書　評

ガウスの数論世界をゆく
—正多角形の作図から相互法則・数論幾何へ—

栗原将人 著，数学書房，2017 年

東北大学大学院理学研究科
山崎　隆雄

飛行機に乗ると富士山が見えることがある．その姿は実に美しい．歩いて頂上まで登ってもその姿は見ることができないし，その山容や地形を正確に把握することも難しい．しかし当然ながら，飛行機から見るよりも歩いて登る方がずっと心に残る体験である．

本書の目指すところをたとえていうと，ガウスの開拓した数論という山を，飛行機から見下ろすのではなく，自分の足で歩いて登ってみるということにある．ガウスから二百年，数論は爆発的に発展したし，著者はその発展を知り尽くした第一線の研究者であるから，現代的な高い視点を活かして名所を効率よく案内することもできたであろう．しかし，本書ではその対極にある道を選んだ．ガウスが未踏の世界を開拓せんと悪戦苦闘していたときの，その悪戦苦闘ぶりを追体験することが本書の主眼であると言ってもよい．予備知識がほとんど不要という意味では高校生でも読めるのだが，議論と計算をたどるには熱い意欲と分厚い計算用紙が必要である．定理を効率よく習得する以上のものが，そこにはある．

本書の主題はガウス周期である．これはガウスが著書『数論研究』の中で導入したもので，幅広い応用を持つ．本書では（素数 $p = 17$ に対する八次の）ガウス周期を求めることで正十七角形の作図可能性が示されている．これと関連するが，円分方程式 $x^n - 1 = 0$ が冪根で解けるという定理（これもガウスの結果である）や，クンマーの円分体論でもガウス周期が有効に使われた（[2, 3] を参照）．しかし，なんといっても重要な応用は相互法則で，本書でも多くのページが割かれている．ガウスの与えた多くの平方剰余の相互法則の証明のうち，ガウス周期を用いるものは没後の１８６３年に発表された遺稿にある．これは第七証明と呼ばれているが，実はこれは『数論研究』執筆中の１７９６年には得られていて，年代から言えば三番目の証明になるそうである．そればかりか，ふつう第六証明と呼ばれている１８１８年の論文にある証明は，この「第七証明」から「足場を取り払って」書き直したものだという．

本書はガウスの原典（『数論研究』，上記の遺稿，相互法則に関する論文，手紙など）を素材としており，歴史的な記述も多く，それが魅力の一つとなっている．上では本書を読むのに予備知識はほとんどいらないと述べたが，そもそもガウスの時代には群論もガロア理論も線形代数もなかったのだから，その種の予備知識が不要なのは素材に沿った自然な手法ともいえる．しかし，実際に読み進めていくと，そこかしこで群論やガロア理論でよく使われるアイデアに出会うことになる．これは後世の視点からの色眼鏡でこ

うなったのではなく，逆にガウス以降の数学者がガウスの数学を丹念に研究することで「現代代数学の一般論」が整備されていったという，その事情が正当に反映されたものと言えるだろう．

ここからは数学的内容に踏み込んで本書の内容を見てみよう．一章と二章は準備である．一章では正多角形の作図可能性が，二章は有限体の基礎事項（原始根の存在など）が論じらている．最後の六章はガウス以降の数論の発展について述べたもので，ヴェイユ予想や志村・谷山・ヴェイユ予想などが紹介されている．三〜五章が本書の主要部である．

ガウス周期の定義は簡単である．奇素数 p を固定して 1 の原始 p 乗根 ζ で $\mathbb{Q}$ 上生成される体 $\mathbb{Q}(\zeta)$ を考える．$p-1$ の約数 d と $a \in \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z},\ a \neq 0$ に対し，$\mathbb{Q}(\zeta)$ の元

$$[a]_d := \sum_{\beta \in (\mathbb{F}_p^\times)^d} \zeta^{a\beta} \in \mathbb{Q}(\zeta)$$

を d 次ガウス周期と呼ぶ．三章ではこの定義のあとで，ガウス周期の積をガウス周期の一次結合で表す公式（積公式）が証明される．積公式は強力で，これによって素数 p が与えられればガウス周期を計算できてしまう．本書の中心にある定理は任意の p に対して $d = 2, 4$ の場合に $[a]_d$ が満たす最小多項式を決定したもので，これを「d 次ガウス周期の基本定理」と呼んでいる．その重要性は，$d = 2, 4$ の場合からそれぞれ平方剰余と四乗剰余の相互法則が導かれる，という点に顕著に表れる．これが四，五章で詳細に解説される．以下，その事情を（ガウスの時代にはなかった言葉を用いて）説明してみよう．

