数理解析研究所講究録
第1677巻 2010年 155-164

ガウスの冪剰余の理論について

日本カトリック神学院福岡キャンパス・神学生　伊波 靖 (Yasushi Iha)
JAPAN CATHOLIC SEMINARY
FUKUOKA CAMPUS

1. はじめに

この論文では, ガウスの数論の要である, 平方剰余理論と4次剰余理論に関するオリジナルな研究成果を述べる. 先ず, ガウスの冪剰余の理論にはルジャンドルとの関連が目に付く. その具体例を挙げると, 簡単なメモで, ガウスは, 二つの異なる正の奇素数 p, q に対し, q は p の平方剰余であることを $\left(\frac{q}{p}\right) = +1$ と表し, q は p の平方非剰余であることを $\left(\frac{q}{p}\right) = -1$ で表した. [「VIII. Zum Reziprozitätsgesetz der quadratischen und der biquadratischen Reste」(ガウス全集, 第10巻の第1分冊,pp.53)] これはルジャンドルが考案した記号に他ならない. [『数の理論のエッセイ (Éssai sur la théorie des nombres),Paris,1798』]D.A(『ガウス整数論』) ではこれらはそれぞれ qRp , qNp という記号で表されている. 『ガウス整数論』以後に公表された諸論文を見てもルジャンドル記号は全く使われていないが, 数学の記号としてはルジャンドル記号の方が簡明さにおいて遙かにガウスの表記よりも勝っている. ガウスもそのことを認識していたと考えられる. ガウスが規定したルジャンドル記号の意味は今日では広く受け入れられているものと同じであるが, この記号の考案者のルジャンドル本人の意図とは異なる. つまり, ルジャンドル記号の意味を今日的な意味に取り替えたのは, 実はガウスであることが分かる. そして, 4次剰余相互法則のガウス自身による証明では, 4次剰余記号を表すために, ルジャンドル記号と同型の記号が採用されている. [「XI. Beweis des Reziproritätssatzes für die biquadratischen Reste, der auf die Kreisteilung gegründet ist」(ガウス全集, 第10巻の第1分冊,pp.65-69)]

更に, これは相互法則の理論の根幹に触れることであるが, 4次剰余の理論の理論展開にあたり, ガウスは「一般化されたフェルマーの小定理」を基礎に据えた. ところが, フェルマーの小定理から出発してルジャンドル記号を導入し, その上で相互法則を提案するという道筋は, 平方剰余の理論の場合に, ルジャンドルが採用した理論展開であった. 二つの異なる正の奇素数間に成立する法則を探索しようとするルジャンドルに対し, ガウスのねらいは平方剰余の理論の「基本定理」を確立するところにあったので, ルジャンドルのようにフェルマーの小定理から出発する理由はなく, 実際, ガウスは『ガウス整数論』ではそのような理論展開をしなかった. しかし, 4次剰余の理論ではルジャンドルの考え方が全面的に採用されたのである.

2. 「平方剰余の理論における基本定理」の現代的な表記法との関係について

先ず, 現代的な表記による平方剰余相互法則とその第一補充法則及びガウス独自の平方剰余相互法則は次の通りである.

定理 2.1　ルジャンドル記号による平方剰余相互法則

p , q が相異なる奇素数ならば

$$\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}\left(\frac{p}{q}\right)$$

定理 2.2　ルジャンドル記号による平方剰余相互法則の第一補充法則

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$$

ガウスはD.Aの113条～124条にかけて ± 3 , ± 5 , ± 7 を取り上げて考察し, その都度, オイラーとラグランジュによる素数の形状理論の成果を引き合いに出した. そして, そこにはラグランジュにはなくてガウスにはある独特の視点も存在する. それは「相互性」の認識である.± 3 , ± 5 , ± 7 についてはその都度「相互性」が指摘された. 例えば,$+3$ の平方剰余になる数を次のように並べる. $q_1, q_2, q_3, \cdots\cdots$ このとき, ガウスは逆に ± 3 は $q_1, q_2, q_3, \cdots\cdots$ の平方剰余になるかどうかを調べた. この視点を延ばしていくと,131条の「平方剰余の理論における基本定理」になる. ガウスはこれを1795年に発見し, 翌1796年には証明を与えることにも成功したのである [D.A.135条～144条参照].

定理 2.3　平方剰余の理論における基本定理 (ガウスの平方剰余相互法則)

p が $4n+1$ 型という形の素数なら $+p$ は, 又 p が $4n+3$ 型という形なら $-p$ は, 正に取るときに p の剰余となる任意の素数の剰余であり, 正に取るときに p の非剰余となる任意の素数の非剰余である.

