『数学セミナー』2019年11月号「高校数学ではじめる整数論」

連載●第 8 回

ガウス整数環　付録

谷口 隆◎神戸大学大学院理学研究科

※ 式番号は本誌 2019 年 11 月号の連載と通しで振っています.

◎——1　ユークリッドの補題について

環 $\mathcal{S}=\{a+b\sqrt{-5}\mid a,b\in\mathbb{Z}\}$ では，ユークリッドの補題に相当する命題は成り立ちません．言い換えると，次が成り立ちます.

命題 9　次をみたす $\alpha,\beta,\gamma\in\mathcal{S}$ が存在する.「γ は $\mathcal{S}$ の既約元であり，γ は積 $\alpha\beta$ の約元であるが，γ は α,β いずれの約元でもない.」　□

以下，このような α,β,γ の具体例を挙げることを目標にします.

まず，$\mathcal{S}$ における倍元・約元・ノルム・単元・既約元を，ガウス整数環のときとまったく同じように定義します．$\alpha=a+b\sqrt{-5}\in\mathcal{S}$ について，その共役複素数 $\overline{\alpha}=a-b\sqrt{-5}$ も $\mathcal{S}$ の元です．この α のノルムは $\mathrm{N}(\alpha)=\alpha\overline{\alpha}=a^2+5b^2$ です．$\mathrm{N}(\alpha)$ は 0 以上の整数で，$\mathrm{N}(\alpha)=0$ となるのは $\alpha=0$ のときに限ります．$\alpha,\beta\in\mathcal{S}$ とすると，$\mathrm{N}(\alpha\beta)=\mathrm{N}(\alpha)\mathrm{N}(\beta)$ が成り立つことも，ガウス整数環のときと同じです．したがって，命題 4 と同じ方法で，次が証明できます.

命題 10　$u\in\mathcal{S}$ が単元である必要十分条件は $\mathrm{N}(u)=1$ である.　□

ここから，$\mathcal{S}$ の単元は ±1 の 2 個であることが分かります．$\gamma\in\mathcal{S}$ が $\mathcal{S}$ の既約元であるとは，γ の約元が $1,\gamma$ の単元倍のみ (具体的には，$\pm1,\pm\gamma$ のみ) であることをいいます.

命題 11　2 は $\mathcal{S}$ の既約元である.　□

証明　$\alpha \in \mathcal{S}$ を 2 の約元とする．$2 = \alpha\beta$ となる $\beta \in \mathcal{S}$ が存在する．α, β の一方が単元であることを示せばよい．両辺のノルムを取ると，$4 = \mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$ である．$\mathrm{N}(\alpha)$, $\mathrm{N}(\beta)$ は共に非負の整数だから，$\mathrm{N}(\alpha)$ は $1, 2, 4$ のいずれかである．$\mathrm{N}(\alpha) = 2$ であるとすると，$\alpha = a + b\sqrt{-5}$ とすれば $a^2 + 5b^2 = 2$ であるが，これをみたす整数 a, b は存在しない．したがって $\mathrm{N}(\alpha)$ は $1, 4$ のいずれかである．$\mathrm{N}(\alpha) = 1$ ならば，命題 10 より α は単元である．$\mathrm{N}(\alpha) = 4$ ならば $\mathrm{N}(\beta) = 1$ だから β は単元である．■

これで，命題 9 の α, β, γ の具体例を挙げることができます．$6 \in \mathcal{S}$ の 2 通りの分解

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}) \tag{4}$$

に注目します．この式から，$2 \in \mathcal{S}$ は，$1 + \sqrt{-5}, 1 - \sqrt{-5} \in \mathcal{S}$ の積の約元です．一方，

$$\frac{1 + \sqrt{-5}}{2} = \frac{1}{2} + \frac{1}{2}\sqrt{-5} \notin \mathcal{S}, \qquad \frac{1 - \sqrt{-5}}{2} = \frac{1}{2} - \frac{1}{2}\sqrt{-5} \notin \mathcal{S}$$

だから，2 は $1 \pm \sqrt{-5}$ のいずれの約元でもありません．つまり，$\gamma = 2$, $\alpha = 1 + \sqrt{-5}$, $\beta = 1 - \sqrt{-5}$ が命題 9 の具体例になります．

