ガウスの整数論の形成への試論

杉本敏夫

§1．まえおき

さきに［1］関とガウスの正十七角形（上）、（下）で、関孝和とガウスを取り上げ、両者による正十七角形の作図のための計算を比較した。本稿は、[2] ガウスの整数論の冪剰余の章の形成において循環小数が果たした役割、および、円分論で証明される平方剰余の或る定理、この二つを「数学の形成」の立場から詳述する。

§2．循環小数

[3] 高木『数学史談』8章に、

「計算家ガウスは、必要の認められない場合にも驚くべく多くの数字を羅列している、… 幼時、既に 200 以下の素数及び素数冪の逆数を循環小数に化する表を作成し、後年それを 1000 以下まで継続している。」

とある。[2] 整数論には「付表Ⅲ」として 100 以下の素数及び素数冪の逆数が掲げられ、1000 以下の表は遺稿として [4]『全集』第Ⅱ巻に集録されている。後者を便宜、「拡大付表」と呼ぶ。

私は、すでに論考 [5] において、幼時における循環小数の観察から「原始根」の概念に到達したことを考察した。それと重複が多少あるが、再び取り上げよう。

法7の場合、

$1/7=0.142857\cdots,\quad 8/7=1.142857\cdots,\quad 50/7=7.142857\cdots,$

等の<u>小数部分</u>に注目すれば、1/7 と一致している。そこで整数部分を捨象して

$8/7\sim 50/7\sim 1/7=0.142857\cdots$

と置く。 <u>記号～</u> はガウスの合同式記号 ≡ に相当するが、後年のガウスの記号ではなく、もっと素朴に、《 幼時に彼が使ったかもしれない 》記号として、用いる。

さて、分母を 7 とする分数は

$1/7=0.142857\cdots,\quad 2/7=0.285714\cdots,\quad 3/7=0.428571\cdots,$

$4/7=0.571428\cdots,\quad 5/7=0.714285\cdots,\quad 6/7=0.857142\cdots,$

の六つが基本である。我々は<u>十進法</u>を用いるから、1/7 に 10 を掛ける度に、小数は1桁づつ繰り上がる。分子が 10 の冪乗であるような分数を並べ直すと、

$10/7=1.428571\cdots,\quad 10^2/7=14.285714\cdots,\quad 10^3/7=142.8571428\cdots,$

$10^4/7=1428.571428\cdots, 10^5/7=14285.714285\cdots, 10^6/7=142857.142852\cdots$

と、確かに1桁づつ繰り上がる。10, 10^2, 10^3 等を 7 で割った余りに注目すれば、

$10/7\sim 3/7=0.428571\cdots,\quad 10^2/7\sim 3^2/7\sim 2/7=0.285714\cdots,\quad 10^3/7\sim 3^3/7\sim 6/7=0.8571428\cdots,\quad 10^4/7\sim 3^4/7\sim 4/7=0.571428\cdots,$

$10^5/7 \sim 3^5/7 \sim 5/7=0.714285\cdots$, $10^6/7 \sim 3^6/7 \sim 1/7=0.142852\cdots$,
出発値の 1/7 の小数部分は、十進法に拘らなければ、この分数に3 を掛ける度に、と言い換えられ、その都度1桁づつ繰り上がる。ここから「法 7 では 3 が原始根である」という概念が形成される。《原始根》なる概念は、ガウスのブラウンシュヴァイク時代に、オイラーの著作に接して、そこから得たかも知れない。しかし、言葉よりもその実質的な意味は、すでに幼時の《遊び》のなかで会得していたに違いない。

§3．原始根

次に法 13 の場合を考える。[2] ガウスの整数論の「付表Ⅲ」には、

(0) …076923 ; (1) …461538

とある。その意味は (0) $1/13=0.076923\cdots$; (1) $6/13=0.461538\cdots$ であり、法 13 の循環小数が二種類、(0) と (1) の二組に分かれること、第二の組では数 6 が基本であることが分かる。結論を先取りすれば、「法 13 では 6 が原始根である。」さらに

$6/13=0.461538\cdots$, $6^2/13 \sim 10/13=0.769230\cdots$,
$6^3/13 \sim 8/13=0.615386\cdots$, $6^4/13 \sim 9/13=0.692307\cdots$,
$6^5/13 \sim 2/13=0.153846\cdots$, $6^6/13 \sim 12/13=0.923076\cdots$

の観察により、(1) の組と(0) の組が交代で現れ、(1) の組は法 13 の原始根 6 の奇数乗の組であり、(0) の組は法13 の原始根 6 の偶数乗の組であることが分かる。

四組に分かれる例は「付表Ⅲ」に法 53 の場合、三組に分かれる例は「拡大付表」に法 103 の場合がある。法11 の場合、2 が原始根であり、五組に分かれる。

(1) $2^1/11=2/11=0.18\cdots$, $2^6/11\sim9/11=0.81\cdots$, (2) $2^2/11=4/11=0.36\cdots$,
$2^7/11\sim7/11=0.63\cdots$, (3) $2^3/11=8/11=0.72\cdots$, $2^8/11\sim3/11=0.27\cdots$,
(4) $2^4/11\sim5/11=0.45\cdots$, $2^9/11\sim6/11=0.54\cdots$, (0) $2^5/11\sim10/11=0.90\cdots$,
$2^{10}/11\sim1/11=0.09\cdots$.

法 11 で、指数 e と 2 の乗冪2^e 及び指数 e と 3 の乗冪3^eとの対応表を作れば、

e	1	2	3	4	5	6	7	8	9	10
2^e	2	4	8	5	10	9	7	3	6	1

e	1	2	3	4	5
3^e	3	9	5	4	1

となり、底 2 では 10乗したとき初めて1になり(右)、法 11 の凡ての数を巡る。他方、底 3 では 5乗したとき1になる(左)。底 2 は原始根である。一応、底 3 は $(11-1)/2=5$, すなわち約半分の 5回の乗冪で 1 になるから、原始根でない。法 11 での乗冪表は、後でヴァンデルモンドの試みとの関連で、重要な論拠となる。

