ラボ探検 A (2023 年後期)

1 環とは

環とは大雑把に言えば, 二つの演算「和」と「 積」が入った集合のことです. 例えば, 整数全体 $\mathbb{Z}$, 実数全体 $\mathbb{R}$, 複素数全体 $\mathbb{C}$ などが環の例です. 他には, 2×2 型の行列全体

$$M_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;\middle|\; a, b, c, d \in \mathbb{R} \right\}$$

も行列の足し算, 掛け算で環の構造を持ちます. 環の詳細は文献 [2], [4] を参考にしてください. 理学部の授業では, 学部 3 年生の代数学 A で扱います. このラボ探検では, 環の例である「ガウス整数環」について紹介します. ガウス整数環のより詳細な話は, 文献 [1, 3, 5] を見てください.

2 ガウス整数環

$\mathbb{C}$ の部分集合

$$R = \{a + bi \mid a, b \in \mathbb{Z}\}$$

を考えます. これに, 足し算と掛け算を次で入れます.

$$(a + bi) + (c + di) := (a + c) + (b + d)i, \quad (a + bi) \cdot (c + di) := (ac - bd) + (ad + bc)i,$$

この演算は複素数と同じものです. この演算で, R は環になり, これを**ガウス整数環** と呼びます.

ガウス整数環の基本事項をみていきます. まず, 写像

$$N : R \to \mathbb{Z} \;\; (a + bi \mapsto a^2 + b^2)$$

を R の**ノルム**と呼びます. 例えば, $\alpha = 1 + 2i$ だと,

$$N(\alpha) = 1^2 + 2^2 = 5.$$

ノルムの重要な性質として, $\alpha, \beta \in R$ のとき,

$$N(\alpha\beta) = N(\alpha)N(\beta) \qquad (1)$$

が成り立ちます.

問題 1 等式 (1) を証明せよ.

定義 1
α, β $(\alpha \neq 0)$ に対して,

$$\alpha \mid \beta \overset{\text{def}}{\iff} \beta = \alpha\gamma\text{を満たす}\ \gamma \in R\ \text{がある.}$$

このとき, α は β の約数と言う. 特に 1 の約数を単数と言う.

例えば, $5 = (1+2i)(1-2i)$ より, $1+2i \mid 5$. また $1 = i \cdot (-i)$ より, i は単数だと分かります.

問題 2 次を示せ.

$$\alpha\text{は単数} \iff N(\alpha) = 1 \iff \alpha = \pm 1,\ \pm i$$

問題 3 R で $\alpha \mid \beta$ ならば, $\mathbb{Z}$ で $N(\alpha) \mid N(\beta)$ が成り立つことを示せ.

定義 2
$\pi \in R$ $(\pi \neq 0, \text{単数})$ を取る.

$$\pi\text{がガウス素数} \iff \pi\text{の約数は, 単数または}\ \pi\ \text{と同伴になる}$$

※ 1　α が β と同伴とは, $\alpha = \beta \times (\text{単数})$ となること.

※ 2　ガウス素数の定義は, 通常の素数の定義が,

$$p\ \text{が}\ \mathbb{Z}\ \text{の素数} \overset{\text{def}}{\iff} p\ \text{の約数は}\ \pm 1,\ \pm p$$

であることとの類似になっている.

ガウス素数の判定には次の定理をよく用います.

定理 1
$\pi \in R$ に対して,

$$N(\pi)\ \text{が素数} \Rightarrow \pi\text{はガウス素数}$$

[**証明**]
$p = N(\pi)$ (p :素数) とする. 問題 2 より, π は 0 でも, 単数でもない. $\alpha \mid \pi$ とすると,

$$N(\alpha) \mid N(\pi) = p.$$

$N(\alpha) \geqq 0$ かつ p は素数だから, $N(\alpha)$ は 1 または p.

(i) $N(\alpha) = 1$ のとき, 問題 2 から α は単数.

(ii) $N(\alpha) = p$ のとき, $\alpha \mid \pi$ より $\pi = \alpha\beta$ となる $\beta \in R$ がある.

$$p = N(\pi) = N(\alpha)N(\beta) = pN(\beta)$$

より $N(\beta) = 1$. よって β は単数になる. 従って α は π と同伴になる.

以上より, π はガウス素数である.

□

定理 1 の使い方を確認しておきます.

$$N(1+i) = 1^2 + 1^2 = 2, \quad N(2+i) = 2^2 + 1^2 = 5, \quad N(3+2i) = 3^2 + 2^2 = 13,$$

より, $1+i$, $2+i$, $3+2i$ は全てガウス素数である. 一方, 定理 1 の逆は成立しない. 例えば, $N(3) = 9$ で素数ではないが, 3 は R の素数である.

問題 4 3 が R の素数であることを示せ.

整数の世界では, $30 = 2 \times 3 \times 5$ のように, 整数は素数の積で表せました. これと同じように, ガウス整数環の元はガウス素数の積で表せます.

定理 2

R の 0 でも, 単数でもない元は, ガウス素数の積で表せ, さらに表し方は次の意味で一意的. α が次のように 2 通りのガウス素数の積で表せたとする.

$$\alpha = \pi_1\pi_2 \cdots \pi_s = \gamma_1\gamma_2 \cdots \gamma_t \qquad (\pi_i, \gamma_j : \text{ガウスの素数})$$

このとき, $s = t$ で, 順番を入れ替えて, π_i と γ_i $(i = 1, ..., s)$ が同伴にできる.

