - v_2 - v_{10} = 0$$

なので,

$$v_1 - v_2 = v_{10} - v_5.$$

β^7 の係数を比較すると

$$v_5 + v_7 - v_{10} - v_{14} = v_{10} + v_{14} - v_5 - v_7 = 0$$

なので,

$$v_{10} - v_5 = v_7 - v_{14}.$$

β^8 の係数を比較すると

$$v_2 + v_3 - v_5 - v_9 = v_1 + v_3 - v_9 - v_{10}$$

なので,

$$v_1 - v_2 = v_{10} - v_5.$$

これらの結果をまとめると,

$$v_1 - v_2 = v_{10} - v_5 = v_7 - v_{14} \tag{3.49}$$

となる．これを (3.45) の右辺に対応させる．1 の係数は $v_0 + v_5 - v_3 - v_{14}$，β^1 の係数は $v_1 + v_3 - v_9 - v_{10}$ のままで考えると，β^2 の係数は

$$v_2 + v_{10} - v_1 - v_5 = -(v_1 - v_2) + (v_{10} - v_5) = 0,$$

β^7 の係数は

$$v_5 + v_7 - v_{10} - v_{14} = -(v_{10} - v_5) + (v_7 - v_{14}) = 0,$$

β^8 の係数は

$$v_2 + v_3 - v_5 - v_9 = (v_2 - v_5) + v_3 - v_9 = (v_1 - v_{10}) + v_3 - v_9$$

となり，β^1 の係数と等しい．この結果を利用して (3.45) の右辺をまとめると，

$$\beta^{-7S}J(\chi_1,\chi_4) = v_0 + v_5 - v_3 - v_{14} + (v_1 + v_3 - v_9 - v_{10})(\beta + \beta^4 - \beta^9 + \beta^8 + \beta^{11})$$

である．ここで

$$\begin{cases} E = v_0 + v_5 - v_3 - v_{14} \\ 2V = v_1 + v_3 - v_9 - v_{10} \end{cases}$$

とおくと

$$\beta^{-7S}J(\chi_1,\chi_4) = E + 2V(\beta + \beta^4 - \beta^9 + \beta^8 + \beta^{11}) \tag{3.50}$$

となり，先ほどの計算より

$$\beta^9 + \beta^{15} + \beta^{18} = (\beta + \beta^4 - \beta^9) + (\beta^8 + \beta^{11})$$

なので

$$\beta^{-7S}J(\chi_1,\chi_4) = E - 2V(\beta^9 + \beta^{15} + \beta^{18}). \tag{3.51}$$

ここで $\beta^9 + \beta^{15} + \beta^{18}$ を具体的な数字で表すために，

$$\begin{cases} x = \beta^9 + \beta^{15} + \beta^{18} \\ y = \beta^3 + \beta^6 + \beta^{12} \end{cases}$$

として，x について考える．

$$\begin{cases} x + y = \beta^3 + \beta^6 + \beta^9 + \beta^{12} + \beta^{15} + \beta^{18} = -1 \\ xy = 3 + \beta^3 + \beta^6 + \beta^9 + \beta^{12} + \beta^{15} + \beta^{18} = 2 \end{cases}$$

なので，x, y を解にもつ方程式は

$$t^2 + t + 2 = 0$$

であり，これを解くと

$$t = \frac{-1 \pm \sqrt{-7}}{2}.$$

$x = \frac{-1-\sqrt{-7}}{2}$ として，(3.51) に代入すると

$$\beta^{-7S}J(\chi_1,\chi_4) = E - 2V\frac{-1-\sqrt{-7}}{2} = E + V + V\sqrt{-7}. \tag{3.52}$$

ここで，p と v_i の関係について考える．$U = E + V$ とすると

$$\beta^{-7S} J(\chi_1, \chi_4) = U + V\sqrt{-7} \tag{3.53}$$

となり，両辺についてノルムを考えれば

$$U^2 + 7V^2 = p \tag{3.54}$$

が得られる．以上より，Dickson-Hurwitz 和で構成された整数 U, V と p の関係を導くことができた．次は，μ と U, V の関係式を導く．そのため，$J(\chi_3, \chi_6)$ の場合について考える．得られた結果を $\mu\beta^{-7S} J(\chi_1, \chi_4) = J(\chi_3, \chi_6)$ に代入すれば，μ と U, V の関係式が作れるので，結果的に p と μ の関係がわかる．$J(\chi_3, \chi_6)$ にも同様の式変形を行うことによって $\mathbb{Q}(\sqrt{-7})$ の形で書くことができる．[8, (3)] より $e = xy$ のとき $J_e(\chi_{ym}, \chi_{yn}) = J_x(\chi_m, \chi_n)$ が成り立つ．$e = 21 = 7 \cdot 3$ なので，$x = 7, y = 3, m = 1, n = 2$ とすると，

