Gaussの整数の素元分解

POMB(神戸大学数学研究会) 代数班

平成27年度

Abstract

本勉強会では, 代数学の幅広い概念を理解することを目標に,1年を通し自主ゼミ活動を続けてきた. これにより, 群論および環論について主要な定義や定理を学習することができた. 代数学は抽象的な内容であるが, 我々が高校数学の頃から使っていた概念を「拡張」して使えるようにしようという試みも多く,「素元分解」も素因数分解を拡張した概念である. 本稿ではこの素元分解を題材に、環論の内容を紹介する. 具体的には, イデアルなどの基礎的な環論の知識を導入し, 実部および虚部がともに整数の複素数である「Gaussの整数」の素因数分解を考えていく. さらに, 整数において成り立つ素因数分解の一意性について、より一般に素元分解が一意的になる条件を考える.

1 準備

本章では, 環の定義から始まり, 環におけるイデアルや単項イデアル整域といった以降の章で必要とされる概念の定義及び性質を述べる.

1.1 環の定義

環の定義を述べる前に, まず可換群の定義をする.

定義 1.1.1 加法 $M \times M \to M; (a,b) \mapsto a+b$ が与えられた集合 M が**可換群** (*commutative group*) であるとは次を満たすことである.

(1) 任意の $a,b,c \in M$ に対して $(a+b)+c = a+(b+c)$. (**結合法則** (*associative law*))

(2) M の元 0 で任意の $a \in M$ に対して $a+0 = 0+a = a$ を満たすものが存在する.
(この 0 を M の**単位元** (*unit element*) と言う.)

(3) 各 $a \in M$ に対して, $a' \in M$ で $a + a' = a' + a = 0$ を満たすものが存在する. （この a' を a の**逆元** (*inverse element*) といい, 以下 $-a$ と書く.）

(4) 任意の $a, b \in M$ に対して $a + b = b + a$. （**交換法則**（*commutative law*））

次に可換環の定義をする.

定義 1.1.2 加法 $R \times R \to R; (a, b) \mapsto a + b$ と乗法 $R \times R \to R; (a, b) \mapsto ab$ が与えられた集合 R が**可換環** (*ring*) であるとは, 次を満たすことである.

(1) R は加法について可換群である. （加法の単位元を 0 と書き, **零元** (*zero element*) と言う. 加法に関する a の逆元を $-a$ と書く.）

(2) 任意の $a, b, c \in R$ に対して $(ab)c = a(bc)$. （乗法の**結合法則**）

(3) 任意の $a, b, c \in R$ に対して $a(b + c) = ab + ac, (a + b)c = ac + bc$.（**分配法則** (*distributive law*)）

(4) R の元 1 で任意の $a \in R$ に対して $a1 = 1a = a$ を満たすものが存在する.（この 1 を R の**単位元**という.）

(5) 任意の $a, b \in R$ に対して $ab = ba$. （乗法の**交換法則**）

注意 1.1.1

(1)〜*(4)* のみを満たす場合,R は環という. しかし,*(1)*〜*(3)* のみを満たすものを環と呼ぶ流儀もある. このときは,*(1)*〜*(4)* を満たすものを**単位元をもつ環** (*unital ring,ring with unity*) という.

例 1.1.1 環の例をいくつか紹介する.

(1) 整数全体の集合 $\mathbb{Z}$, 有理数全体の集合 $\mathbb{Q}$, 実数全体の集合 $\mathbb{R}$, 複素数全体の集合 $\mathbb{C}$ に通常の加法および乗法を与えたものは可換環である.

(2) 一つの元からなる集合 0 に加法, 乗法を $0 + 0 = 0, 00 = 0$ と定めたものは可換環である. これを**零環** (*zero ring*) といい, 0 と書く.

次に整域の定義を述べる.

定義 1.1.3

零環でない可換環 R が**整域** *(integral domain)* であるとは, 条件「$a, b \in R, ab = 0 \Rightarrow a = 0$ または $b = 0$」が成り立つことである.

1.2　イデアルと単項イデアル整域

環のイデアルの定義を述べる.