定理2.3より分かるように, ガウスの「平方剰余の理論における基本定理」の大きな特徴は, p , q が負の場合も扱っていることである. 従って, 正の奇素数のみをあつかっている現代的な表記による平方剰余相互法則の定理2.1ではまだ不十分であることが分かる. つまり, ガウスの「平方剰余の理論における基本定理」により近い形での現代的な表記法による定式化は, 次のように「平方剰余相互法則」と「平方剰余相互法則の第一補充法則」を組み合わせた形であるといえる.

系 2.1　「平方剰余の理論における基本定理」により近い形での定式化

p , q は奇素数で, μ_1 , μ_2 は $\mathbb{Z}$ の単元とする. このとき次の式が成立する.

$$\left(\frac{\mu_2 q}{\mu_1 p}\right) = \frac{\mu_2^{\frac{1}{2}(p-1)}}{\mu_1^{\frac{1}{2}(q-1)}} \cdot (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)} \left(\frac{\mu_1 p}{\mu_2 q}\right)$$

(証明)

$$\left(\frac{\mu_2 q}{\mu_1 p}\right) = \left(\frac{\mu_2 q}{p}\right) = \mu_2^{\frac{1}{2}(p-1)} \cdot \left(\frac{q}{p}\right)$$

$$= \mu_2^{\frac{1}{2}(p-1)} \cdot (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)} \left(\frac{p}{q}\right) \qquad \text{(平方剰余相互法則より)}$$

$$= \mu_2^{\frac{1}{2}(p-1)} \cdot (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)} \left(\frac{p}{\mu_2 q}\right) \qquad \text{(①式)}$$

ここで,

$$\left(\frac{\mu_1 p}{\mu_2 q}\right) = \mu_1^{\frac{1}{2}(q-1)} \cdot \left(\frac{p}{\mu_2 q}\right)$$

したがって, 両辺を $\mu_1^{\frac{1}{2}(q-1)}$ で割ると

$$\left(\frac{p}{\mu_2 q}\right) = \frac{1}{\mu_1^{\frac{1}{2}(q-1)}} \cdot \left(\frac{\mu_1 p}{\mu_2 q}\right) \qquad \text{(②式)}$$

したがって, ①式, ②式より

$$\left(\frac{\mu_2 q}{\mu_1 p}\right) = \frac{\mu_2^{\frac{1}{2}(p-1)}}{\mu_1^{\frac{1}{2}(q-1)}} \cdot (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)} \left(\frac{\mu_1 p}{\mu_2 q}\right)$$

系 2.2　素数の同伴元へ拡張した平方剰余相互法則の A_2 型，B_2 型への配分結果

先ず，次のように相互法則の型式を定義する．

$$\left(\frac{\triangle}{\bigcirc}\right)=\xi_2^2\cdot\left(\frac{\bigcirc}{\triangle}\right)\text{つまり，}\left(\frac{\triangle}{\bigcirc}\right)=\left(\frac{\bigcirc}{\triangle}\right)\quad(A_2\text{ 型相互法則})$$

$$\left(\frac{\triangle}{\bigcirc}\right)=\xi_2\cdot\left(\frac{\bigcirc}{\triangle}\right)\text{つまり，}\left(\frac{\triangle}{\bigcirc}\right)=-\left(\frac{\bigcirc}{\triangle}\right)\quad(B_2\text{ 型相互法則})$$

（ここで，$\bigcirc$，$\triangle\in\mathbb{Z}$ は (2) 以外の素元，ξ_2 は 1 の原始 2 乗根とする．）

このとき，ガウスの基本定理の全ての配分結果として次の表のようになる．

① $p\equiv 1\pmod 4$，$q\equiv 1\pmod 4$ のとき

	p	$-p$
q	A_2 型相互法則	A_2 型相互法則
$-q$	A_2 型相互法則	A_2 型相互法則

② $p\equiv 1\pmod 4$，$q\equiv 3\pmod 4$ のとき

	p	$-p$
q	A_2 型相互法則	B_2 型相互法則
$-q$	A_2 型相互法則	B_2 型相互法則

③ $p\equiv 3\pmod 4$，$q\equiv 1\pmod 4$ のとき

	p	$-p$
q	A_2 型相互法則	A_2 型相互法則
$-q$	B_2 型相互法則	B_2 型相互法則

④ $p\equiv 3\pmod 4$，$q\equiv 3\pmod 4$ のとき

	p	$-p$
q	B_2 型相互法則	A_2 型相互法則
$-q$	A_2 型相互法則	B_2 型相互法則

（証明）

$$\left(\frac{\mu_2 q}{\mu_1 p}\right)=\frac{\mu_2^{\frac{1}{2}(p-1)}}{\mu_1^{\frac{1}{2}(q-1)}}\cdot(-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}\left(\frac{\mu_1 p}{\mu_2 q}\right)$$