§4．冪剰余と平方剰余

[2] ガウスの整数論、第 3 章 冪剰余、第4章 平方剰余の実質的な内容も、数値例としては、幼児期以来の《数値実験》から得られていた、と想像される。

例えば法 7 の場合、

$1^6/7\sim1/7$. $2^3/7\sim1/7$, $2^6/7\sim1/7$. $3^6/7\sim1/7$. $4^3/7\sim1/7$,
$4^6/7\sim1/7$. $5^6/7\sim1/7$. $6^2/7\sim1/7$, $6^6/7\sim1/7$

等を観察すれば、冪剰余における基本定理「フェルマの小定理」(50条) が成立してい

る。また $(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6)/7 \sim 3^{0+2+1+4+5+3}/7 \sim 3^{15}/7 \sim 6/7$ となること、及び、分子の 6 に 1 を足した $(6+1)/7=7/7=1$ となることを見て、「ウィルソンの定理」(76 条) の成立を読み取ったかもしれない。私は、ガウスの発見が「整数論全体を律する《原始根》の概念と密接に結びついている」と考え、しかもガウスが幼少の頃、遊びとして弄んだ《循環小数》の組分けが、後の理論に発展した、と考える。

次に平方剰余の理論を見よう。法 7 の平方剰余は $2/7 \sim 3^2/7$, $4/7 \sim 3^4/7$, $1/7 \sim 3^6/7$ で、非剰余は $3/7 \sim 3^1/7$, $6/7 \sim 3^3/7$, $5/7 \sim 3^5/7$ である。こうした分類を素数 q ごとに調べれば、[2] 整数論の「付表 II」が作られる。付表 II の一部を次に示す。ガウスはルジャンドル記号を用いない。表は平方剰余の欄に横線 — が記入され、ルジャンドル記号の負号 − と紛らわしい。横線 — は、法 3 で +3, +7, +13, +19 が平方剰余であり、法 5 で −1, +5, +11, +19 が平方剰余であることを示す。横線 — が無ければ、非剰余を表わす。等々。

	−1	+2	+3	+5	+7	+11	+13	+17	+19
3			—		—		—		—
5	—			—		—			—
7		—			—	—			
11			—	—		—			
13	—		—				—	—	

この付表 II を眺めただけで、各素数 p と q との組み合わせについて、それが $4n+1$ 型（文字 a を用いる）であるか、$4n+3$ 型（文字 b を用いる）であるかに従って、どの組み合わせのとき平方剰余となり、どの組み合わせのとき平方非剰余となるのか、すなわち、「相互法則」を抽出するのは困難である。[2] 整数論、第 4 章「平方剰余」131 条のガウスの基本定理は、平方剰余の記号 R (residorum の略) と非剰余の記号 N (no residorum の略) を、文字 a や b と組み合わせて、例えば aRb, aNb の、壮大な一覧表となる。この表は、見る人を威圧する。ガウスはルジャンドル記号を用いないから、「平方剰余の相互法則」は、この様な表の形を取らざるを得なかった。

§5. 平方剰余の諸例

オイラー・ラグランジュの時代、平方剰余は次の如く扱われた。a と b と c を普通の数、p を素数とするとき、b が法 p の平方剰余であるとは、或る数 c が存在して方程式 $a^2-b=pc$ が成立すること、上記のガウスの表示では、bRp となる。b が法 p の平方非剰余とは、どんな数 c をとっても同じ方程式が成立しない、どんな数 c をとっても $a^2-b\neq pc$ を意味し、ガウスの表示では、bNp となる。

オイラーが 1773 年に証明した定理 (後の第一補充法則) は、次を主張する。-1 を剰余にする素数 p は、p が $4m+1$ の形の素数ならば、$a^2-(-1)=pc$ を成立させるような数 c が存在する(ガウスの表示では $-1Rp$)。p が $4m-1$ の形の素数ならば、如何なる数 c をとっても $a^2-(-1)\neq pc$ となる (ガウスの表示では $-1Np$)。

ルジャンドル記号では、「$(-1/p)$ は p が $4m-1$ の形の素数のときは $+1$ であり、$(-1/p)$ は p が $4m+1$ の形の素数のときは -1 となる」と簡潔に述べられる。ガウスはルジャンドル記号を用いず、言葉で(ガウス表示で)上記のように文章で述べた。

ガウスは、このオイラーの定理を、「1795 年、私が研究を始めた頃、オイラーらの手によって成し遂げられた事柄について、何も知らなかった。… 偶然、この素晴しい真理に出会った。」と、[2] 整数論の序文で述懐した。

法 2 のときは、四次剰余の問題に発展するので他日に回わし、ここでは扱わない。

数 3 は、それとは別の素数 p を法として、ルジャンドル記号を用いて簡潔な式にまとめられる。しかし、ここではオイラー、ラグランジュの時代の記法に戻って説明を続けることにする。以下、素数 p が 3, 5, 7 のとき、それと別の素数 q を法として、いつ pRq となるか、また、いつ pNq となるか、それが当面の問題である。

特に素数 p が $+3$ または -3 であり、法 q が $4n+1$ または $4n+3$ の形の数であるとき、「いつ pRq となり、いつ pNq となるか?」それが問題となる。ガウスはオイラー・ラグランジュに倣い、q を $12n+5$, $12n+11$, $12n+7$, $12n+1$ の 4 種に分類する。ここでは簡素化のため、q_5, q_{11}, q_7, q_1 と表す。後の言葉で、「数 3 に対する相互法則」と呼ばれる内容は、ガウスの場合は式の形ではなく、[2] 整数論、第 4 章 二次合同式、第 131 条に見る一覧表の形を取る。

Ⅰ. $-3Nq_5$, $+3Nq_5$, Ⅱ. $-3Nq_{11}$, $+3Rq_{11}$,

Ⅲ. $+3Nq_7$, $-3Rq_7$, Ⅳ. $+3Rq_1$, $-3Rq_1$.