定義 1.2.1 環 R の部分集合 I が次を満たすとき, I を R の**左 (右) イデアル** *(left (right) ideal)* と言う.

(1) $0 \in I$.

(2) $x, y \in I \Rightarrow x + y \in I$.

(3) $a \in R, x \in I \Rightarrow ax \in I (xa \in I)$

左かつ右イデアルであるとき**両側イデアル** *(two-sided ideal)* という. R が可換環のときは左右の区別はないので単に**イデアル** *(ideal)* という.

定義 1.2.2
R を環とする.$x \in R$ のとき,x を含む最小の左 *(右)* イデアル $\{ax|a \in R\}(\{xa|a \in R\})$ を x の生成する R の左 *(右)* イデアルといい $Rx(xR)$ と書く. このように R の一つの元から生成されるイデアルを**単項左 (右) イデアル** *(principal right (left) ideal)* という.R が可換環のときは, 単に**単項イデアル** *(principal ideal)* という.

定義 1.2.3
任意のイデアルが単項イデアルであるような整域を**単項イデアル整域** *(principal ideal domain)* という. 以下これを *PID* と呼ぶことにする.

この節の最後に, 重要な事実として $\mathbb{Z}$ が単項イデアル整域であることを示す.

例 1.2.1
$\mathbb{Z}$ は単項イデアル整域であることを示すため, I を $\mathbb{Z}$ のイデアルとし, $I = \{0\}$ のときとそうでないときで場合分けし, どちらも I が単項イデアルとなることを示す.

(1) $I = \{0\}$ のとき,$I = 0\mathbb{Z}$.

(2) $I \supset \{0\}$ のときは I は 0 でない元を含むが, 必要ならば (-1) 倍することにより I が正整数を含むことがわかる. したがって I に属する最小の正整数 n が存在する. このとき $I \supseteq n\mathbb{Z}$. また,m を I の任意の元として $m = nq + r(q, r \in \mathbb{Z}, 0 \leq r < n)$ と割り算すると $r = m - nq \in I$. すると n の定義より $r = 0$ でなければならない. したがって $m = nq \in \mathbb{Z}$ となるので $I = n\mathbb{Z}$.

以上の議論から $\mathbb{Z}$ が単項イデアル整域であることが示された.

2　Gaussの整数の素元分解

本章では、実部と虚部がともに整数である複素数（Gaussの整数）について, 整数環$\mathbb{Z}$における素因数分解を拡張した素元分解を試み,Gaussの整数における「素数」が3つのパターンに整理できることを示す. この定理を示すために、7つの補題と1つの命題を証明する.

2.1　「素数」概念拡張の導入

定義 2.1.1
環Rにおいて乗法の逆元をもつ元を**単元**という.

注意 2.1.1
以下, 環Rにおける単元の集合を$R^\times$で表す.
$R^\times$は乗法について群をなし, **単数群**という.

例 2.1.1
$\mathbb{Z}$において*1,-1*は単元だが,*2*は単元でない.

定義 2.1.2
$a, b \in R$について,aとbが**同伴**であるとは, 条件「$\exists u \in R^\times : b = au$」が成り立つことであり,$a \sim b$と表す. このとき$\sim$は同値関係となる.

注意 2.1.2
$a \mid b$は条件「$\exists u \in R : b = au$」が成り立つことを言う（整除関係）.　$\mid$は同値関係になるとは限らない.

定義 2.1.3
$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$を**Gaussの整数**という.　*Gauss*の整数は単項イデアル整域（*PID*）である（証明略）.

定義 2.1.4
$\mathbb{Z}[i]$のノルムNを,

$$N : \mathbb{Z}[i] \to \mathbb{N}; \alpha = a + bi \mapsto \alpha\overline{\alpha} = a^2 + b^2$$

で定める.

定義 2.1.5
零元でも単元でもない$r \in R$について

(1) $s \in R$について条件「$s \mid r \Rightarrow \quad s \sim 1 \vee s \sim r$」をみたす$r$のことを$R$の**既約元**という.

(2)　$a, b \in R$ について条件「$r \mid ab \Rightarrow \quad r \mid a \vee r \mid b$」をみたす r のことを R の**素元**という.

