ガウスと虚数平面

杉本敏夫

§1．まえおき

前回［1］ガウスへの試論で、円分論の証明のための《円分数》を論じた。今回の主題である《四乗剰余》の理論では、「高等数論の一般理論の確立のため、《数の領域》の殆ど無限な拡大が、必然的に要請される」と述べた。論文［2］の第一部(1825)と第二部(1831)前半まで、実整数の範囲に止まり、第二部後半に到って、ガウスは初めて《数の領域の拡大》を迫られた。しかしずっと以前に、［3］学位論文「代数学の基本定理の新しい証明」(1799)の中でも、既に虚数平面を縦横に活用していた。《数学における発見》の観点から、再考を試みたい。

§2．随伴の概念

［4］ガウスの整数論(1801) の証明方法で、オイラーに基づく「随伴」概念（77 条）が重要である。素数 p の法で、$p-1$ 個の剰余 $C = \{1, 2, \cdots, p-1\}$ のうち、$a \cdot b \equiv 1 \pmod{p}$ となる二数 a と b を随伴と呼ぶ。話を具体化するために、法 13 で、2 を原始根とする『乗冪の表』を示そう。

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

ここでは 2 と 7, 4 と 10, 8 と 5, 3 と 9, 6 と 11 の 5 組は随伴である。残る 1 と 12 は随伴でなく、$1 \cdot 12 = 12 \equiv -1 \pmod{13}$ となる。そこで、凡ての剰余の積は $\equiv -1 \pmod{13}$ となり、一般の素数 p の場合、ウィルソンの定理「$1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \equiv -1 \pmod{p}$」が証明された（76～77 条）。

法 p で b が平方剰余であるとは、$a \cdot a \equiv b \pmod{p}$ を満たす a の存在を言う。もしも合同式を満たす a が存在しないときは、非剰余と言う。上の乗冪表が予め計算されていれば、表で e が偶数である 2^e 即ち 4, 3, 12, 9, 10, 1 が平方剰余である。ガウスはルジャンドル記号を排し、独自のガウス記号を用いる。131 条の記号：$+3R13$ を「法 13 で +3 は平方剰余である」と定め、$8N13$ を「法 13 で 8 は平方非剰余である」と定める。私はそれに追加して(ガウスは使わないが)、$a \cdot a \equiv 1 \pmod{p}$ となる数 a を自己随伴と呼べば都合が良いと考える。$12 \cdot 12 = 144 \equiv 1 \pmod{13}$ だから 12 が自己随伴である。ガウスは予め、上のような乗冪の表を多数計算して置いて、定理を確かめたであろう。

§ 3．平方剰余の第一補充定理

ガウスによる第一、第二補充定理の証明を概観する。彼はルジャンドル記号を用いず、多くの場合分けをし、必然的に証明が長い。原文は［4］高瀬氏訳、［5］マーゼルの独訳を参照し、ガウスに特徴的な証明の仕方を例示する。

便宜のため、数 a が数 b で割れる、を $b \mid a$ で、その否定を $b \nmid a$ で表す。証明の根拠は 106 条「オイラーの規準」で、「素数 $p=2m+1$ に対して $p \nmid a$ なる a は、法 p で $a^m \equiv +1$ ならば平方剰余であり、$a^m \equiv -1$ ならば平方非剰余である」と言う。108 条、第一補充定理は、「-1 は、素数 $p=4m+1$ の平方剰余であり、$p=4m+3$ の平方非剰余である」と言う。その第一証明は「オイラーの規準」に基づき、現代の教科書[1 0]と変わらない。興味あるのは 109 条の第二証明で、「随伴」の概念を用い、110 条の第三証明はウィルソンの定理に基づく。1, 2, …, $p-1$ の中には $(p-1)/2$ 個の平方剰余と同数の平方非剰余を含む。よって、非剰余の個数は p が $4m+1$ 型のときは偶数、$4m+3$ 型のときは奇数となり、積 $1 \cdot 2 \cdot \cdots \cdot (p-1) \equiv -1$ は、前の型のとき剰余、後の型のとき非剰余となる。(ルジャンドル記号を用いない証明としては優れている。)

§ 4．ガウスの態度

ここで、ガウスの立場というよりも彼の態度について、一言しよう。その『整数論』の序文に言う（私なりに言い直し、要約する)。「1795 年の初め、私が初めてこの種の研究に着手した頃、この領域で既に成し遂げられた事柄について何も知らず、…私は素晴らしい定理 [所謂、平方剰余の第一補充定理] に出会った。」…「初めの四つの章の事柄の大半は、他の幾何学者によって … とっくに解決済みの事柄であった。」しかし、それらの「初期の研究成果を省かず、(私の) 新しい方法を用いて … 十分適切な仕方で説明」しようと意図した。

ガウスが合同式記号 ≡ を発明したことは、高く評価される。その点については、私も異論はない。しかし、それのみならず、初めの四つの章において、オイラー・ラグランジュ等、先駆者の業績を「十分適切な仕方で」まとめ直した点が、『整数論』の功績なのである。私はそのように考える。

§ 5．平方剰余の第二補充定理

第二補充定理は、ルジャンドル記号ならば、$(2/p)=(-1)^{(p^2-1)/8}$ と簡明である。ガウス（整数論 112～113 条）はルジャンドル記号を拒否し、多くの「場合分け」に応じて文章で記述する。有理整数の場合も、数 2 の平方的性質は、既に法 8 で考える必要に迫られていた。

その前に、ガウスが述べなかった事実を補充する。それは、$4m+1$ 型ではあっても、$8m+1$ 型ではない場合である。§ 2の、法 13 の乗冪表を見よ。ここ

では、$2^6=12\equiv-1$ (mod. 13) であるから、第一補充定理は成立する。しかし、$12\div4=3$ であって、$2^3=8$ となり、8 は法 13 で -1 と合同にならない。従って、法 13 は第二補充定理についての不適切な例である。ガウスが考えたような $8m+1$ 型の場合、法 17 の場合などを考えることが要請される。