(ルジャンドル記号に馴れた我々にとっては冗長だが、当時はかかる一覧表であった。) このうち 特に Ⅳ. の場合 $-3Rq_1$ の証明が困難であった。その切り抜け策:$4(a^3-1)=4(a^2+a+1)(a-1)$ は q_1により割り切れるが、$(a-1)$ は q_1により割り切れないから、$4(a^2+a+1)$ が q_1 で割り切れるか? $4a^2+4a+4$ は $(2a+1)^2+3$ と変形されるから、q_1 で割り切れる。まとめて $-3Rq_1$ を得る。これに、オイラーが示した $-1Rq_1$ と組み合わせると、$+3Rq_1$ も成立する。

次に、素数 p が 5 の場合、法 q_1 が $20n+1$ の形の数であるとき、(それは q_1 が $5n+1$ の形の数であるとき、と換言される、) ここでも $4a^4+4a^3+4a^2+4a+4$ が $(2a^2+a+2)^2-5a^2$ と変形されるので、$5Rq_1$ となる、という事実を用いた。

さらに、素数 p が 7 であり、法 q_1 が $7n+1$ の形の数であるとき、$4a^6+4a^5+4a^4+4a^3+4a^2+4a+4$ を $(2a^3+a^2-a-2)^2+7(a^2+a)^2$ と変形する。aNq_1, $(a+1)Nq_1$ だから、必然的にもう一つの因数 -7 が$-7Rq_1$ となる、という事実を用いる。これもラグランジュの工夫であり、この計算も、素晴らしい。

ガウスの所謂《美しい定理》とは、法 p が素数 3, 5, 7 である場合の $p-1$ 次の式の変形が、法がもっと一般の素数 p の場合にも成立することを主張するのである。

これらを合併したガウスの「基本定理」(すなわち今日の「平方剰余の相互法則」) は、[2] 整数論、第 4 章 二次合同式、第 131 条に掲げられた、

「1. もし $\pm aRa'$ なら $\pm a'Ra$ である。」

に始まる、8 項目を並べた壮大な一覧表を形成する。(一覧表は、ぜひ『整数論』を見て欲しい。) 今日のルジャンドル記号を用いた「平方剰余の相互法則」の表現が、如何

ほど事態を簡潔化するか、ガウスの一覧表と比べてみれば分かる。

所で、ルジャンドル記号 (a/p) にも、二段階の意味がある。本人の用いた意味は、$a^{(p-1)/2}$ を p で割ったときの剰余（$-p/2$ と $+p/2$ の間にとる）を表し、（フェルマの小定理により、$+1$ と -1 のいずれかの値を取る）単なる略記号に過ぎず、その値には、直接、平方剰余か非剰余かを示す意味はなかった。

(a/p) の意味を「記号 (a/p) が $+1$ ならば法 p で a が平方剰余であり、-1 ならば 法 p で a が非剰余である」と述べるのは、後世の新たな定義づけである。記号の意味は、かなり複雑な内容を包含する。（高瀬氏の翻訳[2] の訳注(492 頁)参照）

§6. ガウスの手紙

本稿後半の主題は、ガウスからゲルリング宛の返事、すなわち「ガウスの手紙」にも出て来る「美しい定理」である。この言葉が出て来る個所を、[3]『数学史談』からではなく、[4]ガウス全集 X-1 巻 121 頁から直接翻訳してみよう。

「この発見については一度も公表したことがないが、正確に覚えている。それは 1796 年 3 月 29 日〔ガウス日記では 30 日〕のことであり、偶然に恵まれたのではない。既に以前から、すべては方程式〔引用者注、以下便宜のため、式番号を振る〕

$$(*1)\qquad (x^p-1)/(x-1)=0$$

の根を二組に分けることに関係していて、そこから『整数論』のなかの或る美しい定理〔357 条〕が出て来ることを発見した。日付は記さなかったが、ゲッチンゲン大学での最初の冬学期のことだ。数論の基礎に立って凡ての根の相互関係のことを張り詰めて熟考しているうち、休暇で故郷ブラウンシュヴァイクに帰省していた、あの日の朝、ベッドから起きだす前に、〔それらの根の相互の〕関係を明瞭に直観するという幸運がやってきた。それを正十七角形なる特別の場合に応用して、数値的に裏付けることは即座にできた。もちろん『整数論』第 7 章に述べた研究はその後の追加だ。この発見をたまたまイエナ学芸報知に報せたから、同年 5～6 月頃に記事がある筈だ。私の『整数論』の印刷は 1798 年 4 月に始めたが、ようやく 1801 年夏に完成した。〔下略〕 」

この記述は、二つの内容を含む。一つは、前回［1］関とガウスの正十七角形（下）で述べたように、従来、定規とコンパスによる作図が正五角形までしか知られていなかった所に、予期せぬ正十七角形が作図できるという内容だから、《ユークリッド以来の発見》としてセンセーショナルな話題であり、学生ガウスを一躍有名人にした。

いま一つの内容は、本稿が眼目とする、具体的な定理の発見を伝える。

§7. 美しい定理

手紙の中の「美しい定理」とは、[2]『整数論』第 4 章 124 条で予告された内容である。すなわち、第 7 章で、円分体の議論の展開が一段落した段階で登場する、357 条の定理を指す。

「一般に式

$$(*2)\qquad 4X=4(x^p-1)/(x-1)=4(x^{p-1}+x^{p-2}+\cdots+x^2+x+1)$$

はつねに

$$(*3)\qquad 4X=Y^2\mp pZ^2$$

（ここで上の符号は p が $4n+1$ 型のとき採用し、下の符号は p が $4n-1$ 型のとき採用する）という形に変えることができる」

と主張する。第4章119条では素数 3 の場合、123条では素数 5 の場合、124条では素数 7 の場合に証明された定理を一般化して、素数 p の場合に証明する。（ガウスはさらに一般の整数 n の場合を述べているが、実際に用いられる素数 p の場合だから、その場合に限定して引用する。）

ガウスは勿論、一般的に述べている。ここでは具体的な意味を確かめたいので、ラグランジュが $p=7$ の場合で打ち切ったその次に来る、$p=11$ の場合を取り上げる。第7章、357条の付表によれば、

$$Y=2x^5+4x^4-2x^3+2x^2-x-2,\quad Z=x^4+x$$

である。これから Y^2+11Z^2 を計算してみよう。

$$Y^2=4x^{10}+4x^9-7x^8+4x^7+4x^6-18x^5+4x^4+4x^3-7x^2+4x+4,$$

$$11Z^2=11x^8+22x^5+11x^2$$

から和を求めれば、確かに

$$Y^2+11Z^2=4x^{10}+4x^9+4x^8+4x^7+4x^6+4x^5+4x^4+4x^3+4x^2+4x+4,$$
$$=4(x^{11}-1)/(x-1)$$