ちなみに本誌 11 月号では，ガウス整数環 $\mathcal{R}$ でユークリッドの補題に相当する命題が成り立つことを示しましたが，$\mathcal{S}$ で同じ証明をたどろうとすると，命題 7 がうまくいきません．具体的には，証明の 5-6 行目のところが，

$$\left|\frac{\alpha}{\beta} - \gamma\right|^2 = (s - m)^2 + 5(t - n)^2 \leqq \left(\frac{1}{2}\right)^2 + 5\left(\frac{1}{2}\right)^2 = \frac{3}{2}$$

となってしまって，$\left|\dfrac{\alpha}{\beta} - \gamma\right| < 1$ が示せないのです．

注　命題 11 と同じ証明で，$3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ はすべて $\mathcal{S}$ の既約元であることが証明できます．したがって，命題 9 の具体例の γ として，これらのどれを取ることも可能です．またこのことから，(4) は $\mathcal{S}$ においては「既約元への分解が順序と単元倍を除いて一通りである」とはいえないことの実例を与えていることにもなります．

◎——2　定理 2 の別証明

11 月号本誌では，定理 2『$p \equiv 1 \pmod 4$ のとき，$p = x^2 + y^2$ となる整数 x, y が存在する』を，ガウス整数環を使って証明しました．ここでは，それ以外の証明を 3 つ紹介します．はじめの 2 つは命題 3 を使うものです．最後は命題 3 に拠らない証明です．以下では，p は必ず $p \equiv 1 \pmod 4$ となる素数を表すものとします．

2.1　「降下法」による証明

この「降下法」は一般的な呼び名ではないのですが，数を順々に減らしていくことで最終的な目的に到達する方法を仮にそう呼ぶことにします．大まかに喩えれば，数学的帰納法を逆向きにしたような感じのもので，数学の証明でときどき使われます．まず，次の命題を証明します．

命題 12　m を $1 < m < p$ となる正の整数とし，$x^2 + y^2 = pm$ は整数解 x, y を持つとする．このとき，$0 < r < m$ となる整数 r で，$x^2 + y^2 = pr$ が整数解 x, y を持つようなものが存在する．　□

証明　$x^2 + y^2 = pm$ の整数解 x, y を取る．整数 a, b を，$a \equiv x \pmod m$, $b \equiv y \pmod m$ であって $|a| \leqq \dfrac{m}{2}$, $|b| \leqq \dfrac{m}{2}$ をみたすようにとる．$x^2+y^2 \equiv 0 \pmod m$ だから $a^2+b^2 \equiv 0 \pmod m$ である．つまり，$a^2+b^2 = rm$ となる整数 r が存在する．

$$rm = a^2 + b^2 \leqq \frac{m^2}{4} + \frac{m^2}{4} = \frac{m^2}{2}$$

だから，$r \leqq \dfrac{m}{2} < m$ である．$r = 0$ であるとすると，$a = b = 0$ となり，x, y は共に m の倍数になる．よって $x^2 + y^2$ は m^2 の倍数となるから，これと $x^2 + y^2 = pm$ より，p は m の倍数である．つまり m は p の約数となるが，$1 < m < p$ で p は素数なので，これはありえない．したがって $r \neq 0$ である．よって $0 < r < m$ である．

$x^2 + y^2 = pr$ が整数解 x, y を持つことを示せば，証明が完了する．

$$rpm^2 = rm \cdot pm = (a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2 \tag{5}$$

を考える．$a \equiv x, b \equiv y \pmod m$ より $ay - bx \equiv 0 \pmod m$ である．よって $(ay - bx)^2$ は m^2 の倍数である．よって (5) から，$(ax + by)^2$ も m^2 の倍数である．素因数分解の一意性から，$ax + by$ は m の倍数である．

以上から，$ax + by = mc$, $ay - bx = md$ となる整数 c, d が存在する．(5) より $c^2 + d^2 = pr$ である．　■

この命題を使い,「降下法」によって定理 2 を証明します.