数学史研究の方法について、一言する。著者（ガウス）が論及した場合のみならず、著者が述べなかった事例の扱いである。著者は積極的に或る事実を主張する意図を持つので、それに適合する事例を提出するのは当然である。《反例》は、或る主張を反駁するときにしか挙げないから、著者が触れようとしないのは当然である。だが、数学史を研究する者（ここでは私）は、書かれておらない《物事の裏側》にも目を配らなければなるまい。当面の事例として、法 13 が不適切な例であり、法 17 が適例なのである。

§6．平方剰余の第二補充定理（弐）

第二補充定理のガウス自身の説明に戻る。数 2 の平方的性質は、$8n+1$ 型の法 p で考える必要に迫られた。記述短縮のため、法 8 で素数 p を四分割し、剰余 1, 3, 5, 7 に応じて p_1, p_3, p_5, p_7 と記述する。またガウス記号を用いて、法 p で a が剰余ならば $a\,R\,p$, 非剰余ならば $a\,N\,p$ と表す。定理は
(i) $+2\,Np_3, -2\,Rp_3$, (ii) $+2\,Rp_7, -2\,Np_7$, (iii) $\pm2\,Np_5$, (iv) $\pm2\,Rp_1$
を主張する。このうち初めの三つは次のように証明される。

便宜のため、一般の整数を k で表す。ガウスは一つの例として、(i) $+2\,Np_3$ のような否定的命題のほうが証明し易い、と言う。前回報告[1]の§4で紹介した「100 以下の素数 p についての平方剰余の表」を見れば、+2 を平方剰余とする素数は、7,17, 23, 31, 41, 47, 71, 73, 79, 89, 97 であり、これらは $8n\pm1$ 型であり、この中には $8n\pm3$ 型は含まれない。もしも、限界 100 を超えた或る素数 $t_3=8n+3$ で、$t_3\mid a^2-2$ が成立したと仮定すれば、$u_3<t_3$ なる u_3 でも $u_3\mid a^2-2$ の成立が容易に示せる。これを繰り返せば、次々に「より小さい」$8n+3$ 型の素数 $q<100$ でも成立することになって、上で確認した 7, …, 97 以外の素数 q でも定理は成立する。これは矛盾である。この証明は、k_3 型または k_5 型の合成数が、同型の数を含むことを根拠にしている。

§7．平方剰余の第二補充定理（参）

（整数論 114～115 条）以上の証明法は (iii) の場合までは通用する。しかし最後の (iv). $\pm2\,Rp_1$ の証明には通用せず、別個の証明法が望まれる。

第一証明　a が法 $8n+1$ の原始根なるとき、先に $a^{4n}\equiv-1$ (mod. $8n+1$) が示された。これを $(a^{2n}+1)^2\equiv2a^{2n}$ (mod. $8n+1$) 或いは $(a^{2n}-1)^2\equiv-2a^{2n}$ (mod. $8n+1$) と書き直せば、$2a^{2n}$ と $-2a^{2n}$ が $8n+1$ の剰余となり、従って平

方数 a^{2n} を除いた数 $+2$ と -2 が法 $8n+1$ の剰余となる。

第二証明　$4n+1$ の形の素なる法に対して-1 は常に平方剰余である。そこで f を $ff\equiv-1$ なる数（勿論、実数である）とすれば、4個の数 $+z$, $-z$, $+fz$, $-fz$ （それらは互いに非合同である）の四乗は互いに合同である。それらは同じく、合同式 $x^4\equiv z^4$ を満たす。（いまこの段階では f は或る実数を表わす。f は後の四乗剰余理論において、単位虚数 $\sqrt{-1}$ に変身する。）

§8．四乗剰余の登場

ガウスが言うように、法が (iv) p_1 型の素数の場合は、これまでの証明方法は通用せず、全く独自の手法が要求される。a を法 $8n+1$ の原始根とするとき、-1 は或る四乗数と合同になる。例えば法 17 のとき、$2^4=16\equiv-1\ (\mathrm{mod.}\ 17)$ である。彼の第二補充定理の証明は、かなり難解である。その上さらに、証明のために有理整数の整数論の枠内で、既に「四乗剰余」に直面したのである。

$8n+1$ よりも小さな全ての四乗剰余（0 を除外）の個数は $=2n$，即ち偶数である。（例えば法 17 の四乗剰余は 13, 16($\equiv-1$), 4, 1 の4つ。）さらに、簡単に分かることだが、r が法 $8n+1$ の四乗剰余なら、逆数 $1/r\ (\mathrm{mod.}\ 8n+1)$ も同じく四乗剰余である（$1/4\equiv13$, $1/1\equiv1$, $1/16\equiv16$）。よって四乗剰余の全体は、先に平方剰余が配分されたときと同様の仕方で、幾つかの類に配分される。

このことを用いて（そうすれば証明は全てガウス好みに計算的に進行する）、$g^4\equiv-1$ として、h を $1/g\ (\mathrm{mod.}\ 8n+1)$ の値とするとき、$gh\equiv1$ により、

$$(g\pm h)^2=g^2\pm2gh+h^2\equiv g^2+h^2\pm2$$

となる。ところが、$g^4\equiv-1$ だから、$-h^2\equiv g^4h^2\equiv g^2$ となる。よって、結局、$g^2+h^2\equiv0\ (\mathrm{mod.}\ 8n+1)$ となり、$(g\pm h)^2\equiv\pm2\ (\mathrm{mod.}\ 8n+1)$ を得る。こうして $+2$ 及び -2 が、法 $8n+1$ の「平方剰余」であることが示された。