となる。 私は手探りで計算してみた。しかし、手探りで Y の式、Z の式を探すのは非常に困難であった。$-7x^8$ と $11x^8$ とから $4x^8$ が得られる、などとは、予想もできない。計算に長けていたラグランジュでさえ、$n=7$ までで探求を止めたのも、無理はない。手探りでなく、やはり理論が必要であった。

第7章の当該の個所に戻り、ガウスに従って、証明の概略を辿ろう。

$$(*4)\qquad 4X=4(x^p-1)/(x-1)=z\cdot z'$$
$$z=R+S(m,1)+T(m,g),\qquad z'=R+S(m,g)+T(m,1)$$

ここに $(m,1)$ は、r を 1 の n 乗根、g を法 p の原始根とするとき、r^1 に始まる m 項周期、それを証明の中では $(m,1)$ を（文字 p は既に使ったので、代わりに）u で表す。(m,g) は r^g から始まる m 項周期であり、(m,g) を証明の中では v で表す。

注意すべき点は、前回述べたように、$(m,1)$ や (m,g) は「円分体の数」すなわち虚数である。ガウスは [2]『整数論』すなわち常識的に言えば、整数が相互に割れるか・割れないかを論ずる書物の中で、第7章に這入ると、全く唐突に、虚数、それも特に「円分体の数」を用いる。そもそも凡ての係数が 1 である代数方程式

$$(*5)\qquad X=(x^p-1)/(x-1)=x^{p-1}+x^{p-2}+\cdots+x^2+x+1=0$$

は、解けるのか？ 時は十八世紀の終わり頃である。後述のように、代数方程式の解法は、当時の数学者にとって最も悩ましい課題であった。ガウスは勿論、特別な形の方程式（$*5$）を解いて、「円分体の数」を用いて「美しい定理」を証明した。然しながら、基本定理の証明のための一補助定理に過ぎない「美しい定理」を証明するための道具立てとしては、余りに大袈裟ではないか。《鶏口を割くに牛刀を用いる》たぐいに近い。「円分体の数」を考えた直接の目的は、他にあったに違いない。

§ 8．ガウスの発見とは何か

重要な焦点は、ガウスが「美しい定理」の証明に留まらず、「円分体の数」の総合的な理論を開拓したことである。方程式（＊5）の根たちは、全体として調和の取れた相互関係を持っている。

重複を厭わずに、前回、[1]（下）§16～17, 円の 13 等分方程式の根の相互関係の例を再録する。ガウスが 13 等分方程式を研究したことは、同所で紹介し、さらに私の計算を補った。まず、法 13 における原始根 2 の乗冪表

e	1	2	3	4	5	6	7	8	9	10	11	12
2^e	2	4	8	3	6	12	11	9	5	10	7	1

によって、根 $r=\cos\phi+i\sin\phi$, $\phi=2\pi/13$ から、種々の《根の和》を作る。

$a_1=r^1+r^5+r^{12}+r^8$,　$a_2=r^2+r^{10}+r^{11}+r^3$,　$a_3=r^4+r^7+r^9+r^6$, の三根 a_g は、方程式　$a^3+a^2-4a+1=0$　を満たし、方程式 $b^2+b-1=0$ の二根 $b_1=r^4+r^3+r^{12}+r^9+r^{12}+r^1$, $b_2=r^2+r^8+r^6+r^{11}+r^5+r^7$ は、上の a_g とは交わらない。強いて a_g と b_h の交わりを作れば $c_1=r^{12}+r^1$, $c_2=r^5+r^8$, $c_3=r^{10}+r^3$, $c_4=r^2+r^{11}$,　$c_5=r^4+r^9$,　$c_6=r^7+r^6$　は、$c^6+c^5-5c^4-4c^3+6c^2+3c-1=0$ を満たす。他に可能な根は $d_1=r^3+r^9+r^1$,　$d_2=r^4+r^{12}+r^{10}$,　$d_3=r^8+r^{11}+r^7$, $d_4=r^2+r^6+r^5$ であり、方程式　$d^4+d^3+2d^2-4d+3=0$　を満たす。そして c_i と d_j の交わりは、12 個のすべての根 r^k から成り、それらの根 r^k は、円の 13 等分方程式 $X=r^{12}+r^{11}+r^{10}+\cdots\ \cdots+r^2+r+1=0$　を満たす。

ここに登場した凡ての根は、途中で複線に分かれ、最後に E に至って、次の根の系統図の中に納まる。出発の Ω は 1 以外の 12 根の凡て和 $=-1$ である。

$$\begin{array}{ccccc}
\Omega\ (\text{12 根の和}) & \text{———} & B\ (\text{2個の}\ b_h) & \text{———} & D\ (\text{4個の}\ d_j) \\
| & & | & & | \\
A\ (\text{3個の}\ a_g) & \text{———} & C\ (\text{6個の}\ c_i) & \text{———} & E\ (\text{12個の}\ r^k)
\end{array}$$

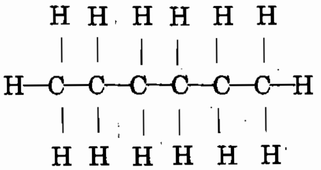
（前回、§14 の正七角形の場合も、§21 の正十九角形の場合も、凡ての根は複線の系統図に分かれる例であった。後者は、[2]『整数論』に載っている。）

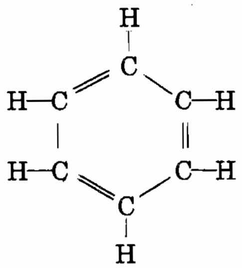
肝心な点は、「ガウスの手紙」の中の言葉「凡ての根の相互関係」である。私の推測では、A と B に分かれては再び C で会う。C と D に分かれては再び E で会う。このような根どうしの離合集散的な構成原理の発見こそが、記念すべき日の朝の発見と考えたい。これに対して正十七角形の場合は、系統図が「直線的」（上の組が下の組を包含する）であって、「凡ての根の相互関係」なる言葉には相応しくない。

ガウスは前夜、もやもやしたまま、（この十三等分方程式とは限らないが）「複線に分かれる場合の凡ての根の相互関係」を、こんを詰めて考えていた。 摩訶不思議！この未解決の問題が、寝ているうちに整理されて、起床直前に《解決》したのだ。