$$J_{21}(3, 6) = J_7(1, 2) = J_7(1, -1 - 2) = J_7(1, 4).$$

β^3 は 1 の 7 乗根なので

$$J_7(1, 4) = \sum_{j=0}^{6} b_7(j, 4)\beta^{3j}.$$

$\overline{4} = 2$ より $b_7(j, 4) = b_7(\overline{4}j, \overline{4}) = b_7(2j, 2) = b_7(2j, 7 - 2 - 1) = b_7(2j, 4)$ だから

$$\begin{cases} b_7(1, 4) = b_7(2, 4) = b_7(4, 4) \\ b_7(3, 4) = b_7(6, 4) = b_7(5, 4) \end{cases} \tag{3.55}$$

なので

$$\begin{aligned} \sum_{j=0}^{6} b_7(j, 4)\beta^{3j} =& b_7(0, 4) + b_7(1, 4)(\beta^3 + \beta^6 + \beta^{12}) \\ &+ b_7(3, 4)(\beta^9 + \beta^{15} + \beta^{18}). \end{aligned} \tag{3.56}$$

β に関しては，先ほどの結果より

$$\begin{cases} \beta^3 + \beta^6 + \beta^{12} = \frac{-1+\sqrt{-7}}{2} \\ \beta^9 + \beta^{15} + \beta^{18} = \frac{-1-\sqrt{-7}}{2} \end{cases} \tag{3.57}$$

がわかっているので，これを使って式変形すると

$$\begin{aligned} J_{21}(\chi_3, \chi_6) =& b_7(0, 4) - \frac{b_7(1, 4) + b_7(3, 4)}{2} \\ &+ \frac{(b_7(1, 4) - b_7(3, 4))\sqrt{-7}}{2} \end{aligned} \tag{3.58}$$

となる．(3.35) より $\mu\beta^{-7S}J(\chi_1,\chi_4)=J(\chi_3,\chi_6)$ なので，(3.53) と (3.58) の右辺の 1 と $\sqrt{-7}$ の係数を比較すると

$$\begin{cases} 2U=\mu(2b_7(0,4)-b_7(1,4)-b_7(3,4)) \\ 2V=\mu(b_7(1,4)-b_7(3,4)) \end{cases} \tag{3.59}$$

がわかる．[8, (3)],[7, (2.11)] より，$e=xy$ のとき

$$\begin{cases} J_e(\chi_{ym},\chi_{yn})=J_x(\chi_m,\chi_n) \\ J(\chi_n,\chi_{vn})=(-1)^{vnf}\displaystyle\sum_{j=0}^{e-1}b(j,v)\beta^{nj} \end{cases} \tag{3.60}$$

が成り立ち，この 2 つの式より $b_x(j,v)=\displaystyle\sum_{r=0}^{y-1}b_e(j+rx,v)$ なので

$$\begin{cases} b_7(0,4)=b_{21}(0,4)+b_{21}(7,4)+b_{21}(14,4)=v_0+v_7+v_{14} \\ b_7(1,4)=b_{21}(1,4)+b_{21}(8,4)+b_{21}(15,4)=v_1+v_8+v_{15}=v_1+v_2+v_9 \\ b_7(3,4)=b_{21}(3,4)+b_{21}(10,4)+b_{21}(17,4)=v_3+v_{10}+v_{17}=v_3+v_{10}+v_5 \end{cases}$$

であることがわかる．これを (3.59) に代入すると

$$\begin{cases} 2U=\mu(2v_0+2v_7+2v_{14}-v_1-v_2-v_9-v_3-v_5-v_{10}) \\ 2V=\mu(v_1+v_2+v_9-v_3-v_5-v_{10}) \end{cases} \tag{3.61}$$

がえられる．$\mu=\pm1$ なので，μ の値に応じて U,V がどのような条件がもつかを場合わけして考える．

(i) $\mu=+1$ のとき

$$\begin{cases} 2V=v_1+v_3-v_9-v_{10} \\ 2V=v_1+v_2+v_9-v_3-v_5-v_{10} \end{cases}$$

なので，辺々足すと

$$4V=2(v_1-v_{10})+v_2-v_5.$$

$v_2-v_5=v_1-v_{10}$ であるので

$$4V=3(v_1-v_{10}).$$

よって，V は 3 の倍数であることがわかる．

(ii) $\mu = -1$ のとき

$$\begin{cases} E = v_0 + v_5 - v_3 - v_{14} \\ 2V = v_1 + v_3 - v_9 - v_{10} \end{cases}$$