例 2.1.2

$R = \mathbb{Z}$ の場合,（*1*）は素数の定義.（*2*）は素数の性質である.

注意 2.1.3

R が整域なら,「素元 $\Rightarrow$ 既約元」が成り立ち,R が *PID* ならその逆も成り立つ.*Gauss* の整数は *PID* であるから,*Gauss* の整数についての議論においては素元と既約元は同値となる. よって, 片方の性質が示されればもう片方の性質も成り立つといえることに注意されたい.

2.2　素元分解のための補題証明

2.1 で導入した定義などを用いて、素元分解の定理証明に用いる補題を証明する.

補題 2.2.1

$\mathbb{Z}[i]$ の単元は $N(\alpha) = 1$ であるような α, すなわち $1, -1, i, -i$ の 4 つである.

証明

$\alpha = a + bi$ を $\mathbb{Z}[i]$ の単元とすると

$$(a + bi)(c + di) = 1 \tag{1}$$

をみたす $c, d \in \mathbb{Z}$ が存在する.

このとき

$$(a - bi)(c - di) = 1 \tag{2}$$

も成り立つ.

(1) $\times$ (2) より

$$(a^2 + b^2)(c^2 + d^2) = 1$$

これより

$$a^2 + b^2 = c^2 + d^2 = 1$$

したがって $N(\alpha) = 1$ であり, そのような α が $1, -1, i, -i$ の 4 つであることは容易に分かる.（証明終）

補題 2.2.2

$N(\pi) = p \in \mathbb{Z}$ が素数なら π は（$\mathbb{Z}[i]$ の）既約元である.

証明

$\alpha \mid \pi$ とすれば
$\pi = \alpha\beta \quad (\beta \in \mathbb{Z}[i])$ と表せて

$$\begin{aligned} N(\alpha)N(\beta) &= \alpha\overline{\alpha}\beta\overline{\beta} \\ &= (\alpha\beta)(\overline{\alpha}\overline{\beta}) \\ &= (\alpha\beta)(\overline{\alpha\beta}) \\ &= N(\pi) \\ &= p \end{aligned}$$

これより

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

ゆえに

$$(N(\alpha), N(\beta)) = (1, p), (p, 1)$$

$N(\alpha) = 1$ なら補題 2.2.1 より α は単元 $(\alpha \sim 1)$
$N(\alpha) = p$ なら $N(\beta) = 1$ より β は単元で,$\alpha \sim \pi$
よって π は $\mathbb{Z}[i]$ の既約元.（証明終）

注意 2.2.1
$\mathbb{Z}[i]$ は *PID* より,π は素元でもあることもこれで示したことになる.

補題 2.2.3
π が素元なら $\pi \mid p$ となる素数 p がただ 1 つ存在する.
証明
存在性と一意性についてそれぞれ証明する.
（存在性）
$\pi \mid \pi\overline{\pi} = N(\pi)$ より,$N(\pi) \in \mathbb{Z}^{>0}$ を $\mathbb{Z}$ の範囲で素因数分解して $N(\pi) = p_1 \dots p_r$ とすると π は素元より少なくとも 1 つの p_i を割り切る.
（一意性）
π が 2 つの異なる素数 p_1, p_2 を割り切るならば
$rp_1 + sp_2 = 1$ をみたす $r, s \in \mathbb{Z}$ について
$\pi \mid rp_1 + sp_2$ から $\pi \mid 1$
つまり $\exists u \in \mathbb{Z}[i]; u\pi = 1$
これより π は単元となり, 素元であることに矛盾.
よって素数 p はただ 1 つ存在する.（証明終）

補題 2.2.4
$\pi = a + bi$ が素元,p が素数で $\pi \mid p$ なら $\pi \sim p$ または $N(\pi) = a^2 + b^2 = p$
証明

$p = \pi\delta$ とすれば

$$\begin{aligned} N(\pi)N(\delta) &= (\pi\delta)(\overline{\pi\delta}) \\ &= p^2 \end{aligned}$$

よって

$$(N(\pi), N(\delta)) = (1, p^2), (p, p), (p^2, 1)$$

$N(\pi) = 1$ は素元の定義に反する.
$N(\pi) = p^2$ なら $N(\delta) = 1$ から $\pi \sim p$.
以上により示された.（証明終）