より，

(1)　$\mu_1=1$，$\mu_2=1$ のときは今までの平方剰余の相互法則である．

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)\quad(p,\ q\text{ が同時に }4k+3\text{ 型でないとき})$$

$$\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right)\quad(p,\ q\text{ が同時に }4k+3\text{ 型のとき})$$

(2)　$\mu_1=1$，$\mu_2=-1$ のとき

$$\begin{aligned}\left(\frac{-1\cdot q}{1\cdot p}\right)&=\frac{(-1)^{\frac{1}{2}(p-1)}}{1}\cdot(-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}\left(\frac{1\cdot p}{-1\cdot q}\right)\\&=(-1)^{\frac{1}{2}(p-1)+\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}\left(\frac{1\cdot p}{-1\cdot q}\right)\\&=(-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q+1)}\left(\frac{1\cdot p}{-1\cdot q}\right)\end{aligned}$$

したがって，「$p=4k+3$ 型かつ $q=4k+1$ 型」以外のとき

$$\left(\frac{-1\cdot q}{1\cdot p}\right)=\left(\frac{1\cdot p}{-1\cdot q}\right)$$

「$p=4k+3$ 型かつ $q=4k+1$ 型」のとき

$$\left(\frac{-1\cdot q}{1\cdot p}\right)=-\left(\frac{1\cdot p}{-1\cdot q}\right)$$

(3) $\mu_1=-1$, $\mu_2=1$ のとき

$$\left(\frac{1\cdot q}{-1\cdot p}\right)=(-1)^{\frac{1}{2}(p+1)\cdot\frac{1}{2}(q-1)}\left(\frac{-1\cdot p}{1\cdot q}\right)$$

したがって,「$p=4k+1$ 型かつ $q=4k+3$ 型」以外のとき

$$\left(\frac{1\cdot q}{-1\cdot p}\right)=\left(\frac{-1\cdot p}{1\cdot q}\right)$$

「$p=4k+1$ 型かつ $q=4k+3$ 型」のとき

$$\left(\frac{1\cdot q}{-1\cdot p}\right)=-\left(\frac{-1\cdot p}{1\cdot q}\right)$$

(4) $\mu_1=-1$, $\mu_2=-1$ のとき

$$\left(\frac{-1\cdot q}{-1\cdot p}\right)=\frac{(-1)^{\frac{1}{2}(p-1)}}{(-1)^{\frac{1}{2}(q-1)}}\cdot(-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}\left(\frac{-1\cdot p}{-1\cdot q}\right)$$

(i) $p=4k+1$, $q=4k'+1$ のとき

$$\frac{(-1)^{\frac{1}{2}(p-1)}}{(-1)^{\frac{1}{2}(q-1)}}\cdot(-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}=\frac{\mathbf{1}}{\mathbf{1}}\cdot\mathbf{1}=1$$

(ii) $p=4k+1$, $q=4k'+3$ のとき

$$\frac{(-1)^{\frac{1}{2}(p-1)}}{(-1)^{\frac{1}{2}(q-1)}}\cdot(-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}=\frac{\mathbf{1}}{\mathbf{-1}}\cdot\mathbf{1}=-1$$

(iii) $p=4k+3$, $q=4k'+1$ のとき

$$\frac{(-1)^{\frac{1}{2}(p-1)}}{(-1)^{\frac{1}{2}(q-1)}}\cdot(-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}=\frac{\mathbf{-1}}{\mathbf{1}}\cdot\mathbf{1}=-1$$

(iv) $p=4k+3$, $q=4k'+3$ のとき

$$\frac{(-1)^{\frac{1}{2}(p-1)}}{(-1)^{\frac{1}{2}(q-1)}}\cdot(-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}=\frac{\mathbf{-1}}{\mathbf{-1}}\cdot(\mathbf{-1})=-1$$

以上と同様な考察を 4 次剰余の理論においても行うと以下のようになる. 先ず, 現代的な表記法による 4 次剰余相互法則とその第一補充法則及びガウスの 4 次剰余の理論の基本定理（4 次剰余相互法則）[Gauss, Theoria residuorum biquadraticorum. Commentatio secunda , Werke , volume : bd. 2 , 95–148, 第 67 条参照] は次のようである.