例えば, $\alpha = 1 + 3i$ とすると,

$$\alpha = (1+i)(2+i) \qquad (2)$$

と分解され, また $1+i$, $2+i$ はガウス素数だったので, (2) が α の R での素因数分解になります.

問題 5 π をガウス素数とし, $\alpha, \beta \in R$ とする. 定理 2 を利用して次を証明せよ.

(1) $\pi \mid \alpha\beta$ ならば, $\pi \mid \alpha$ または $\pi \mid \beta$.

(2) $N(\pi)$ は素数または (素数)^2.

通常の素数はガウス整数環で次のように素因数分解されます.

定理 3

(1) $p = 2$ のとき,

$$2 = (\text{単数}) \times (1+i)^2$$

ここで, $1+i$ がガウス素数.

(2) $p \equiv 1 \pmod 4$ のとき,

$$p = \pi\bar{\pi}$$

と素因数分解される. ここで, $\bar{\pi}$ は π の複素共役で, π と $\bar{\pi}$ は同伴でないガウス素数.

(3) $p \equiv 3 \pmod 4$ のとき, p はガウス素数.

[証明]
参考文献 [1] の定理 5.45 を参照のこと. □

例えば, $3, 7, 11$ はガウス素数になります. 一方で, $5, 13, 17$ はガウス素数ではなく, それぞれ

$$5 = (1+2i)(1-2i), \quad 13 = (2+3i)(2-3i), \quad 17 = (1+4i)(1-4i)$$

と R 上ではさらに素因数分解されます.

問題 5 $14 + 4i$ をガウス素数の積で表せ.

問題 6 $x^2 + y^2 = 221$ を満たす自然数の組 (x, y) を一つ求めよ.

3 ガウス整数環の応用

最後にガウス整数環の応用を一つ紹介します. 原始ピタゴラストリプルとは次を満たす自然数の組 (x, y, z) です.

$$x^2 + y^2 = z^2, \quad \gcd(x, y) = 1, \quad y \text{ は偶数}$$

例えば, $(3, 4, 5)$, $(5, 12, 13)$ などが原始ピタゴラストリプルとなります.

定理 4
原始ピタゴラストリプル (x, y, z) に対して, 次を満たす自然数の組 (a, b) が存在する.

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2.$$

例えば, $(x, y, z) = (3, 4, 5)$ ならば $(a, b) = (2, 1)$, $(x, y, z) = (5, 12, 13)$ ならば $(a, b) = (3, 2)$,

として (a, b) が取れます.

[証明のスケッチ]
(x, y, z) の仮定から

$$z^2 = x^2 + y^2 = (x + iy)(x - iy) \qquad (3)$$

となる. このとき, $x + iy$, $x - iy$ は R で互いに素になる (問題). よって, (3) と素因数分解の一意性から

$$x + iy = (a + bi)^2 \qquad (4)$$

を満たす自然数 a, b が取れる. よって $x = a^2 - b^2$ であり, $y = 2ab$ で, さらに

$$z^2 = x^2 + y^2 = (a^2 - b^2) + (2ab)^2 = (a^2 + b^2)^2$$

より $z = a^2 + b^2$ が従う.

□

問題 7 上の証明で $x + iy$ と $x - iy$ が互いに素であることを示せ. ここで α, β が互いに素とは, 共通のガウス素数で割れないと言う意味.

(証明のポイント) 定理 4 の証明では, ポイントが二つあります. 一つは, (3) で $x^2 + y^2 = (x + iy)(x - iy)$ と 1 次式の積に変形する所で, これは整数の範囲ではできません. つまり, 整数の範囲から少し空間を広げることで可能になる変形です. もう一つは, R における素因数分解の一意性を用いる点で, これがないと (4) を導けません. このように, 現代整数論では, 整数の問題であっても, 整数の範囲だけで考えるのではなく, **問題に都合の良い「環」を考え, さらにその構造を調べる**というアプローチをよく用います.

最後に補足ですが, 一般的な環では素因数分解の一意性が成立しないものもあります. 例えば, $x^2 + 5y^2 = z^2$ において, 同様の問題を考えようとすると, 環としては,

$$Q = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$$

を考えることになります. そうすると,

$$z^2 = x^2 + 5y^2 = (x + y\sqrt{-5})(x - y\sqrt{-5})$$

と変形でき, 定理と同様の議論ができそうです. しかし, Q では素因数分解の一意性が成立しないため, 同じやり方はできません. 実際, Q において, $2, 3, 1 \pm \sqrt{-5}$ は全て素数になりますが,

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

となり, 6 は 2 通りの素因数分解を持っています. この問題を解消する方法として, 「イデアル」と呼ばれる概念があります. 興味がある人は文献 [1, 2, 4, 3, 5] を参照にしてください. 授業では, 3 年生の代数学 A で勉強します.

参考文献

[1] 青木昇, 素数と 2 次体の整数論, 共立出版.

[2] 新妻弘, 木村哲三, 群・環・体入」」, 共立出版.

[3] 山崎隆雄, 初等整数論, 共立出版.

[4] 雪江明彦, 代数学 2　環と体とガロア理論, 日本評論社.

[5] 大学数学の授業ノートの「環論」