補題 2.2.5
p を素数とする.
(1) $a^2 + b^2 = p$ をみたす $a, b \in \mathbb{Z}$ が存在しないとき p は $\mathbb{Z}[i]$ の素元である.
(2) a, b が存在するとき,$\pi = a + bi$ として $p = \pi\overline{\pi}$ が p の $\mathbb{Z}[i]$ における素元分解である.
証明
(1) p が $\mathbb{Z}[i]$ の素元でないとすると,$\pi \mid p$ となる素元 π $(\pi \not\sim p)$ が存在する.
p は素数なので補題 2.2.4 から $\pi \sim p$ または $N(\pi) = a^2 + b^2 = p$ となるが, 仮定より $a^2 + b^2 = p$ となる a, b が存在しないので $\pi \sim p$ となる. これは $\pi \not\sim p$ に矛盾. よって p は $\mathbb{Z}[i]$ の素元.

(2)$\pi = a + bi$, $\overline{\pi} = a - bi$ は補題 2.2.2 より $\mathbb{Z}[i]$ の素元で $p = \pi\overline{\pi}$ と表せる.

なお, 補題 2.2.5(1) の証明については"$\mathbb{Z}[i]$ の任意の元が素元分解可能である"ことを暗黙裡に仮定している. このことについては 3 章で言及する.

2.3 Gauss の整数における「素数」

本節では以下の定理の証明を行う.

定理 2.3.1
$\mathbb{Z}[i]$ の「素数」、つまり素元は次の 3 つのみからなる.

(a) $1 + i$ とその同伴元 $(ex. -1 - i, -1 + i\ etc)$

(b) $p = 4n + 3$ の形の素数とその同伴元 $(ex. 3, 7, 3i\ etc)$

(c) $p = 4n + 1$ の形の素数の約元になる $a \pm bi (a^2 + b^2 = p)$ とその同伴元
$ex. 5 = (1 + 2i)(1 - 2i)$

証明を行う方針としては, 補題 2.2.3 および補題 2.2.5 から,$\mathbb{Z}[i]$ の素元は $\mathbb{Z}^{>0}$ の素数と対応していることが分かるので, 素数について $\mathbb{Z}[i]$ の範囲で素元分解できるか確認すればよい. 補題 2.2.5 から, 共役複素数の積に素元分解できれば分解した Gauss の整数が素元であり, できなければその素数自体が $\mathbb{Z}[i]$ においても素元であると分かる.
以下, 定理 2.3.1 の $(a), (b)$ を示す.

証明
$(a)\, p = 2$ のとき（唯一の偶数素数）
$2 = (1+i)(1-i)$ と分解できるので 2 は素元でない.
また, 符号を反転させて $2 = (-1-i)(-1+i)$ とも分解できる.
単元倍ではノルムが変わらないので複数通りの表し方がある. 補題 2.2.5 により $1+i$ とその同伴元は素元である.（証明終）

$(b)\, p = 4n+3$ の形の素数について
$a^2 + b^2 = p$ をみたす p が存在しない（$\because$ 任意の $s \in \mathbb{Z}$ について $s^2 \equiv 0 \vee s^2 \equiv 1\,(mod\,4)$）ので補題 2.2.5 より p は素元.（証明終）

(c) についてはこれを示すために 1 つの命題が必要となる.

命題 2.3.1
$p = 4n+1$ の形の素数について $x^2 = -1\,(mod\,p)$ をみたす $x \in \mathbb{Z}$ が存在.
証明
巡回群 $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} - \{\overline{0}\}$ を考えると,（単位元は $\overline{1}$）
この群 $\mathbb{Z}_p^\times$ の位数は $p-1$ であり,4 の倍数.
$\mathbb{Z}_p^\times$ の生成元を x とすると, $x^{\frac{p-1}{4}} = y$ について, $y \in \mathbb{Z}_p^\times$
$y^4 = \overline{1}, y^2 \neq \overline{1}$ であり $\mathbb{Z}_p$ が体であることから

$$y^4 - \overline{1} = (y^2 - \overline{1})(y^2 + \overline{1}) = 0$$

$y^2 - \overline{1} \neq \overline{0}$ より

$$y^2 + \overline{1} = 0$$

これより $y^2 \equiv -1\,(mod\,p)$ となる.（証明終）

これを利用して定理 2.3.1 の (c) を示す.
証明
p が $\mathbb{Z}[i]$ における既約元であると仮定する.
命題 2.3.1 より x^2+1 が p の倍数になる $x \in \mathbb{Z}$ が存在する.