定理 2.4　現代的な表記法による 4 次剰余相互法則

m , n を $\mathbb{Z}[i]$ の primary な素元とし, $(m)\neq(1+i)$, $(n)\neq(1+i)$, $(m)\neq(n)$ のとき次が成立する.

$$\left(\frac{m}{n}\right)_4=(-1)^{\frac{1}{4}(Nm-1)\cdot\frac{1}{4}(Nn-1)}\left(\frac{n}{m}\right)_4$$

定理 2.5　現代的な表記による４次剰余の第一補充法則

$\pi = a + bi \in \mathbb{Z}[i]$ を primary な素元とすると, 次が成立する.

$$\left(\frac{i}{\pi}\right)_4 = i^{-\frac{1}{2}(a-1)}$$

定理 2.6　４次剰余の理論の基本定理 (ガウスの４次剰余相互法則)

$a+bi$, $a'+b'i$ は, それらの随伴数の内で primary であるような, すなわち, 法 $2+2i$ に関して 1 と合同であるような素数を表すとしよう. このとき,2 つの数 $a+bi$, $a'+b'i$ の両方とも, 或いは少なくとも一方が第 1 種の法に属するならば, すなわち法 4 に関して $\equiv 1$ ならば, 数 $a+bi$ の法 $a'+b'i$ に関する 4 次剰余指標は, 数 $a'+b'i$ の法 $a+bi$ に関する指標と一致する. それに対して,2 つの数 $a+bi$, $a'+b'i$ がいずれも第 1 種の法に属さないならば, すなわち, 両方とも法 4 に関して $\equiv 3+2i$ とすれば, これらの指標は 2 だけ相異なる.

ここで, 定理 2.4 の現代的な表記法による４次剰余相互法則と定理 2.6 のガウスの４次剰余相互法則は同値である.[伊波靖, 「ガウスの４次剰余の理論について (1)」, 数理解析研究所講究録 1625, 数学史の研究,pp.56-66, 京都大学数理解析研究所, 2009 年を参照] 次に, ４次剰余相互法則の４つの型を定義する.

定義 2.2　４次剰余相互法則の型の定義

$$\left(\frac{\triangle}{\bigcirc}\right)_4 = \xi_4 \cdot \left(\frac{\bigcirc}{\triangle}\right)_4 \quad C_4 \text{ 型相互法則} \qquad , \qquad \left(\frac{\triangle}{\bigcirc}\right)_4 = \xi_4^2 \cdot \left(\frac{\bigcirc}{\triangle}\right)_4 \quad B_4 \text{ 型相互法則}$$

$$\left(\frac{\triangle}{\bigcirc}\right)_4 = \xi_4^3 \cdot \left(\frac{\bigcirc}{\triangle}\right)_4 \quad D_4 \text{ 型相互法則} \qquad , \qquad \left(\frac{\triangle}{\bigcirc}\right)_4 = \xi_4^4 \cdot \left(\frac{\bigcirc}{\triangle}\right)_4 \quad A_4 \text{ 型相互法則}$$

(ここで,$\bigcirc$, $\triangle \in \mathbb{Z}[i]$ は $(1+i)$ 以外の素元 , ξ_4 は 1 の原始４乗根とする.)

$\mathbb{Z}[i]$ の数 $\alpha = a+bi$ が primary ならば, つまり $\alpha \equiv 1 \pmod{2+2i}$ ならば,

$$a \equiv 3 \pmod 4 \text{ かつ } b \equiv 2 \pmod 4 \qquad \text{あるいは} \qquad a \equiv 1 \pmod 4 \text{ かつ } b \equiv 0 \pmod 4$$

であった. 上の primary から導かれる式より次の系が成立する.

系 2.3

(1)　$a \equiv 3$, $b \equiv 2 \pmod 4$ ならば $a^2+b^2-1 \equiv 4 \pmod 8$.

(2)　$a \equiv 1$, $b \equiv 0 \pmod 4$ ならば $a^2+b^2-1 \equiv 0 \pmod 8$.

４次剰余記号の primary な素数の同伴元への計算の拡張の「切り札」として, 系 2.3 の式を次のように拡張する.

系 2.4

(1)　$a^2+b^2-1 \equiv 4 \pmod 8$ はさらに, 次の　I_4型 , II_4型　に分けられる.

$$\mathrm{I}_4\text{型} : a^2+b^2-1 \equiv 4 \pmod{16} \quad , \quad \mathrm{II}_4\text{型} : a^2+b^2-1 \equiv 12 \pmod{16}$$

(2)　$a^2+b^2-1 \equiv 0 \pmod 8$ はさらに, 次の III_4型,IV_4型 に分けられる.

$$\mathrm{III}_4\text{型} : a^2+b^2-1 \equiv 0 \pmod{16} \quad , \quad \mathrm{IV}_4\text{型} : a^2+b^2-1 \equiv 8 \pmod{16}$$

primary な素数の同伴元まで拡張した４次剰余相互法則は, 簡潔にいえば「４次剰余相互法則」と「４次の第１補充法則」を組み合わせると２次の場合と同様に次のように「定式化」できる.