$[a]_d$ の値は a の $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^d$ における類のみで定まる．$\mathbb{F}_p^\times$ は位数 $p-1$ の巡回群であるから（原始根の存在），その生成元 g を一つ固定すれば，$[a]_d$ の値は d 個の元からなる集合 $B_d := \{[1]_d, [g]_d, [g^2]_d, \ldots, [g^{d-1}]_d\}$ に収まる．B_d で張られる $\mathbb{Q}(\zeta)$ の $\mathbb{Q}$-線型部分空間を K_d としよう．「積公式」によって K_d は $\mathbb{Q}$ の d 次拡大体となることが分かり，B_d は K_d の $\mathbb{Q}$ 上の基底となる．これはただの基底ではなく正規基底でもある．すなわち，$K_d/\mathbb{Q}$ はガロア拡大で，$B_d = \{\sigma([1]_d) \mid \sigma \in \mathrm{Gal}(K_d/\mathbb{Q})\}$ が成立する．より詳しく書くと次のようになる．$\mathbb{Q}(\zeta)/\mathbb{Q}$ のガロア群 G は $\mathbb{F}_p^\times$ と同型である（円分多項式の既約性）．$a \in \mathbb{F}_p^\times$ に対応する元 $\sigma_a \in G$ は $\sigma_a(\zeta) = \zeta^a$ で定まる．σ_a の $G/G^d = \mathrm{Gal}(K_d/\mathbb{Q})$ における類を $\sigma_a^{(d)}$ と書けば，ガウス周期の定義により $[a]_d = \sigma_a^{(d)}([1]_d)$ となっている．こうして三つの集合の間の全単射 $(\mathbb{F}_p^\times)/(\mathbb{F}_p^\times)^d \cong \mathrm{Gal}(K_d/\mathbb{Q}) \cong B_d$ が構成される．この全単射から次の事実が従う：p と異なる奇素数 ℓ に対し，三条件 $\ell \in (\mathbb{F}_p^\times)^d$, $\sigma_\ell^{(d)} = \mathrm{id}_{K_d}$, $[\ell]_d = [1]_d$ は同値である．これが相互法則への応用において基礎となる．第一の条件は ℓ が p の d 乗剰余であることを意味する．第二の条件を ℓ における剰余拡大のガロア群で見ることで，p が ℓ の d 乗剰余であるかどうかを論じることができる．（これは代数的整数論を用いて平方剰余の相互法則を証明するときの標準的な方法である．）それと同等のことは，第三の条件を用いてガウス周期の言葉で論ずることもできる．そこで鍵となるのが $[a]_d$ の最小多項式（すなわち体 K_d）を記述する「ガウス周期の基本定理」である．（なお，ここまでの記述において括弧つきで述べた「原始根の存在」「積公式」「円分多項式の既約性」はすべてガウスの結果であることに注意したい．また，「第二の条件」のところで用いた有限

体の拡大体の理論にあたるものも，ガウスが「第七証明」の遺稿の中で考察していた.）

四章では二次の基本定理に三つの異なる証明を与えた上で，平方剰余の相互法則を導出している．三つの証明のうち第一のものは，有限体上の二次曲線の有理点を勘定することによるもので，五章ではこの方法を発展させることで四次の基本定理を証明している．五章の残りの部分では，基本定理から四乗剰余の相互法則への道のりが説明される．この部分は圧巻で，ほとんど鬼気迫るものがある．四次ガウス周期の基本定理はガウスの遺稿に暗示されていたものの，明示的には書かれていないそうである．また，四乗剰余の相互法則についてもガウスは証明を書き残さなかったそうであるが，著者は推測し考えたこととしてそれを再構築している．（アイゼンシュタインの証明とほぼ同じだそうである.）

数学セミナーの記事 [1] は本書の研究余滴とでもいうべきもので，ぜひ併読をお勧めしたい．（本稿でも同記事を大いに参考にした.）最後に [1] から一文を引用しておこう．

> ガウスの論文からは，ただ純粋に，整数の性質を調べたい，という気持ちが伝わってくると私は思った．整数論はこうでなければならない（たとえば，ある種のことと結びついたことだけが意味がある，など）といったような教条的なこととは遠く離れて，端的に言って，おもしろいと思うことを，とことん調べて行きたい，という気持ちである．

本書を読んだ感想はこれに相似している．ガウスの数学世界の面白さ，素晴らしさを読者に伝えたいという筆者の純粋な情熱が，本書の端々からほとばしっているように感じた．

参考文献

[1] 栗原将人，「ガウスと相互法則 (I), (II)」数学セミナー，2017 年 7, 8 月号.

[2] 原田耕一郎，「群の発見」岩波書店，2001 年.

[3] ニコラ ブルバキ（村田全・清水達雄・杉浦光夫訳)，「ブルバキ数学史（上・下)」ちくま学芸文庫，2006 年.