こうした事実を、多くの学者が述懐している。《発見学の核心！》 就寝前に《もやもやした》問題を、こんを詰めて考えている。翌朝、目覚める直前に発見が生じる。

化学者ケクレによる環状化合物「ベンゼン」の構造式の《発見》が記録されている。鎖状化合物では C_6H_6 を満たす構造式が見つからず、左図の鎖状化合物では H が多すぎて困っていた。たまたま《夢》の中で、蛇が自分の尻尾を咬むのを見て、六角形の構造式（右図）を発見した。





§9．ラグランジュの成功と失敗

ガウスの「美しい定理」を論じるに際して、[7] ティニョル等を参照して、簡単に代数方程式の解法の歴史を回顧しておこう。二次方程式（以下、各次の方程式とも、各係数を首項の係数で割った式の形にして考える）

（∗6）　$x^2+px+q=0$

の解法は、古代より知られていた。（今の中学校では、根の公式として教える。）

カルダノによる三次方程式の解法は画期的である。変形して y の二次の項の欠けた

（∗7）　$y^3+py+q=0$

の三根を a, b, c とし、三根の一次結合（後述）を v と w とし、さらに $y=v+w$ と置いて、$y=v+w$ を（∗7）に代入し、（∗7）の判別式を

（∗8）　$(v-w)^2 = q^2+(4/27)p^3 = d$

と置く（何故そのように置くのか、理由は後述）。これから簡単な計算により、

（∗9）　$v=\sqrt[3]{(-q+\sqrt{d})/2}$，　$w=\sqrt[3]{(-q-\sqrt{d})/2}$

を得る。いま補助的に、1の虚数立方根を

（∗10）　$j=(-1+\sqrt{-3})/2$，　$j^2=(-1-\sqrt{-3})/2$

と置く。三根 a, b, c に 1, j, j^2 を割り当てる順序を任意とすれば、a, b, c は、

（∗11）　$a=v-(p/3)w$，　$b=jv-(p/3)j^2w$，　$c=j^2v-(p/3)jw$

と表される。（1, j, j^2 の割り当て方を変えれば、a, b, c の順序が変わるのみ。）

カルダノ公式を再考したのが十八世紀の [8] ラグランジュである。カルダノの根の公式は v と w の定め方が《随意》だったのに対して、それを合理化した。いま a, b, c を三根とし（ただし、その三根は後で定まる《仮定》された数に過ぎない）、1の虚立方根を式（∗10）のように定めるとき、カルダノの v と w は

（∗12）　$v=a+jb+j^2c$，　$w=a+j^2b+jc$

のように《定義》しなければならない。その立方 v^3 と w^3 を作ると、二つの立方の和は 3, 積は 1 となる。v^3 または w^3 を z で表せば、z は必然的に二次方程式

（∗13）　$z^2-3z+1=0$

の二根となる。この補助の二次方程式（ラグランジュの分解式）を解いて、$z=v^3$ 及

び $z=w^3$ を得て、それぞれを立方根に開けば v と w が求められる。この助変数 v, w を用いれば、三根 a, b, c は式（*11）のように表される。

ラグランジュにとっては、1, j, j^2 と v, w との組み合わせが問題となる。試しに a の v, w に共に 1 を割り当てれば、あとの b, c には、必然的に式（*11）のような j, j^2 と v, w の組み合わせしか残らない。このように式（*11）を作るとき、必然的な組み合わせしか生じないことが僥倖であった。三つよりも多くの根を持つ場合は、飛躍的に組み合わせのカズが増えてしまい、困難に直面する。

発見学の立場から言えば、《類推》は新しい事実を導く重要な推進力である。二次方程式では、式（*6）の係数 p は二根の負の和、係数 q は二根の積であることから、根の公式が作られた。$-q=x^2+px$ と置いて右辺を $(x+p/2)^2$ で置き換えようとすれば、$(x+p/2)^2=x^2+px+p^2/4=-q+p^2/4=(-4q+p^2)/4$. これから、根の公式 $x=-p/2\pm\sqrt{(-4q+p^2)/4}$ が出る。

カルダノは、三次方程式の解法の場合に、類推によって、二次方程式の解法で用いられた工夫を二重、三重に用いようとした。そのとき、係数 p は二根どうしの積の和が $ab+ac+bc$ であること（それは $(a+b+c)^2$ を展開するときに生ずる)、また係数 q は三根の積であること（それも $(a+b+c)^3$ の展開で生ずる）を用いて、巧妙に三根の一次結合と結び付けようとした。勿論、二次方程式の場合ほど簡単には行かない。さらに、1 の虚立方根 j, j^2 までも必要になる。最も苦心したのは、一次結合

（*12）　$v=a+jb+j^2c$,　$w=a+j^2b+jc$

と、それぞれの三乗を作ることであった。そこにカルダノの非凡なる創意があった。

こうして類推は、より困難な問題を解くとき最大の武器となる。しかし類推が総てを成功に導くとは限らない。ラグランジュは三次方程式で成功したこの方法が、類推によって、五次の《一般》方程式にも適用できる筈だと考えて様々に試みたが、結果は《不成功》に終わった。それも当然であって、数十年後に、アーベルとガロアが、五次の《一般》方程式に通用する一般的な解法が存在しないことを証明した。

しかしいま、私たちは、十八世紀の末に戻って、方程式の解法を論ずべきであろう。ガウスは[2]『整数論』365 条で、五次方程式は「より低次の方程式に帰着させることは不可能であることを、完全に厳密に証明することができる」と述べながら、自身の五次方程式の不可能性の証明は、生涯を通じて公表しなかった。[3]『史談』29 頁に、未公表の或る発見に関する、ガウスの不公正な態度が紹介されているが、この件の場合はどうか？

§１０．ヴァンデルモンドの試み

[９]ヴァンデルモンドは、[１０] ルヴェーグ（有名な、同名の人とは別人）の研究によれば、ラグランジュとは独立に、特殊な五次方程式の場合に、１の虚数五乗根を用いて成功した。上述のように、一般の五次方程式の場合は代数的に解けない。しかし、特殊な係数を持つ場合にのみ、代数的に解ける！　以下、[２]ガウスの円分論の以前に、ヴァンデルモンドが試行錯誤によって辿り着いた道を歩むことにしよう。