系 2.5　primary な素数の同伴元へ拡張した 4 次剰余相互法則の定式化

m , n は primary な素数で 4 次剰余相互法則の成立条件を全て満たし,μ_1 , μ_2 は $\mathbb{Z}[i]$ の全ての単元とする. このとき次の式が成立する.

$$\left(\frac{\mu_2 n}{\mu_1 m}\right)_4 = \frac{\mu_2^{\frac{1}{4}(N m-1)}}{\mu_1^{\frac{1}{4}(N n-1)}} \cdot (-1)^{\frac{1}{4}(N m-1)\cdot\frac{1}{4}(N n-1)} \left(\frac{\mu_1 m}{\mu_2 n}\right)_4$$

(証明)

$$\left(\frac{\mu_2 n}{\mu_1 m}\right)_4 = \left(\frac{\mu_2 n}{m}\right)_4 = \mu_2^{\frac{1}{4}(N m-1)} \cdot \left(\frac{n}{m}\right)_4$$

$$= \mu_2^{\frac{1}{4}(N m-1)} \cdot (-1)^{\frac{1}{4}(N m-1)\cdot\frac{1}{4}(N n-1)} \left(\frac{m}{n}\right)_4$$

$$= \mu_2^{\frac{1}{4}(N m-1)} \cdot (-1)^{\frac{1}{4}(N m-1)\cdot\frac{1}{4}(N n-1)} \left(\frac{m}{\mu_2 n}\right)_4 \qquad (①式)$$

ここで, 次が成立する.

$$\left(\frac{\mu_1 m}{\mu_2 n}\right)_4 = \mu_1^{\frac{1}{4}(N n-1)} \cdot \left(\frac{m}{\mu_2 n}\right)_4$$

したがって

$$\left(\frac{m}{\mu_2 n}\right)_4 = \frac{1}{\mu_1^{\frac{1}{4}(N n-1)}} \cdot \left(\frac{\mu_1 m}{\mu_2 n}\right)_4 \qquad (②式)$$

したがって, ①式, ②式より

$$\left(\frac{\mu_2 n}{\mu_1 m}\right)_4 = \frac{\mu_2^{\frac{1}{4}(N m-1)}}{\mu_1^{\frac{1}{4}(N n-1)}} \cdot (-1)^{\frac{1}{4}(N m-1)\cdot\frac{1}{4}(N n-1)} \left(\frac{\mu_1 m}{\mu_2 n}\right)_4$$

系 2.6　primary な素数の同伴元へ拡張した 4 次剰余相互法則への配分結果

$m = a + bi$, $n = c + di$ とする. ここで,m , n は primary な素数でかつ相互法則の成立条件をすべて満たしているとする. そのとき, 次の表が成立する. ただし,$\mu_1 m$ が左下と右上,$\mu_2 n$ は左上と右下とする.

① m, n ともに I_4型のとき

	m	$-m$	im	$-im$
n	B_4	A_4	C_4	D_4
$-n$	A_4	B_4	D_4	C_4
in	D_4	C_4	B_4	A_4
$-in$	C_4	D_4	A_4	B_4

② m が I_4型,n が II_4型のとき

	m	$-m$	im	$-im$
n	B_4	A_4	D_4	C_4
$-n$	A_4	B_4	C_4	D_4
in	D_4	C_4	A_4	B_4
$-in$	C_4	D_4	B_4	A_4

③ m が II_4型,n が I_4型のとき

	m	$-m$	im	$-im$
n	B_4	A_4	C_4	D_4
$-n$	A_4	B_4	D_4	C_4
in	C_4	D_4	A_4	B_4
$-in$	D_4	C_4	B_4	A_4

④ m,n ともに II_4型 のとき

	m	$-m$	im	$-im$
n	B_4	A_4	D_4	C_4
$-n$	A_4	B_4	C_4	D_4
in	C_4	D_4	B_4	A_4
$-in$	D_4	C_4	A_4	B_4

⑤ m , n ともに III_4型 のとき

	m	$-m$	im	$-im$
n	A_4	A_4	A_4	A_4
$-n$	A_4	A_4	A_4	A_4
in	A_4	A_4	A_4	A_4
$-in$	A_4	A_4	A_4	A_4

⑥ m が III_4型,n が IV_4型 のとき

	m	$-m$	im	$-im$
n	A_4	A_4	B_4	B_4
$-n$	A_4	A_4	B_4	B_4
in	A_4	A_4	B_4	B_4
$-in$	A_4	A_4	B_4	B_4

