蛇の補題の2次体の整数環への応用

青山学院大学　理工学部　物理・数理学科
学籍番号：15119057　坂本 知優
指導教員：西山 享

2023年2月21日

概 要

この論文では**蛇の補題**を 2 次体の整数環へ応用することを考える．A を単位元を持つ可換環とし，M を A-加群とする．$K = \mathbb{Q}(\sqrt{m})$ を 2 次体，$\mathcal{O}_K$ を 2 次体 K の整数環とする．蛇の補題とは，A-加群の短完全列による可換図式から長完全列が得られるという補題である．この補題は様々な分野で応用されている．本研究では，蛇の補題を 2 次体の整数環に応用する．簡単な場合に $\mathcal{O}_K/(x)$（(x) は $\mathcal{O}_K$ の単項イデアル）の $\mathbb{Z}$-加群としての構造決定するのにを蛇の補題を応用することを考える．$\mathcal{O}_K/(x)$ の $\mathbb{Z}$-加群としての構造は整数論ではよく知られていることではあるが，蛇の補題を応用するための一つの実例として考えることにした．

目 次

1　序論

1.1　研究の背景

本研究のきっかけは，私自身の蛇の補題への理解を深めたいと思ったことである．蛇の補題は様々な分野で応用される重要な主張である．本研究では，この蛇の補題を虚 2 次体の整数環 $\mathcal{O}_K$ の構造を調べるのに応用した．虚 2 次体とは有理数体 $\mathbb{Q}$ の二次拡大であって $K = \mathbb{Q}(\sqrt{m}) \quad (m \in \mathbb{Z}_{<0})$ の形をしているものを指す．このとき，K の整数環は $\mathcal{O}_K = \mathbb{Z}[\omega]$ の形をしている．但し

$$\omega = \begin{cases} \frac{1+\sqrt{m}}{2} & (m \equiv 1 \pmod 4) \\ \sqrt{m} & (m \equiv 2, 3 \pmod 4) \end{cases} \tag{1.1}$$

である．虚 2 次体の整数環 $\mathcal{O}_K$ については既に多くのことが知られていて ([3]，[5] などを参照)，特に $\mathcal{O}_K/(x)$（(x) は $\mathcal{O}_K$ の単項イデアル）の $\mathbb{Z}$-加群としての構造はよく知られている．しかしこれらの事実の証明には蛇の補題は通常使わない．そこで，$\mathcal{O}_K/(x)$ の $\mathbb{Z}$-加群としての構造を蛇の補題から調べられないかという着想の上に，本研究を行った．

1.2　研究の主結果

本論文では，虚 2 次体の整数環 $A = \mathcal{O}_K$ を単項イデアルで割った $A/(x)$ の $\mathbb{Z}$-加群としての構造を，$x \in \mathbb{Z}$ の場合と $x = a + b\omega \quad (a, b \in \mathbb{Z})$ が $a, b \neq 0$ かつ $\gcd(a, b) = 1$ の場合に分けて調べている．その主要な考察の対象は次の定理である（例えば [5] の定理 6.27 を参照）．

定理 1.1. $x = a + b\omega \in A \backslash \{0\} \quad (a, b \in \mathbb{Z})$ を A の単元でない元とし，(x) を A の単項イデアルとする．このとき次が成り立つ．

1. $x \in \mathbb{Z}$ ならば，$A/(x) \simeq \mathbb{Z}_x \oplus \mathbb{Z}_x$,
2. $a, b \neq 0$ かつ $\gcd(a, b) = 1$ ならば，

$$A/(x) \simeq \mathbb{Z}_{N(x)}. \tag{1.2}$$

証明には $\#(A/(x))$ が x のノルム $N(x)$ と一致することを使うが，これを示すのに蛇の補題を用いている．また $N(x) = pq \quad (p \neq q)$ とノルムが素因数分解されるときに $A/(x) \simeq \mathbb{Z}_{pq}$ となることにも蛇の補題を応用した．

1.3　本論文の構成

§2 では可換環論の基本事項について述べ，§3 では加群と完全列について述べる．§4 では蛇の補題を紹介し，§5 では 2 次体の整数環 $\mathcal{O}_K$ の定義やそれに関する定理を述べる．§6

では，特定の条件の元での $\mathcal{O}_K/(x)$ の $\mathbb{Z}$-加群としての構造を蛇の補題から決定した．§7 ではまとめと今後の課題を述べる．基本事項で挙げた定理などについては，ほとんどが [1] と [5] からの引用であるが，一々引用箇所は挙げなかった．

2 可換環論

この章では可換環論の基本事項を [1] に従って述べる．

定義 2.1. 環（ring）A とは，次の条件を満たす 2 つの二項演算 (加法，乗法) を持つ集合のことである．

1. A は加法に関してアーベル群,
2. A は乗法に関して結合律

$$(xy)z = x(yz) \quad (x, y, z, \in A) \tag{2.1}$$

を満たし，分配律

$$x(y+z) = xy + xz \quad (y+z)x = yx + zx \quad (x, y, z, \in A) \tag{2.2}$$

を満たす．

定義 2.2. 環 A が**可換**であるとは，次の条件を満たすことである．

$$xy = yx \quad (x, y \in A). \tag{2.3}$$

定義 2.3. 環 A が条件：

$$^{\exists}1 \in A, \quad ^{\forall}x \in A \quad \text{s.}t. \quad x1 = 1x = x \tag{2.4}$$