ヴァンデルモンドが取り組んだ「正十一角形の作図」のための方程式は、まず

(*14)　$t^{11}-1=(t-1)(t^{10}+t^9+\cdots+t+1)=0$

と分解され、第一根が $t-1=0$ の根 1 であるのは当然として、残る 10 根は、第二の括弧内を T と置けば

(*15)　$T=t^{10}+t^9+\cdots+t+1=0$

を満たす。ここで T を t^5 で割って、$t+1/t=u$ と置いて書き直すと、

(*16)　$U=u^5+u^4-4u^3-3u^2+3u+1=0$

を得る。課題は今や、この五次方程式（*16）の解析に還元された。

いま $\phi=2\pi/11$, $r=\cos\phi+i\sin\phi$ と置き、さらに（*16）の五つの根を、二つづつに根の和と考えて、

(*17)　$a=r+1/r,\ \ b=r^2+1/r^2,\ \ c=r^3+1/r^3,\ \ d=r^4+1/r^4,$
　　$e=r^5+1/r^5$

と置く。また i を虚数単位 $=\sqrt{-1}$ とし、さらに1 の原始５乗根 h を

(*18)　$h=\cos(2\pi/5)+i\sin(2\pi/5)$

と表す。こうした準備の下、ヴァンデルモンドの分解式（ラグランジュの分解式と実質は同じ）を

(*19)　$V_1=a+hb+h^2d+h^3c+h^4e=a+hb+h^3c+h^2d+h^4e$

と置く。根 a の係数 $h^0=1$ は必然として、h の指数 1, 2, 3, 4 と根 b, c, d, e との組み合わせ方を（*19）のように定めたときにのみ成功するのである。ヴァンデルモンドは恐らく試行錯誤の末に、この特別な順序に辿り着いたのであろう。

（ガウスは根の順序と指数の順序の対応を、§4 の如く正しく把握していたから、迷わずこの点を越えたであろう。）

§１１．ヴァンデルモンドの試み（続）

不思議なことに、分解式 V_1 を５乗すれば式(*21)の第一式のように、仮定された根 a, b, c, d, e とは無関係な数値が得られ、これを５乗根に開いて根を得る。ヴァンデルモンドは、さらに（*19）の V_1 に類似した分解式 V_2, V_3, V_4 をこしらえて、

$$(*20)\quad \begin{cases} V_2=a+hc+h^2b+h^3e+h^4d=a+h^2b+hc+h^4d+h^3e \\ V_3=a+hd+h^2e+h^3b+h^4c=a+h^3b+h^4c+hd+h^2e \\ V_4=a+he+h^2c+h^3d+h^4b=a+h^4b+h^2c+h^3d+he \end{cases}$$

と置く。誠に不思議なことに、これらも同じく５乗すれば、a, b, c, d, e に無関係な

$$(*21)\quad \begin{cases} V_1{}^5=11\cdot(-16-10h+10h^4+25h^2)=11\cdot(-36.225\cdots-i\cdot 4.326\cdots) \\ V_2{}^5=11\cdot(-16-10h^2+10h^3+25h^4)=11\cdot(-8.274\cdots-i\cdot 35.532\cdots) \\ V_3{}^5=11\cdot(-16+10h^2-10h^3+25h)=11\cdot(-8.274\cdots+i\cdot 35.532\cdots) \\ V_4{}^5=11\cdot(-16+10h-10h^4+25h^3)=11\cdot(-36.225\cdots+i\cdot 4.326\cdots) \end{cases}$$

を得る。そこで、（*21）の右辺を数値として、それぞれを５乗根に開けば、

$$(*22)\quad \begin{cases} V_1=\sqrt[5]{11\cdot(-16-10h+10h^4+25h^2)}=2.7287\cdots-i\cdot 1.8851\cdots \\ V_2=\sqrt[5]{11\cdot(-16-10h^2+10h^3+25h^4)}=3.1041\cdots-i\cdot 1.1681\cdots \\ V_3=\sqrt[5]{11\cdot(-16+10h^2-10h^3+25h)}=3.1041\cdots+i\cdot 1.5321\cdots \\ V_4=\sqrt[5]{11\cdot(-16+10h-10h^4+25h^3)}=2.7287\cdots+i\cdot 1.8851\cdots \end{cases}$$

のように、目標とした各 V の値が求まった。

ここで根と係数の関係から、$-1=a+b+c+d+e$ を得る。三次方程式の解法からの類推で、式(＊22)で得られた V_1, V_2, V_3, V_4 に適当に1の原始5乗根 h を掛けた和を作り、-1 を加えた和を作れば、(簡単のため、$\phi=2\pi/11$ と置く)、

$$(*23)\begin{cases} 5a=-1+V_1+V_2+V_3+V_4 = 5\cdot 1.6825\cdots = 5\cdot 2\cos\phi \\ 5b=-1+h^4V_1+h^3V_2+h^2V_3+hV_4=5\cdot 0.8308\cdots = 5\cdot 2\cos 2\phi \\ 5c=-1+h^2V_1+h^4V_2+hV_3+h^3V_4=5\cdot(-0.2846\cdots)=5\cdot 2\cos 3\phi \\ 5d=-1+h^3V_1+hV_2+h^4V_3+h^2V_4=5\cdot(-1.3097\cdots)=5\cdot 2\cos 4\phi \\ 5e=-1+hV_1+h^2V_2+h^3V_3+h^4V_4=5\cdot(-1.9189\cdots)=5\cdot 2\cos 5\phi \end{cases}$$

を得る。我々は、式(＊23)の《からくり》を知っているから、得られた式(＊23)の値が、右辺のように余弦表示できることを、当然だと思うが、さて、ヴァンデルモンドは?