したがって,$p \mid x^2+1=(x+i)(x-i)$
仮定より p は既約元なので

$$p \mid x+i \vee p \mid x-i$$

ところが

$$\frac{x \pm i}{p} = \frac{x}{p} \pm \frac{1}{p}i \notin \mathbb{Z}[i] \ (\because \frac{1}{p} \notin \mathbb{Z})$$

これより $p \nmid x \pm i$
よって p は $\mathbb{Z}[i]$ で既約元（$\Leftrightarrow$ 素元）でない.
ゆえに, 補題 2.2.5(1) の対偶から $p=a^2+b^2$ をみたす a, b が存在する.（証明終）

以上で Gauss の整数における「素数」が定理 2.3.1 の 3 通りに整理されることが示された. なお, $p=4n$ の形の素数は当然存在せず, $p=4n+2$ の形の素数は $p=2$ のみであり、それについては (a) で考察していることに注意されたい.

3　素元分解の一意性等について

補題 2.2.5 の証明において, $\mathbb{Z}[i]$ の素元でない元 p が素元の積に分解されることを暗黙裡に仮定している. しかし, 本当にそうなのだろうか. 本章では, 余談としてこの問題に取り組んでいく.

定理 3.0.2
整域 R において 1 つの元を素元の積に表す方法は, 順序と単元倍を除いて一意的. つまり,$p_i, q_j \in R$ を素元として

$$p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_r$$

とすると $r=s$ であり, かつ番号を付け替えることで $q_i \in p_i R^\times$（つまり $p_i \sim q_i$）とできる.
証明
$p_1 \mid q_1 q q_2 \cdots q_s$ で p_1 は素元だから $\exists j : p_1 \mid q_j$
番号をつけかえることで $j=1$ とする. $q_1 = p_1 u_1$ $(\exists u_1 \in R)$ と書けるが q_1 は既約元（$\because$ 整域なら素元は既約元）で $p_1 \notin R^\times$ より $p_1 \in q_1 R^\times$. つまり $p_1 \sim q_1$, すなわち $u_1 \in R^\times$ である. また,R は整域なので
$p_2 p_3 \cdots p_r = u_1 q_2 q_3 \cdots q_s$ となる.
以下,$p_2, p_3, \cdots$ について繰り返し
$p_i = q_i u_i$ $(\exists u_i \in R^\times), r=s$ かつ $1=u_1 u_2 \cdots u_r$ となる.（証明終）

定義 3.0.1
R : 整域は R の 0 でも単元でもない任意の元が素元の積に書けるなら素元分解整域, または**一意分解整域** (*unique factorization domain*) という. 以下これを *UFD* と呼ぶ.

注意 3.0.1
定理 3.0.2 は整域においては,”元が素元分解可能な場合”, それが一意的に分解できることを保証するものである. *UFD* は”任意の元が素元分解可能”な整域であることに注意されたい.

定理 3.0.3
PID は *UFD* である.

定理 3.0.3 の証明については,”環 R におけるイデアルの任意の増大列が止まる”性質をもった Noether 環を用いるのだが, 難解な気がするので今回は省略する.（私も疲れてきた）
ひとまず, 定理 3.0.3 と,$\mathbb{Z}[i]$ が PID であることから,$\mathbb{Z}[i]$ が UFD であることが分かる. したがって,$\mathbb{Z}[i]$ の任意の元が素元分解可能であるという補題 2.2.5 において暗黙裡においた仮定については, 誤りでないことが分かった.

4 参考文献等

松坂和夫著（1976）『代数系入門』, 岩波書店
神戸大学理学部数学科講義「代数学 2」