§9．四乗剰余の探求

画期的な「四乗剰余」の論文[2]は、全集で二部併せて 84 頁に及ぶ大作である。その第一部(1825)、第二部(1831)前半までは、「整数論」(1801)の延長上、実整数の範囲で書かれた。ここでは、[5]マーゼルによる独逸語訳、[6] H. J. S. Smith の要約、高瀬氏の試訳を参照し、要点を再録する。ガウスは（当時、全く新奇な理論を導入するため）多くの数値例（その分量も膨大）を掲げ、一歩づつ進めた。本稿では丁寧な引用を諦め、簡略な紹介に止める。

「四乗剰余」の用語。biquadatische を直訳すれば「複二次」であり、「quadatische の自乗」の意味が良く出る。だが、慣用の「四乗」に従う。

3条、p が $4n+3$ 型の場合、例えば、法 11 の場合、$x^4\equiv a(\mathrm{mod.}\ p)$ の解は、$x=c$ と $x=-c$ の二つに限られ、これ以上の新たな展開はない。$a=3$ では、

$4^4=256\equiv 3$ (mod. 11), $7^4=2401\equiv 3$ (mod. 11) で、4 と 7 が解であり、両者は $7\equiv -4$ (mod. 11) なる関係で結ばれている。

4条以下は、「専ら $8n+1$ 型の場合に限る」としている。この型の法は、17, 41, 73, 89, 97 などである。法 17 を例にして、原始根 3 の乗冪表を掲げよう。

e	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3^e	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

三種類（内一つを便宜、二分する)、具体例では、$p=17$ の場合、$A(1, 4, 13, 16)$, $B(3, 5, 12, 14)$, $C(2, 8, 9, 15)$, $D(6, 7, 10, 11)$ に四分類する。A は四乗剰余（下線付)、D は四乗非剰余(下点付)、B と C は平方剰余かつ四乗非剰余である。

この四つの組は相互に行き来が可能である。即ち、A 組の数 (1, 4, 13, 16) に $h=3$ を掛ければ $(3, 12, 39, 48)\equiv(3, 12, 5, 14)$: B の数になり、A の組の数に $h^2=9$ を掛ければ $(9, 36, 117, 144)\equiv(9, 2, 15, 8)$: C の数になり、A の組の数に $h^3=27\equiv 10$ を掛ければ $(10, 40, 130, 160)\equiv(10, 6, 11, 7)$: D の数になる。このように四つの組は、相互に緊密な関係を持って結ばれている。

§１０．四乗剰余の探求（続）

この調子で「四乗剰余」論文を追えば、ガウス論文のように長くなる。従って、[6]スミスの報文を参照して、重要な定理を（説明は省略して）列挙する。６条～１２条。特に９条。いま、$4n+1$ 型の法 p の原始根を f とすれば（f はこの段階では実数)、法 p と素である数 a は、法 p で、(i) 1, (ii) f, (iii) -1, (iv) f^3 に合同なる四つの集まりに分けられており、各 $(p-1)/4$ 個の数から成る。(i) の組は $x^4\equiv a$(mod. p) の解から成り、法 p の四乗剰余である。(iii) の組は四乗非剰余でしかも平方剰余である。(ii) と (iv) の組は共に平方非剰余である。

第一論文１３条で、法 $p=8n+1$ に対する数 2 の四乗的性質を徹底的に検討する。この型の素数 p は、二つの平方数の和に分解されて、$p=a^2+b^2$ ($a\equiv 1$, mod. 4 ; $b\equiv af$, mod. p)となる。$b/2$ が $4n, 4n+1, 4n+2, 4n+3$ に属するのに従って、2 は第一、二、三、四に属する。例えば、法 17 で 4, 8, 12, 16 は第一の組、5, 9, 13, 1 は第二、6, 10, 14, 2 は第三、7, 11, 15, 3 は第四の組に属する。

16 条～19 条で、$8n+1$ 型の素数を法とするときの、四つの組への分類を実行する。α と α' が「集まり A」の不定数を表すとき、方程式 $\alpha+1=\alpha'$ が「異なる何通りの様式で満たされるのか」を記号（００）で示す。ガウスの記述を忠実に再現しよう。組 A の数のすぐ次の数が組 A に属するとき(００), 組 A の数のすぐ次の数が組 B に属するとき(０１), …。組 D の数のすぐ次の数が組 C に属するとき(３２), 等々。このガウスの記号法は、新奇なる理論を「何とかして他人に理解させようとする意欲」の現われではあるが、それらの記号が新理論の紹介のために、果たして成功しているか否かは、異論もあろう。

現在は、ルジャンドル記号を四次剰余理論に適合させた［6］スミス記号がある。それは$[p/q]_4=\pm 1$ と表わされ、符号によって$+1$ なら法 q の下で p が四次剰余、-1 なら非剰余を表す。ガウスはルジャンドル流の記号を意図的に排除するので、句による表現が多くなった。

ガウスは、左側の配列図式を、$p=17$ の場合、右側の数値配列で示した。

(00), (01), (02), (03)	0, 2, 1, 0
(10), (11), (12), (13)	2, 0, 1, 1
(20), (21), (22), (23)	1, 1, 1, 1
(30), (31), (32), (33)	0, 1, 1, 2

ガウスの執念は良い！　だがスミス記号［p/q]$_4$ 等のルジャンドル式記号に馴れた者には、「数値配列が法則を示す」ガウス式記号には着いて行けない。

§１１．四乗剰余の探求（三）

ガウスは 22 条で重要な宣言をする。「ここまで展開した理論は、前著[整数論]で扱った、方程式 $x^p-1=0$ の理論（所謂、円分論）と混在させることはせず、純粋に『整数論様式』の枠内で展開する」と。ガウスの気持ちを推測すれば、同じく虚数平面上の点ではあっても、円分論は「ノルム１の円周上に並ぶ虚数」を扱った。四乗剰余理論では、虚数平面全体に規則的に散在する《虚なる点》全部を対象とする。後で、私が描いた虚数平面上の網目の例を示そう。