⑦ m が IV_4型,n が III_4型 のとき

	m	$-m$	im	$-im$
n	A_4	A_4	A_4	A_4
$-n$	A_4	A_4	A_4	A_4
in	B_4	B_4	B_4	B_4
$-in$	B_4	B_4	B_4	B_4

⑧ m , n がともに IV_4型 のとき

	m	$-m$	im	$-im$
n	A_4	A_4	B_4	B_4
$-n$	A_4	A_4	B_4	B_4
in	B_4	B_4	A_4	A_4
$-in$	B_4	B_4	A_4	A_4

⑨ m が I_4型 で n が III_4型 のとき

	m	$-m$	im	$-im$
n	A_4	A_4	A_4	A_4
$-n$	B_4	B_4	B_4	B_4
in	C_4	C_4	C_4	C_4
$-in$	D_4	D_4	D_4	D_4

⑩ m が I_4型 で n が IV_4型 のとき

	m	$-m$	im	$-im$
n	A_4	A_4	B_4	B_4
$-n$	B_4	B_4	A_4	A_4
in	C_4	C_4	D_4	D_4
$-in$	D_4	D_4	C_4	C_4

⑪ m が II_4型 で n が III_4型 のとき

	m	$-m$	im	$-im$
n	A_4	A_4	A_4	A_4
$-n$	B_4	B_4	B_4	B_4
in	D_4	D_4	D_4	D_4
$-in$	C_4	C_4	C_4	C_4

⑫ m が II_4型 で n が IV_4型 のとき

	m	$-m$	im	$-im$
n	A_4	A_4	B_4	B_4
$-n$	B_4	B_4	A_4	A_4
in	D_4	D_4	C_4	C_4
$-in$	C_4	C_4	D_4	D_4

⑬ m が III_4型 で n が I_4型 のとき

	m	$-m$	im	$-im$
n	A_4	B_4	D_4	C_4
$-n$	A_4	B_4	D_4	C_4
in	A_4	B_4	D_4	C_4
$-in$	A_4	B_4	D_4	C_4

⑭ m が III_4型 で n が II_4型 のとき

	m	$-m$	im	$-im$
n	A_4	B_4	C_4	D_4
$-n$	A_4	B_4	C_4	D_4
in	A_4	B_4	C_4	D_4
$-in$	A_4	B_4	C_4	D_4

⑮ m が IV_4型で n が I_4型のとき

	m	$-m$	im	$-im$
n	A_4	B_4	D_4	C_4
$-n$	A_4	B_4	D_4	C_4
in	B_4	A_4	C_4	D_4
$-in$	B_4	A_4	C_4	D_4

⑯ m が IV_4型で n が II_4型のとき

	m	$-m$	im	$-im$
n	A_4	B_4	C_4	D_4
$-n$	A_4	B_4	C_4	D_4
in	B_4	A_4	D_4	C_4
$-in$	B_4	A_4	D_4	C_4

(証明)
次の表の値

	$i^{\frac{1}{4}(N\pi-1)}$ の値	$(-1)^{\frac{1}{4}(N\pi-1)}$ の値	$(-i)^{\frac{1}{4}(N\pi-1)}$ の値
I_4型	i	-1	$-i$
II_4型	$-i$	-1	i
III_4型	1	1	1
IV_4型	-1	1	-1

と,m , n の両方とも I_4型か II_4型のとき B_4 型相互法則が成立するので

$$(-1)^{\frac{1}{4}(N\,m-1)\cdot\frac{1}{4}(N\,n-1)}=-1$$

と, 上記以外ならば A_4 型相互法則が成立するので

$$(-1)^{\frac{1}{4}(N\,m-1)\cdot\frac{1}{4}(N\,n-1)}=1$$

を使えば簡単に計算できる. ここでは, 1 例だけやる.
m が I_4型で,n が II_4型で $\mu_1=i$, $\mu_2=-i$ のとき.

$$\left(\frac{\mu_2 n}{\mu_1 m}\right)_4=\frac{\mu_2^{\frac{1}{4}(N\,m-1)}}{\mu_1^{\frac{1}{4}(N\,n-1)}}\cdot(-1)^{\frac{1}{4}(N\,m-1)\cdot\frac{1}{4}(N\,n-1)}\left(\frac{\mu_1 m}{\mu_2 n}\right)_4$$

を使い計算する.