[9], [10]ヴァンデルモンドが、こうした結果をどこまで予想していたか、私には分からない。さらに、ヴァンデルモンドの研究は、ラグランジュとは独立に為されたのであるが、論文提出の前後関係（印刷の前後関係か？）から、後者の名に隠れた。

〔補足〕ヴァンデルモンドが、もしも余弦表示に気付いていたら、数値的に余弦の倍角公式を用いて、検算したかも知れない。$\phi=360°/11=32.7272\cdots°$ と置き、

$$(*24)\begin{cases} a=2\cos\phi=1.68520\cdots, \quad b=2\cos 2\phi=a^2-2=0.83083\cdots \\ c=2\cos 3\phi=a^3-3a=-0.28463\cdots, \\ d=2\cos 4\phi=a^4-4a^2+2=-1.30972\cdots \\ e=2\cos 5\phi=a^5-5a^3+5a=-1.91898\cdots \end{cases}$$

を得る。これらの値は、上の式（＊23）と一致する。また、その和

$$a+b+c+d+e+d=a^5+a^4-4a^3-3a^2+3a=-1$$

は、上の式(＊16)の u^4 の係数と調和する。

§12. p乗根の割り当て

§8で述べたように、また[7] ティニョルによると、《分解式》を作る際、ラグランジュにとって、根と1の虚立方根との組み合わせが限られることが幸いした。三次方程式の3根を a, b, c とすれば、《組み合わせ》は、a に1 を割り当てるのは自然として、次の b に j を割り当てれば、残る c には必然的に j^2 を割り当てざるを得ず、$a\times 1+b\times j+c\times j^2$ が出る。後に残る割り当て方は、$a\times 1+b\times j^2+c\times j$ しかあり得ない。以下、五次方程式の場合は、私の考察である。

ヴァンデルモンドの場合は、1の虚 11 乗根から作られた五つの数値

$$\begin{cases} a=\cos\phi+i\sin\phi, (\phi=2\pi/11), \quad b=\cos 2\phi+i\sin 2\phi, \\ c=\cos 3\phi+i\sin 3\phi, d=\cos 4\phi+i\sin 4\phi, \quad e=\cos 5\phi+i\sin 5\phi \end{cases}$$

を、1の虚 5 乗根 $h=\cos\phi+i\sin\phi, (\phi=2\pi/5)$ と組み合わせて《分解式》を作るとき、a には 1 を、b には h を割り当てるのは良いとして、残りの c, d, e に h^2, h^3, h^4 のどれを割り振るか、$3!=6$ 通りの自由度がある。どの割り当てが《有効》か、一意には決まらない。$c\times h^2+d\times h^3+e\times h^4$ も $c\times h^3+d\times h^4+e\times h^2$ も可能、等々。有効なのは $c\times h^3+d\times h^2+e\times h^4$ と $c\times h^4+d\times h^2+e\times h^3$ の二つだけ

である。 何故これが有効なのだろうか？ヴァンデルモンドの場合は、試行錯誤の末に $a+bh+h^3c+h^2d+h^4e$ と $a+bh+h^4c+h^2d+h^3e$ を選んだのに過ぎない。所で $1=h^0$ だから先頭は 0 として、残る数字の割り振りを、(1 3 2 4) と(1 4 2 3) にする必然性は、何を意味するか？

その回答には、《原始根》という概念が重要な鍵となる。[2] ガウスの原始根なる概念を用いれば、[8]ヴァンデルモンドが試行錯誤の末に与えた指数の順序を、次のように説明できる。今度は法 5 の場合、原始根 2 または原始根 3 を選び、それぞれについての冪乗表を作る。(k の並び方は、意図的に変えた。)

k	1	3	2	4
2^k	2	3	4	1

k	1	3	2	4
2^k	b	c	d	e

k	1	4	2	3
3^k	3	1	4	2

k	1	4	2	3
3^k	c	e	d	b

最初の表で 2^k の欄の数字を、$2\to b, 3\to c, 4\to d, 1\to e$, と読み替えれば、第二の表が出来る。第三と第四の表も同様。アルファベットと指数 k との対応は、上記の $bh+h^3c+h^2d+h^4e$ と密接に結び付く。アルファベットの並び方は、ふだん番号付けにも使われるから、この考えは妥当である。こうして循環小数の周期の分類の原理の考察から、自然にガウスの原始根の概念が形成された、と考えてもよい。

§１３．ガウスの秘密主義

ガウスは (先輩ルジャンドルへの態度と同様)、ヴァンデルモンドの論文を読んだと思われるのに、ヒタ隠しにした。この事情は [10] ルベーグに詳しい。ガウスがヴァンデルモンドの位置解析 (トポロジー) の論文を読んだことは、1802 年 10 月 2 日付けのオルバース宛の手紙からも明らかである。位置解析の記事を載せた同じ雑誌のすぐ近くの頁に、何とヴァンデルモンドの十一次方程式 $t^{11}-1=0$ の論文が載っているではないか！ ガウスがこの論文を読んだ可能性は非常に高いが、秘して語らない。

ヴァンデルモンドが用いた「1 の 11 乗根」！ それは円の分割から得られる有限個の「虚数」である。法 p で考えた (有限個の) 数もまた、1, 2, …, 11 まで数えれば、再び 1 に戻る。全く異なる対象であっても、法 11 で考えた有限個の数と「円分数」とは完全に対応する！ ガウスはここに《密接な対応を読み取った》に違いない。法 11 の数とヴァンデルモンドの十一次方程式の根との関係は、完全に平行している！ そうだ、ヴァンデルモンドの与えた式 (＊19) の指数の割り当ては、必然だったのだ。

そのときガウスに生じた閃き！ その閃きこそは「ザルツブルクの塩」という諺に相応しい。「飽和した塩水は、僅かな振動を加えただけで、結晶になる！」(地名の由来：ザルツは塩、ブルクは城。この地は多くの岩塩鉱を持ち、有名な岩塩の産地として、古くから栄えた。私はウィーンの科学史博物館で、大きな岩塩の塊を見た。)

ガウスは [2] 整数論の第 7 章で、p 等分方程式

(＊25) $(t^p-1)/(t-1)=t^{p-1}+t^{p-2}+\cdots+t+1=0$

を展開し、その根を $t=\cos\phi+i\ \sin\phi$, $\phi=2\pi/p$, と置いた。第 7 章の理論を用いた実例、そのうち特に $p=11$ の場合をガウス自身に代わって示そう。§ 3 の対応表において、指数 e と 2 の乗冪 2^e との対応を見て、e が奇数であるときの 2^e の値を取り出せば 2, 8, 10, 7, 6 である。これらの数を仮に m で表して、それらから作ら

れる $t=\cos m\phi+i\ \sin m\phi$ の値を特に f_m と表せば、f_2, f_8, f_{10}, f_7, f_6 なる 5 つの値が得られる。この五つの値を根とする五次方程式は