四乗剰余の研究は、1831 年に出た[２]第二論文に続く。前半は、まだ有理整数の範囲に止まり、焦点は、「数 +2 を、前論文で分けた四つの集まり A, B, C, D のどれに算入すべきか」の決定である。後半で、多くの数値例を元に、実整数の世界から虚数の世界に飛躍する。ガウスは、「虚空に漂う精霊の影を捉えようとして頭が一杯になっている最中…」と言った[７]。しかし、天才と雖も虚空から真理を掴んだのではなく、多くの数値例を土台にしている。

先に、整数論的な虚数単位 $ff\equiv -1\,(\mathrm{mod.}\,p)$ となる数 f（それは勿論、実数であった）を考えた。しかし、いま、≡記号を＝記号に置き換え、$-1\,(\mathrm{mod.}\,p)$ から $(\mathrm{mod.}\,p)$を取り去れば、$ff=-1$ となり、$f=\sqrt{-1}$ と考えることは自然ではないか。私は、私の頭の中を語っている。「ガウスがどのように考えたか」というガウスの頭の中は、勿論永久に分からない。私は、発見学の立場から、凡そ、このようなヒラメキがあっただろう、と推測を廻らした。

ガウスは実はそれよりずっと以前に、虚数の世界にドップリと浸かっていたのだ。それは次節以下に回し、ガウスが第二論文で、どのように論を進めたか、見ておこう。ここでもまた[６] スミスの報文を参照する。有理(実)整数は、新しい種に分けられる。第二論文の 30 条で、ガウスは次のように述べる。

「私は 1805 年以来、熟考を開始したが、［四乗剰余を研究する場として］整

点線と２と４を結ぶ実線は、交互に円内に入り、交互に出て行くから、Fig.4（記号 P, C 等は無視）のように、円内で両者は必ず交わる筈である。（互い違いに並ぶ二種類の曲線が円内に這入り、互い違いに円内から出るから必ず交点があるという論法が、後に批判される。）実例では４つの交点を得、この交点こそ方程式(＊6)の根である。私の計算では、例題（＊6)の場合、根は次の四点である。

第一、第二　$-1.45 \pm 0.765\, i = (1.639\ ,\ \pm \angle 152.19°\ )$

第三、第四　$+1.45 \pm 1.272\, i = (1.929\ ,\ \pm \angle 41.27°\ )$

Fig.2.

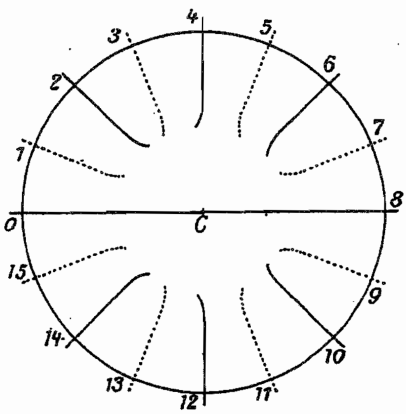
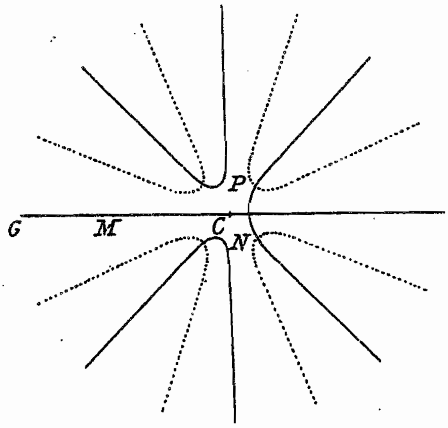


Fig.4.



§ １４．代数学の基本定理（続）

私が試みた計算の結果を示す。ガウスの□付き番号を、○付き数字とする。

上掲の Fig.2 は、証明の眼目である「十分大きな半径 R の円（私のは仮に半径 4）を描き、その円と U=0 との丁度 2m 個の交点と、V=0 との丁度 2m 個の交点が存在する」に相当する。私の図は、実軸に対して上半のみを示した。

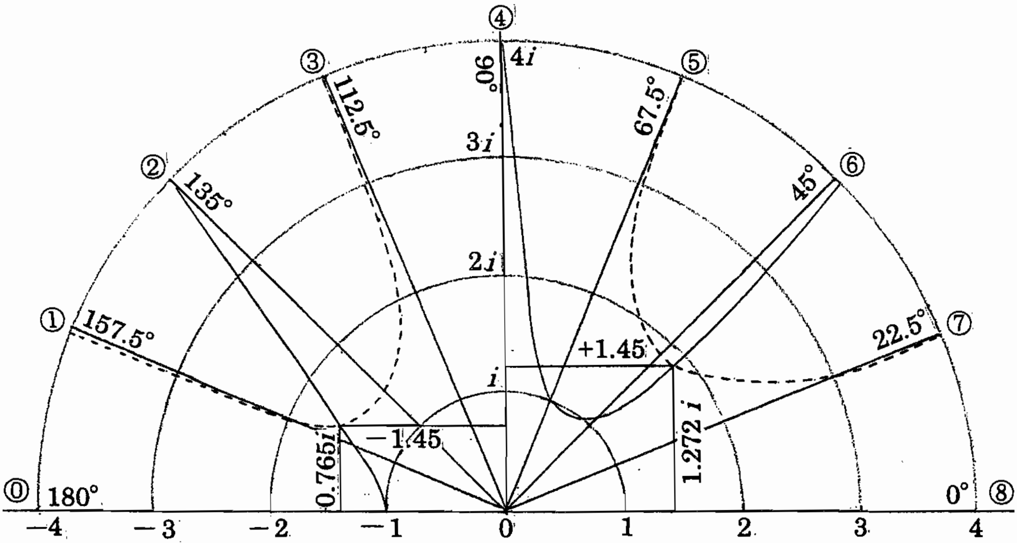
	⓪	①	②	③	④	⑤	⑥	⑦	⑧
r=4	—	159. 90°	137. 25°	114. 00°	89. 37°	65. 48°	43. 67°	22. 41°	—
r=3	—	159. 65°	139. 25°	115. 60°	88. 57°	63. 06°	42. 90°	23. 56°	—
r=2	—	158. 85°	145. 66°	122. 40°	85. 66°	68. 07°	44. 71°	34. 85°	—
r=1	—	—	180°	—	67. 65°	—	43. 67°	—	—