$$\frac{\mu_2^{\frac{1}{4}(N\,m-1)}}{\mu_1^{\frac{1}{4}(N\,n-1)}}\cdot(-1)^{\frac{1}{4}(N\,m-1)\cdot\frac{1}{4}(N\,n-1)}=\frac{(-i)^{\frac{1}{4}(N\,m-1)}}{i^{\frac{1}{4}(N\,n-1)}}\cdot(-1)=\frac{-\mathbf{i}}{-\mathbf{i}}\cdot(-1)=-1$$

したがって, この場合次のように B_4 型相互法則が成立する.

$$\left(\frac{-in}{im}\right)_4=-1\cdot\left(\frac{im}{-in}\right)_4$$

他の全ての場合も同様に計算すればよい.(証明終わり)

これで, 4 次剰余相互法則を primary な素元の同伴元に拡張することができ, 前述の 4 つの相互法則の型を定義することにより,$(1+i)$ を除く, 全てのガウス整数の素元を, 4 つの型に配分することが出来た. 3 次の場合も同様なことができるが, 紙面の都合上この論文では割愛する.

3. 2次, 3次, 4次剰余相互法則の「構造」に関する考察

このセクションでは, ガウス独自の平方剰余の理論における基本定理及び 4 次剰余の理論の基本定理と深

い関係にある, 現代的な表記法による２次, ３次, ４次剰余相互法則の構造について考察する. 先ず, 必要な基本事項を述べることにする. ここで, ω は１の原始３乗根とする.

定義 3.1　$\mathbb{Z}[\omega]$ のノルム

$\alpha = a + b\omega \quad (a, b \in \mathbb{Z})$ のノルム $N\alpha$ を次のように定義する. $N\alpha = \alpha\overline{\alpha} = a^2 - ab + b^2$.

定義 3.2　３次剰余の primary

π が $\mathbb{Z}[\omega]$ の素元で $\pi \equiv 2 \pmod 3$ のとき primary という. $\pi = q$ (有理素数) のときは何の意味も付加されない. $\pi = a + b\omega$ のとき, π が primary ならば　$a \equiv 2 \pmod 3$　,　$b \equiv 0 \pmod 3$.

定理 3.1　ルジャンドル記号による３次剰余相互法則

$m \in \mathbb{Z}[\omega]$, $n \in \mathbb{Z}[\omega]$ は primary な素元で $Nm \neq 3$, $Nn \neq 3$, $(m) \neq (n)$ のとき

$$\left(\frac{n}{m}\right)_3 = \left(\frac{m}{n}\right)_3$$

先ず, ノルムについて考えてみたい. ここで３つの現代的な表記による冪剰余相互法則を見比べると, 「ノルムの意味」は, 次の表 3.1 のようにユークリッド域のその「環に用いられる大きさ」と考えると上手くいくことが分かる. したがって, 今, ２次のノルムを定義 3.3 のように定義することにする.

(表 3.1)　**ユークリッド域のその「環に用いられる大きさ」**

環	用いられる大きさ	
有理整数環	絶対値 $\|\quad\|$	$a = bq + r \qquad 0 \leqq r < \|b\|$
多項式環	次数 deg	$f(x) = g(x)q(x) + r(x)\ \ 0 \leqq \deg r(x) < \deg g(x)$
ガウス整数	ノルム $N(\ )$	$\alpha = \beta\gamma + \rho \qquad 0 \leqq N\rho < N\beta$

定義 3.3　平方剰余相互法則におけるノルムの定義

r は整数とする. このとき, 整数 r のノルム Nr を次のように定義する.

$$Nr = \|r\| \qquad (\|r\| \text{ は } r \text{ の絶対値})$$

そして, もう一つ問題がある. それは２次及び４次剰余相互法則の

$$\underline{(-1)}^{\frac{1}{2}(Np-1)\cdot\frac{1}{2}(Nq-1)} \quad , \quad \underline{(-1)}^{\frac{1}{4}(Nm-1)\cdot\frac{1}{4}(Nn-1)}$$

のアンダーライン部に於ける -1 である. これは以下のように考えるとうまくいく. 平方剰余相互法則

$$\left(\frac{q}{p}\right) = \underline{(-1)}^{\frac{1}{2}(Np-1)\cdot\frac{1}{2}(Nq-1)}\left(\frac{p}{q}\right)$$

でアンダーライン部の -1 は次のように考えるとうまくいく. つまり,

１の原始２乗根 -1 が作る２位の群 $\{-1, 1\}$ 内の全ての元の積

と考えるとうまくいく. つまり　$(-1) \times 1 = -1$. 同様に４次剰余相互法則

$$\left(\frac{m}{n}\right)_4 = \underline{(-1)}^{\frac{1}{4}(Nm-1)\cdot\frac{1}{4}(Nn-1)}\left(\frac{n}{m}\right)_4$$