証明　命題 3 より，$n^2 + 1 = pk$ となるような，整数 n, k が存在する．ここで，n を p で割った余りを s とすると，$s^2 + 1 \equiv n^2 + 1 \equiv 0 \pmod p$ だから，$s^2 + 1 = pm$ となる整数 m が存在する．$0 \leqq s \leqq p - 1$ より $0 < m < p$ である．$x^2 + y^2 = pm$ には整数解 $(x, y) = (s, 1)$ が存在する．$m = 1$ ならば定理 2 が示されているので，$m > 1$ とする．命題 12 より，m より小さな正の整数 r で，$x^2 + y^2 = pr$ が整数解を持つようなものが存在する．$r \leqq m - 1$ である．$r = 1$ ならば定理 2 が示されている．$r > 1$ ならば同じことを繰り返すと，毎回 1 以上小さくなるので，有限回の繰り返しの後，必ず 1 になって操作が止まる．よって定理 2 が成立する．　■

2.2　鳩の巣原理による証明

2 つ目の証明です．やはり命題 3 を使いますが，鳩の巣原理をうまく使った，短い証明です.

証明　$[\sqrt{p}]$ で，$\sqrt{p}$ を超えない最大の整数を表す．$\sqrt{p}$ は整数でないので，$\sqrt{p} - 1 < [\sqrt{p}] < \sqrt{p}$ である．命題 3 が成り立つ n，つまり $n^2 + 1 \equiv 0 \pmod p$ となる整数 n を取る．

整数 a, b を $0 \leqq a, b \leqq [\sqrt{p}]$ となるように動かしたときの (a, b) の組の総数は $([\sqrt{p}] + 1)^2$ 個である．

$$([\sqrt{p}] + 1)^2 > (\sqrt{p})^2 = p$$

なので，このような (a, b) の組は p 個より多い．$a + bn$ を p で割ると余りは p 通りなので，鳩の巣原理により，この中の異なる二つの組 (a_1, b_1), (a_2, b_2) であって，$a_1 + b_1 n \equiv a_2 + b_2 n \pmod p$ となるものが存在する．

$a = a_1 - a_2$, $b = b_1 - b_2$ とおくと，$(a,b) \neq (0,0)$ であり，$a + bn \equiv 0 \pmod{p}$ である．また，$|a| \leqq [\sqrt{p}]$, $|b| \leqq [\sqrt{p}]$ である．

mod p の合同計算で，

$$a^2 + b^2 \equiv a^2 - b^2n^2 \equiv (a - bn)(a + bn) \equiv 0 \pmod{p}$$

だから，$a^2 + b^2$ は p の倍数である．また，

$$a^2 + b^2 \leqq 2[\sqrt{p}]^2 < 2p$$

である．よって $a^2 + b^2$ は 0 か p のいずれかだが，$(a,b) \neq (0,0)$ なので $a^2 + b^2 = p$ である． ■

2.3 ザギエによる巧妙な証明

最後に取り上げる証明は，命題 3 を使わない，きわめて巧妙な証明です．ザギエという数学者によって考案されました．これは問題形式にします．考えてみてください．

用語を二つ定義しておきます．S を集合とし，$f\colon S \to S$ を S から S 自身への写像とします．S の元 x が f による固定点であるとは，$f(x) = x$ であることをいいます．また，f が S 上の対合であるとは，f の二度の合成 $f \circ f$ が S 上の恒等写像であること，つまりすべての $x \in S$ について $f(f(x)) = x$ であることをいいます．

問 1 S を有限集合とし，f を S 上の対合とする．S の元の個数を n とし，S の f による固定点の個数を m とすると，$n - m$ は偶数である．

問 2 有限集合 S を

$$S = \{(x,y,z) \mid x,y,z \text{は正の整数で } x^2 + 4yz = p \text{ をみたす}\}$$

で定める．S 上の関数 f, g を

$$f(x,y,z) = \begin{cases} (x + 2z, z, y - x - z) & x < y - z \text{ のとき} \\ (2y - x, y, x - y + z) & y - z < x < 2y \text{ のとき} \\ (x - 2y, x - y + z, y) & 2y < x \text{ のとき} \end{cases}$$

と $g(x,y,z) = (x,z,y)$ で定める．($(x,y,z) \in S$ ならば $x \neq y - z$, $x \neq 2y$ であることに注意．)

(1) $(x,y,z) \in S$ ならば $f(x,y,z) \in S$ である．つまり，$f\colon S \to S$ が定まる．
(2) f は S 上の対合である．
(3) S の f による固定点はただ一つである．したがって問 1 より，S は奇数個の元からなる．
(4) $(x,y,z) \in S$ ならば $g(x,y,z) \in S$ で，g も S 上の対合である．
(5) S の g による固定点が存在する．
(6) $a^2 + b^2 = p$ となる整数 a, b が存在する．

[たにぐち たかし]
[絵／森脇かみん]