左端から順に、半径４の円上に① から ⑦ まで７個の点が並び、夫々等分点

⓪ 180°　①157.5°　②135°　③112.5°　④90°　⑤67.5°　⑥45°　⑦22.5°

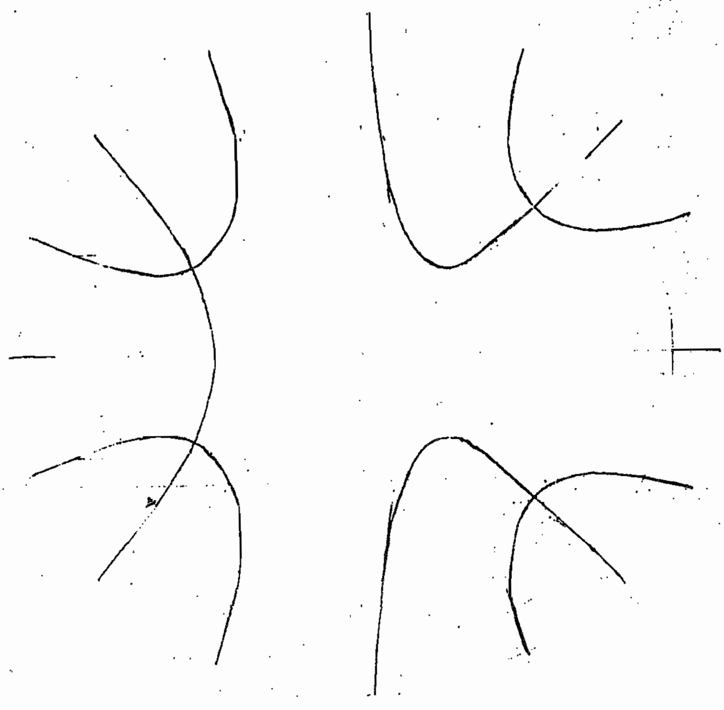
とごく僅かズレている。ここを起点として内側の曲線を描けば、ガウスの Fig. 4 が描ける筈が、事実は違う！　困ったことに、出来上がった私の図はガウスの Fig. 4 と全く異なる！　一体どうしたことか？　何度計算をやり直しても、最後に得られたグラフは次の通りである。ガウスの Fig. 4 と私の図を比べてみれば、実線と点線の交点が、似ても似つかない位置にある。私の計算は正しい。

その一方、計算の名手ガウスが《計算間違いを冒さない》ことは有名だ。



§15．代数学の基本定理（参）

話は以外な結末を迎えた。前回、私が1980年代に、ゲッチンゲンで大量のガウスの手稿をコピーした、と述べた。コピーの幾つかはこのシンポジウムでも紹介した。手稿が余りに大量なため、帰国後も未整理の束が残った。それを探すうち、何とガウス自身のグラフがあった！　縦 20 センチ、横 21 センチの大きな図なので、縮小して掲げよう。(紙片番号 Math20, Nr. 20 ウ)



ガウスはやはり正しく計算していたのだ！ しかも勿論、私の図と一致した！
（論文の Fig.2 と Fig.4 は、印刷屋に渡す際、誤って左右を反転したのか？）
ガウスの証明は位相幾何の観点から欠陥（点線と実線の交点の存在の確実性への疑問）が指摘され、後にオストロフスキー(1920)が証明を補充した。しかし、１８世紀末、ガウスの時代の証明としては、完全であったと言えよう。

§１６．虚数の加減乗除

数学における《虚数使用・虚数平面の正当性》は、ガウスの《代数方程式の根の存在証明》と《数論への虚数の導入》に起源を持つ。今回、ガウスによる《虚数平面の導入とその自在なる活用》を考察した。代数方程式のように、虚数平面上の連続した点の加減乗除はガウスも手馴れていた。しかし四乗剰余で扱われるのは、碁盤目の飛び飛びの位置にある点と点相互の加減乗除である。これらの点に四則を施せば、果たして、元の碁盤目の点に戻れるか？

ガウスが達成したのは、現代の言葉では、「有理数体に虚数単位 $i=\sqrt{-1}$ を添加した数体に於ける整数論」である。そこでは確かに元の点群に戻れる。次に考察すべきは、「１の虚立方根 $h=(-1+\sqrt{-3})/2$ を添加した数体に於ける整数論」である。さすがはガウス、「四乗剰余の理論」の第二論文の 30 条、虚の量 $i=\sqrt{-1}$ を添加した数の領域の考察を告げた処で、次を注記した。

> 「事のついでにここではせめて、この様に定められた領域は、四次剰余の理論のために特に適切であることに留意すると良い。同様に、立方剰余の理論は $a+bh$ の形の数の考察を基礎に、その土台の上に築かねばならない。ここで h は、方程式 $h^3-1=0$ の虚根、例えば $h=-1/2+(\sqrt{3}/2)\cdot i$ である。同様に一層高次の冪剰余の理論では、他の虚量の導入が要請される。」