で, アンダーライン部 -1 は何を意味しているかというと

１の原始４乗根 i が作る４位の群 $\{i, i^2, i^3, i^4\}$ 内の全ての元の積

と考えると良い. $i \times i^2 \times i^3 \times i^4 = i \times (-1) \times (-i) \times 1 = -\mathbf{1}$. 同様に3次剰余相互法則

$$\left(\frac{m}{n}\right)_3 = \underline{\mathbf{1}} \cdot \left(\frac{n}{m}\right)_3$$

で, アンダーライン部 $\mathbf{1}$ は何を意味しているかというと

1の原始3乗根 ω が作る3位の群 $\{\omega, \omega^2, \omega^3\}$ 内の全ての元の積

と考えるとうまくいく. $\omega \times \omega^2 \times \omega^3 = \omega^6 = \mathbf{1}$. ここで, ξ_n は1の原始 n 乗根とし,

$$\xi_n \cdot \xi_n^2 \cdot \xi_n^3 \cdot \cdots\cdots \xi_n^{n-2} \cdot \xi_n^{n-1} \cdot \xi_n^n$$

を考える. この式の値は, n が「奇数」のとき「1」,「偶数」のとき「-1」になる. ここで, $2 \leqq n \leqq 4$ の範囲で, 上の式が意味を持つことを許すならば, ガウスらによりこれまでに具体的に発見され, 現代的な表記により定式化されている, 平方剰余相互法則, 3次剰余相互法則, 4次剰余相互法則は次の一つの式にまとめることが出来る. つまり, 現代的な表記のレベルでは2次, 3次, 4次剰余相互法則は全く同一の構造をしていることが示された.

2次, 3次, 4次剰余相互法則を一つにまとめた式

$$\left(\frac{\alpha}{\beta}\right)_n = \left(\xi_n \cdot \xi_n^2 \cdot \xi_n^3 \cdot \cdots\cdots \xi_n^{n-2} \cdot \xi_n^{n-1} \cdot \xi_n^n\right)^{\frac{1}{n}(N\alpha-1)\cdot\frac{1}{n}(N\beta-1)} \left(\frac{\beta}{\alpha}\right)_n$$

($2 \leqq n \leqq 4$; $n = 2$ のときは α, β は奇素数, $n = 3, 4$ のときは primary な素元)

参考文献

[1] Gauss, Theoria residuorum biquadraticorum. Commentatio prima, Werke , volume : bd. 2 , 67–91,http://www-gdz.sub.uni-goettingen.de/cgi-bin/digbib.cgiPPN23599524X

[2] Gauss, Theoria residuorum biquadraticorum. Commentatio secunda , Werke , volume : bd. 2 , 95–148,http://www-gdz.sub.uni-goettingen.de/cgi-bin/digbib.cgiPPN23599524X

[3] Gauss, Kubische und biquadratische Reste, Werke , volume : bd. 10, Abt 1 ,37–77,http://www-gdz.sub.uni-goettingen.de/cgi-bin/digbib.cgiPPN236018647

[4] 高瀬正仁訳, 『ガウス整数論』(Disquisitiones Arithmeticae), 朝倉書店,1995 年

[5] 高瀬正仁, 「ガウスの数学日記について」, 第 14 回数学史シンポジウム会報 pp.13-28 , 津田塾大学数学・計算機科学研究所 ,2003 年

[6] 高瀬正仁, 「ガウスの数学日記について (続)」, 第 15 回 数学史シンポジウム会報 pp.30-43, 津田塾大学数学・計算機科学研究所, 2004 年

[7] 高瀬正仁, 「オイラーの数論とガウスの数論」, 数理解析研究所講究録 1625, 数学史の研究,pp.78-87, 京都大学数理解析研究所, 2009 年

[8] 高瀬正仁, 『ガウスの遺産と継承者たち』, 海鳴社,1990 年

[9] 倉田令二郎, 『平方剰余の相互法則』, 日本評論社,1992 年

[10] 足立恒雄, 『フェルマーの大定理』, 日本評論社,1996 年

[11] 加藤和也, 黒川信重, 斉藤毅, 『数論 I 』, 岩波書店, 2005 年

[12] 平松豊一, 『相互法則入門』, 牧野書店, 1998 年

[13] 河田敬義, 『19 世紀の数学 -整数論- 』, 共立出版, 1992 年

[14] 久保田富雄, 『数論論説』, 牧野書店, 1999 年

[15] 伊波靖, 「ガウスの 4 次剰余の理論について (1)」, 数理解析研究所講究録 1625, 数学史の研究,pp.56-66, 京都大学数理解析研究所, 2009 年