(＊26)　$t^5+kt^4-t^3+t^2+\ell t-1=0$

である。ただし k と ℓ は虚の二次数 $k=(-1+\sqrt{-11})/2$ と $\ell=(-1-\sqrt{-11})/2$ を表す。残りの（e が偶数の 2^e の値 4, 5, 9, 3, 1 を n で表す）$t=\cos n\phi+i\sin n\phi$ と表される五つの値 g_4, g_5, g_9, g_3, g_1 を根とする五次方程式は、

(＊27)　$t^5+\ell t^4-t^3+t^2+kt-1=0$

である（係数が入れ替わっていることに注目)。そこで、初めの十次方程式

(＊14)　$T=(t^{11}-1)/(t-1)=t^{10}+t^9+\cdots+t+1=0$

に戻れば、それは二つの五次方程式（＊26）と（＊27）の積に分解される。

この二つの五次方程式はそれぞれ、もはやそれ以上分解されない。

§１４．文献上の難点と私案

私が二十数年前、ガウスの原資料を求めてゲッチンゲンに行った時、（この津田塾大学のシンポジウムで 2003 年から報告して来たような）ガウスのレムニスケート積分の研究を目標にしていた。と言うのは、当時、ガウスの『整数論』については既に研究し尽くされた、と考えていたからである。（その後間もなく、高瀬氏による『整数論』の翻訳が出た。）実は『整数論』執筆以前および執筆中のガウスの手書きの資料は、ゲッチンゲンに豊富に残されていた。滞在日数の限界から、宝の山に踏み込みつつも、整数論関係のノートや紙片を見なかったことを、いまから考えて残念に思う。

当面必要なのは、「ガウスがヴァンデルモンドを何時読んだか？」である。私は [10] ルベーグに基づいて書いて来た。手許の使える資料からは、隔靴掻痒の感がある。

ガウスのゲッチンゲン大学入学は、1795 年 10 月 15 日、そして重要な発見が生じたのは、故郷ブラウンシュヴァイクに帰省していた、翌年 3 月 30 日の早朝である。

幸いにも、その間の事情を示す [11] ダニングトンの『ガウス伝』付録に、「ガウスがゲッチンゲン図書館から借り出した本」という非常に貴重な資料（ダニングトンの調査による）がある。このリストは、2006 年のこのシンポジウムでも紹介した。

大学一年生のガウス青年は、英仏文学にも多大の興味を示して居り、リチャードソンの『クラリッサ』、ルサージュの『ジル・ブラス』などを借り出した。

数学・天文学に関する、1795―96 年冬学期の一覧表（多くはない）は次の通り：

1795 年 10 月 24 日　Lambert, Beiträge zum Gebrauch der Mathematik (3 vol . Berlin, 1765-1772)

10 月 12 日　Memorie della Societa italiana, Vol. Ⅰ.

14 日　LaLande, Astronomie, Vol. Ⅰ.　同月 24 日　Vols. Ⅱ & Ⅲ.

12 月 1 日　Leipziger Magazin zur Naturkunde, (3 Vols. ; Funk, Leske, Hindenburg)

20 日　Miscellanea Taurinenensia, Vols. Ⅰ・Ⅲ.

1796 年 1 月 22 日　Nouvelles Mémoires de l' Academie de Berlin, Ⅰ・Ⅳ (1770-74, Lagrange).

2 月 9 日 Mémoires de l'Academie de Berlin, V ・ VII (1775-77).

24 日 Mémoires de l'Academie de Berlin, (1779-81, 83).

ご覧のように、残念ながら、ヴァンデルモンドの論文の載った、パリの

Mémoire sur la résolution des équations, l' Histoires de l'Academie, 1771.

は、この一覧表には登場しない。それでは、ルベーグの「ガウスはヴァンデルモンドの論文から十一次方程式の根の公式の示唆を得た」という仮説は、この「ガウスが借り出した本」のリストからは、成立しないではないか。

私は推理を重ねる。《借り出しカード》が必要なのは、本を下宿に持ち帰るときであり、指導教授がカードにサインするからカードが残る。借り出さなくとも、ガウスが図書館で論文を読んだ可能性は高い！ 飽和していた《塩水》は、ヴァンデルモンドの十一次方程式の論文を《見る》という刺激だけで、一瞬にして《結晶》した！

今の私は、ただ事実を報告し、それに推理を加えるだけに止めた。

本稿で後回しにした法2の場合、四次剰余の研究（ガウスの「複二次剰余」の研究）に這入れば、必然的に虚数に直面する。ガウスは、「円分体」（虚平面上の円周の等分点）を考えていたのと同じ頃、所謂「ガウスの虚整数」も考えていた。その証拠もある。これらは、また機会を改めて検討しなければなるまい。

文献

［1］杉本敏夫：関とガウスの正十七角形（上）、津田塾大学、数学・計算機科学研究所報、30, 2008年。同（下）、所報、31, 2009年。

［2］C. F. Gauss : Disquisitiones arithmeticae, Gerh. Fleischer, Lipsiae, 1801. 高瀬正仁訳、ガウスの整数論、朝倉書店、1995.

［3］高木貞治、近世数学史談、岩波文庫、1995.

［4］C. F. Gauss : Werke, X-1, Gottingen, 1917. Reprinted by G. Olms, 1981.

［5］杉本敏夫：循環小数のある難題の解決（補）、数学史研究、No. 198, 2008.

［6］A. M. Legendre : Théorie des nombres, Firman Dido Frère, 1830. ルジャンドル、高瀬正仁訳、数の理論（原著の前半）、海鳴社、2007.

［7］J. -P. Tignol : Galois' s theory of algebraic equations, World Publishing Co., 2001. ティニョル、新妻弘訳、代数方程式のガロア理論、共立出版、2005.

［8］J. L. Lagrange : Réflections sur la résolution algébraique des équations, Nouveaux Mémoires de l 'Académie Royale, Berlin, 1770, 134-215; 1771, 138-254.

［9］A.-T.Vandermonde, Mémoire sur la résolution des équations, l ' Histoire de l'Académie, 1771, 365-415.

[10] H. Lebesgue, : L'Oeuvre mathématique de Vandermonde, L' Enseignemant mathématique , Nouv. Ser. 1955, 77-79.

[11] G. Waldo Dunnington : Carl Friedrich Gauss — Titan of science, Hafner, 1955. With additional material by J. Gray and Fritz-Egbert Dohse, The Mathematical Association of America, 2004.