ガウスはこう述べたが、「四乗剰余の理論」の第三論文も[９]「立方剰余の理論」も未発表で、彼の到達点は分からない。立方剰余では斜めの線の交叉点にある点相互の計算を扱う。四則演算の後に、果たして同一の点群に戻れるか？

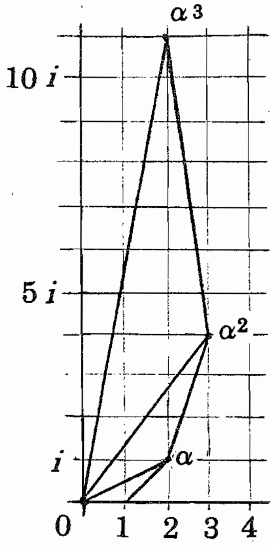
§１７．網目の幾何学

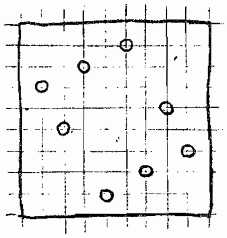
網目の幾何学の作図は、横軸に実数の整数点、縦軸に虚数の整数点を取り、網目を描く。加減算で同種の数を得る。この網目上に一点 $\alpha=2+i$ を取り、次々に乗冪を作る。$\alpha^2=(2+i)^2=3+4i$, $\alpha^3=(2+i)^3=2+11i$ となる。0, 1, α が頂点；0, α, α^2 が頂点；0, α^2, α^3 が頂点の各三角形は、相互に相似である（左上）。

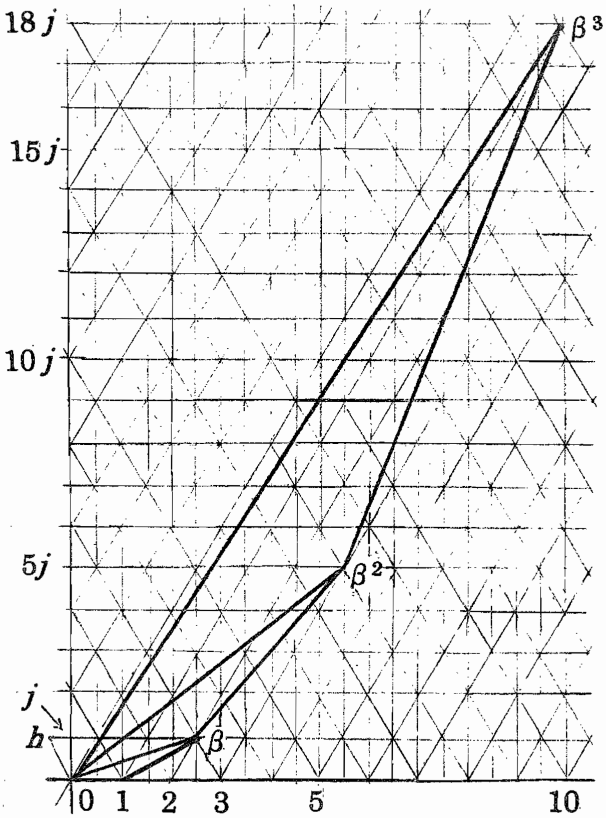
次にこれと違う網目を作る。虚軸方向に $j=(\sqrt{3}/2)\cdot i$ を取り、$h=-1/2+j$ を基点として、正三角形の網目を作る。加減算で同種の数を得る。$\beta=3+h$ を取り、次々に乗冪を作る。0, 1, β を頂点とする三角形、$\beta^2=(3+h)^2=5.5+5j$ を求め、0, β, β^2 が頂点の三角形、$\beta^3=(3+h)^3=10+18j$ を求め、0, β^2, β^3

が頂点の各三角形は、相互に相似である(右)。

ガウスがこの図を描いたか否か分からない。私が二十数年前に、彼の図のコピーを求めたとき、整数論関係の紙片は探さなかったので、何ともいえない。







§１８．網目の幾何学（続）

ガウスは晩年パズル『八人の女王(Achatköniginnen)』に凝った。8×8 のチェス盤に八人のチェスの駒女王(Königin)を並べ、女王相互の《利き》(将棋の飛車と角行を併せ持つ）が回避される条件で考える。ガウスは数例解き、結果を方眼紙に綺麗に描いた(一例 Math21-(50)オを左下に示す)。私は紙片のコピーを持ち帰り、試した。これから類推すれば、ガウスの網目の図は存在するだろう。

話題を元に戻そう。乗法によって作られた三角形の頂点は、再び網目の点と一致するだろうか？　そもそも虚整数に加法・減法を施したとき、それは網目の上の平行移動に過ぎないから寸法に伸び縮じみはなく、同じ網目の点に移るのは当然である。重要な論点は、乗法（それは拡大･縮小、回転を含む）を施したときにも、果たして同じ網目のいずれかの点と一致するだろうか？

「代数学の基本定理」のように連続した虚数平面の上で計算すれば、図形が

数論の領域を拡大しなければならない。四乗剰余に関する諸定理は、虚の量の領域にまで拡げ、制限なしに、$a+bi$ という数が対象となるようにして、初めて際立った簡明さと真正な美しさを持ち、光を放つ。i は虚の量$\sqrt{-1}$ を表し、a, b は$-\infty$ と $+\infty$ の間のあらゆる不定実整数を表す。我々は、このような数を複素整数と呼ぶ。実数は複素数ではないが、複素数の仲間と見做される。」