より

$$2U = 2E + 2V = 2v_0 - 2v_{14} + 2v_5 + v_1 - v_{10} - v_3 - v_9.$$

これと

$$2U = -(2v_0 + 2v_7 + 2v_{14} - v_1 - v_2 - v_9 - v_3 - v_5 - v_{10}).$$

を辺々足すと

$$4U = 2v_1 + v_2 + 3v_5 - 2v_7 - 4v_{14} == 3(v_1 + v_5 - v_7 - v_{14}) - (v_1 - v_2 - v_7 + v_{14})$$

となり，$v_1 - v_2 - v_7 + v_{14} = 0$ だから

$$4U = 3(v_1 + v_5 - v_7 - v_{14}).$$

よって，U は 3 の倍数であることがわかる．以上の結果より

$$\begin{cases} \mu = +1 \Rightarrow 3|V \\ \mu = -1 \Rightarrow 3|U \end{cases}$$

がいえた．

逆に，U, V が 3 のそれぞれ 3 の倍数である場合について考える．$U^2 + 7V^2 = p$ で，$p \equiv 1\ (21)$ なので，$p \equiv 1\ (3)$．平方数は 3 を法として 0 か 1 と合同なので，U^2 と V^2 は，その和が 3 を法として 1 と合同であることから，必ずどちらかが 0 と合同で，もう一方が 1 と合同である．U を 3 の倍数と仮定すれば，必ず $V \equiv 1\ (3)$ である．今，$\mu = +1$ ならば $V \equiv 0\ (3)$ であることを示したので，この対偶を考えれば，$V \equiv 1\ (3)$ であるとき，$\mu = +1$ でないといえる．このとき，$\mu = \pm 1$ なので，必ず $\mu = -1$ である．以上より，$3|U \Rightarrow \mu = -1$ がいえる．同様にして，$3|V \Rightarrow \mu = +1$ もいえるので，上の結果と合わせると

$$\begin{cases} \mu = +1 \Leftrightarrow 3|V \\ \mu = -1 \Leftrightarrow 3|U \end{cases}$$

となり，同値関係であることがわかる．U と V は p に依存するので，μ も p に依存する．具体的に，$p \equiv 1\ (21)$ である p について考える．$43 = 6^2 + 7 \cdot 1^2, 421 = 13^2 + 7 \cdot 6^2$ なので，43 と 421 は p の条件をみたす．$p = 43$ は，U が 3 の倍数となる例であり，$p = 421$ は V が 3 の倍数となる例である．よって，μ は p によって変化するといえる．よって，関係式の符号は，p によって変化することがわかった．これは Hasse の主張の反例である．

この定理自体は，Jacobi 和の間の関係式について述べたものであるが，結果として Hasse の主張の一つの反例となっていることがわかる．$e = 28$ の場合，$e = 39$ の場合についても，基本的に同じ手法で証明できる．他に，$e = 15, 24$ の場合については [10, (27),(94)]，$e = 20$ の場合については [7, Lemma 3] で反例が述べてある．このように，素数でない e に関しては反例を導くことができると予想されている．

参考文献

[1] J. B. Muskat, Y. -c. Zee, Sign ambiguities of Jacobi sums, Duke Math. J. , 40 (1973) 313–334.

[2] K. Yamamoto, On a conjecture of Hasse concerning multiplicative relations of Gaussian sums, J. Combinatorial Theory 1 (1996) 476–489

[3] H. Hasse, Vorlesungen uber Zahlertheorie, Springer-Verlag, Berlin, 1964.

[4] H. Davenport, H. Hasse, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fallen, J. Reine Angew. Math. , 172 (1935) 151–182.

[5] K. Ireland, M. Rosen, A ClassicalIntroduction to Modern Number Theory, 93–94

[6] J. B. Muskat, The cyclotomic numbers of order fourteen, Acta Arith. , 11 (1966), 263–279

[7] J. B. Muskat, A. L. Whiteman, The cyclotomic numbers of order twenty, Acta Arith. 17 (1970) 185–216

[8] L. E. Dickson, Cyclotomy when e composite, Trans. Amer. Math. Soc. , 38 (1935), 187–200

[9] A. L. Whiteman, The cyclotomic numbers of order ten, Proc. Sympos. Appl. Math. , 10 (1960) 95–111

[10] J. B. Muskat, On Jacobi sums of certain composite orders, Trans. Amer. Math. Soc. , vol.134 (1968) 483–502.