これが、ガウスによる、虚数使用の正当性を主張する宣言である。私は、この宣言が 1830 年の論文で成されたという事実は、勿論認める。しかし、ガウスがずっと以前、1799 年の[3]学位論文で、すでに縦横に虚数を駆使していた事実を重視したい。本稿の目的はガウスの複素整数論ではなく、むしろガウスが「虚数」とどのように向き合ったかを論ずるところにある。

「補記」有理整数論では、素因数分解の際、合成数は $-1, 2, 3, 5$ なる各素数の乗冪の積に分解した。複素整数論では素因数分解の際、3 は分解されず、他の有理素数は $-1=i^2$, $2=(1+i)\cdot(1-i)$, $5=(2+i)\cdot(2-i)$ のように素因子分解される。実はこのとき、$2=(-1-i)\cdot(-1+i)$ のような分解も可能であり、数 2 の因子は四つある。その内どれを代表とすればよいか？ この代表選びのため、第二論文 36 条にプライマリ primary, Primär が出てくる。従来「準素」と訳された。しかし、「素 prim」を遡り「更に根源的に素なるもの」の意味だから不適当である。既に多くの漢字が使われたので漢和辞典を詳査し、私案として「幹」を当てようと考えた。Primary prim は「幹素」となる。

§１２．ガウスの略歴

後半の話題として、所謂[３]「代数学の基本定理」の証明を取り上げる。例えば、[７]「近世数学史談」３節に、ガウスの略歴が載っている。

1777 年　ブラウンシュワイヒに於いて出生。
1795-98 年　ゲッチンゲン大学に在学。
1799 年　ヘルムステット大学に於いて　ドクトル試験通過。
学位論文は代数方程式の根の存在の証明。
1799-1807 年　生地ブラウンシュワイヒに居住（処士時代）　[下略]
[処士とは民間に居て、仕官（就職）しない人]
1807 年　ゲッチンゲン大学教授兼天文台長
[下略]

§１３．代数学の基本定理

以下、1799 年の[３]学位論文「一変数ノ凡テノ代数的有理方程式ハ一次又ハ二次ノ実因子ニ分解可能デアル事ノ新シイ証明」を話題とする。代数方程式の根の存在を証明するこの論文の内容は、多くの著書に紹介されている。ここで

は一例として、[8] ファン・デル・ヴェルデン「代数学の歴史」による。

前半は、ガウスに先行する証明 [ダランベール、オイラー、フォントネス、ラグランジュ] への批判で、後半がガウス自身による「新証明」である。

方程式はガウス自身の記号で

(＊1)　$X = x^m + A\,x^{m-1} + B\,x^{m-2} + \cdots + M = 0$

あるいは $X=0$ と書ける。「代数学の基本定理」は、「実または複素数の凡ての多項式 X が、複素数の範囲で一次因子の積に分解される」ことを主張する。

[7] 数学史談 27 頁によると、ガウスは、1799 年、虚数が未公認な時代に居たので、「多項式は《一次又は二次の因数》に分解される」と言わざるを得なかった[27 頁]。複素数の公認に至る一般的な歴史はそれ自身興味深いが、他の機会に譲り、ガウスに戻ろう。[3] の証明の粗ら筋は次の通り。

実の既約二次因子は、二つの共役な複素根(ガウスは実際には使っている)

(＊2)　$r(\cos\phi \pm i\sin\phi)$

に分解される。従って、共役な二つの一次因子を根とする方程式は

(＊3)　$x^2 - 2xr\cos\phi + r^2 \ (r>0)$

と書くことができる。元の方程式 (＊1) $X=0$ に根(＊2)のうち一つを代入し、実部と虚部に分離すれば、r と ϕ についての一対の実方程式

(＊4)　$U = r^m\cos m\phi + A\,r^{m-1}\cos(m-1)\phi + \cdots + Lr\cos\phi + M = 0$

(＊5)　$V = r^m\sin m\phi + A\,r^{m-1}\sin(m-1)\phi + \cdots + Lr\sin\phi = 0$

を得る。(この二つの曲線の実例は、ガウス自身の証明に用いられた。) 証明の要点は、原点を中心として半径の大きな円を描く。この円周上で、(＊4)と(＊5)とは、半径 r が大きいので、r^{m-1} 以下の低次の項は値が小さく、無視できる。図は、半径の大きな円周上で、(＊4)の点と(＊5)の点が交互に並ぶ。その点を起点として、円の半径を次第に縮めて行けば、$U=0$ と $V=0$ の各 $m-1$ 次以下の項も有効に働き出して、本来の曲線の形状に近づく。ガウスの実例は、

(＊6)　$X = x^4 - 2x^2 + 3x + 10 = 0$

であったから、(＊4) と (＊5) は

(＊7)　$r^4\cos 4\phi - 2r^2\cos 2\phi + 3r\cos\phi + 10 = 0$

(＊8)　$r^4\sin 4\phi - 2r^2\sin 2\phi + 3r\sin\phi = 0$

となる。Fig. 2 は (具体例に即して) 半径 $r=4$ の大円の円周上、(＊7) の最上位の項のみの方程式 $r^4\cos 4\phi = 0$, 及び (＊8) の最上位の項のみの方程式 $r^4\sin 4\phi = 0$ を満たす点が、ほぼ等間隔で交互に並ぶ。半径を縮めれば、ガウスの Fig. 2, 曲線先端の曲がり方が見えてくる。更に半径を縮めれば、ガウスの Fig. 4, 曲線本来の姿が現れる。ガウスの証明の核心は、複素平面上に (＊7) の余弦曲線(実線)と (＊8)の正弦曲線(点線)を別々に描いたとき、実線と点線は円周上で互い違いに並ぶから、実線と点線は円内で必ず交差する。1 と 3 を結ぶ

連続的に相似拡大されることは、直感的に当然と思われる。しかし、いま問題とする「有理整数に虚整数 i または h を添加した整数域」の場合には、実際に飛び飛びに並んだ点が、加・減・乗の三つの算法（特に乗法）に対して閉じている。 ガウスがどう考えただろうか？——宿題として残したい。恐らく彼が「i から生成される網目の左上図」を描いただろうとは、想像がつく。しかし、私の描いた「h から生成される網目の右図」を描いたかどうかは、分からない。

$j=(\sqrt{3}/2)\cdot i$ を添加した数域の立方剰余の研究は、後にアイゼンシュタイン(1844) が完成した。これらについては、［６］スミスを参照。

網目の幾何学は、［１０］高木著では「格子点の幾何学」である。その目的は格子点を用いた連分数の研究にあり、正方形の格子点のみならず平行四辺形の格子点も扱われている。「無理数 ω の有理数近似」が主な話題である。

§１９．定理の発見

発見とは、従来、誰も気付かなかった事実を新たに見出すことである。有名な少年ガウスの発見は、1+2+3+ … +18+19+20 の和を求める問題が提出されたとき、他の少年は頭から正直に 1+2+3+ … と足して行き、時間も掛り、誤りも多かった。一方、ガウスは末尾に注目し、… +18+19+20 が 20, 19, 18, … と逆向きに減っていく事実に注目した。 1+20＝21, 2+19＝21, 3+18＝21, … が 10 組あるから、答えの 210 は直ちに得られる。世に、同じ発見が繰り返し生ずるのは、このように「違った角度から眺め直す」という鍵に由来する。

今回扱った二つの補助定理の発見を、跡付けてみよう。§２の法 13 の乗冪表と§９の法 17 の乗冪表に加えて、法 11 の乗冪表を追加する。

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

第一補助定理は、$a\cdot a\equiv-1\ (\mathrm{mod}.\ p)$ となる数 a が存在するような法 p を尋ねた。法 11 では不可であり、法 13 と法 17 では成立することが、根拠となる。その分かれ目は、$(p-1)/2$ が偶数になるような e の場合という条件であった。法 11 では $(11-1)/2=5$ は奇数、$(13-1)/2=6$ と $(17-1)/2=8$ は共に偶数で、後の二つの場合には成立する。現代ではルジャンドル記号も用い、洒落た表現になっている。しかし昔、定理が発見され、証明された当時（ガウスの整数論執筆の頃）は、実際に或る式が成立するか・しないかを尋ねて、多くの例を見比べる中で得られた。虚空に漂う影ではなく、現実の数値を求めた。

第二補助定理は、$a\cdot a\equiv2\ (\mathrm{mod}.\ p)$ となる数 a が存在する法 p を尋ねた。法 11 と法 13 では不可であり、法 17 では成立することが、根拠となった。法 11 と法 13 の場合と法 17 の場合を区別する条件に《鍵》があり、初めは言葉で述べた。後には $(p^2-1)/8$ が偶数となる条件に整理され、$(11^2-1)/8=15$

は奇数、$(13^2-1)/8=21$ は奇数で、共に成立しない。しかし、$(17^2-1)/8=36$ は偶数であって、法 17 の場合には成立する。

現代の我々には、-1 の肩に来る指数が、前者では $(p-1)/2$ のとき、後者では $(p^2-1)/8$ のとき、と言う数式の形の定理として表される。二つの補助定理の発見と、その証明が求められた当時に於いては、恐らく、上に述べたような、数値に基づいた《もっと原始的な》、言葉による表現が前面に出る形式であった。

いま見た三つの場合の区別は、法とする奇素数が $4n+1$, $4n+3$, $8n+1$ の《どの型》に属するか、という事実に依存する。現代の我々は、完成後の綺麗な定理を見る。開拓者は、足場も残る仕事場で、《あれか・これか》の苦心をした。

発見の心理で面白いのは、第一発見に続く、再発見であろう。第二発見者は、《成る程、そんな見方もあったのか》と唸らせるような機智を思いつく。普通は第一発見のみ尊重されるが、第二発見のほうが、価値が高い場合がしばしば生じる。事実、第二発見の内容が、事柄の本質を衝いている場合が多い。

文献について、多大の便宜を計って頂いた 高瀬正仁氏 に感謝を捧げる。

文　献

［1］杉本敏夫：ガウスの整数論の形成への試論、津田塾大学、数学・計算機科学研究所報、32 号, 2011 年。183-196.

［2］C. F. Gauss：Theoria residorum biquadraticorum. commentatio prima. 1828. commentatio secunda. 1831. Gauss：Werke, Band 2.

［3］C. F. Gauss：Demonstratio nova theorematis omnem functionem algebraicam rationalem integram unius variabilis in factres reales primi vel secundi gradus resolvi posse. 1799. Gauss：Werke, Band 3.

［4］C. F. Gauss：Disquisitiones arithmeticae, Gerh. Fleischer, Lipsiae, 1801. Gauss：Werke, Band 1. ［2］,［3］,［4］, Repr. Olms, 1973.
高瀬正仁訳、ガウスの整数論、朝倉書店、1995.

［5］H. Maser：Untersuchungen über höhere Arithmetik von C. F. Gauss, 1889. Repr. Chersea, 1965.

［6］J.H.S.Smith：Theory of numbers, 1894. Repr. Chersea, 1965.

［7］高木貞治：近世数学史談、岩波文庫、1995. [最旧版、1931.]

［8］B. L. van der Waerden: A history of algebra, 1985.
加藤明史訳：代数学の歴史、現代数学社、1994.

［9］C. F. Gauss：立方剰余。Werke, X-1, Göttingen, 1917. Repr. Olms, 1973.

［10］高木貞治：初等整数論講義、共立出版、初版、1931, 第2版、1971.