を満たすとき，1 を A の**単位元**と呼ぶ．

以降，この論文では「環」は単位元をもつ可換環とする．

定義 2.4. A を環とする．$\mathfrak{a} \subseteq A$ とする．$\mathfrak{a}$ が次の三つの条件を満たすとき，$\mathfrak{a}$ は A の**イデアル**（ideal）であるという．

1. $\mathfrak{a} \neq \emptyset$,
2. $x, y \in \mathfrak{a} \implies x + y \in \mathfrak{a}$,
3. $x \in A, y \in \mathfrak{a} \implies xy \in \mathfrak{a}$ (即ち $A\mathfrak{a} \subseteq \mathfrak{a}$).

定義 2.5. A を環，$\mathfrak{a}$ を A のイデアルとする．加法群としての剰余群 $A/\mathfrak{a}$ は環 A の乗法から自然に乗法が定義され（$a(x+\mathfrak{a}) = ax + \mathfrak{a}$），環となる．この $A/\mathfrak{a}$ を**剰余環**という．

定理 2.6 (中国式剰余定理). ([1] 命題 1.10) A を環，$\mathfrak{a}_1$，$\mathfrak{a}_2$，$\cdots$，$\mathfrak{a}_n$ を A のイデアルとする．このとき次が成り立つ．

1. $i \neq j$ のとき $\mathfrak{a}_i$ と $\mathfrak{a}_j$ が互いに素 $\Longrightarrow \bigcap \mathfrak{a}_i = \mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_n$.
2. $A/\bigcap \mathfrak{a}_i \simeq A/\mathfrak{a}_1 \times A/\mathfrak{a}_2 \times \cdots \times A/\mathfrak{a}_n$.

例 2.7 (中国式剰余定理の例). $A = \mathbb{Z}$ のとき,

- $\mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
- $\mathbb{Z}/28\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$

が成り立つ.

3 加群と完全列

この章では A-加群，完全列の定義や性質を紹介する．

3.1 加群と加群の準同型写像

A-加群とは，環 A が線形に作用する加法群のことである．より正確に述べると次のようになる．

定義 3.1. A を環とする．組 (M, μ) が **A-加群**（A-module）であるとは，次の二つの条件を満たすことである．

- M は加法群
- 写像 $\mu\colon A \times M \to M$ は次の公理を満たす（$\mu(a, m) =: am$ と書く）

$$a(x + y) = ax + ay \quad (a, b \in A; x, y \in M), \tag{3.1}$$
$$(a + b)x = ax + bx, \tag{3.2}$$
$$(ab)x = a(bx), \tag{3.3}$$
$$1x = x. \tag{3.4}$$

以降，A-加群 (M, μ) を単に M と書く．

例 3.2 (A-加群の例).

- $A = \mathbb{Z}$ のとき $\mathbb{Z}$-加群とは加法群のことである．
- A が体 k のとき A-加群とは k-ベクトル空間のことである．

定義 3.3. M を A-加群とする．部分集合 $M' \subseteq M$ が M の**部分加群**（submodule）であるとは，M' は加法群として M の部分群であり，A の作用で閉じていることである．

A のイデアルは A の部分加群に他ならない.

定義 3.4. M を A-加群，M' を M の部分加群とする．加法群としての剰余群 M/M' は $a(x+M')=ax+M'$ と定義することによって A-加群の構造を M から受け継ぐ．A-加群 M/M' を M' による M の**剰余加群**（quotient module）という.

定義 3.5. M,N を A-加群とする．$f\colon M\to N$ が条件

$$\begin{cases} f(x+y)=f(x)+f(y) & (x,y\in M) \\ f(ax)=af(x) & (a\in A; x\in M) \end{cases} \tag{3.5}$$

を満たすとき，f を **A-加群の準同型写像**（A-module homomorphism）（または **A-線形**）という．準同型写像が全単射である時，**同型写像**という.

つまり，A-加群の準同型とは，任意の $a\in A$ の作用と可換である加法群の準同型のことである．A-加群の準同型を単に A-準同型と書くこともある.

定理 3.6 (A-加群の準同型定理). ([7] 定理 10.1) $f\colon M\to N$ を A-準同型とする．このとき次の自然な同型写像 $\bar{f}$ が存在する.

$$\begin{array}{rccc} \bar{f}\colon & A/\mathrm{Ker}f & \to & \mathrm{Im}f \\ & \cup & & \cup \\ & x+\mathrm{Ker}f & \mapsto & f(x) \end{array} \tag{3.6}$$

3.2 完全列

定義 3.7 (完全列). M_i を A-加群，$f_i\colon M_{i-1}\to M_i$ を A-加群の準同型とする．列

$$\cdots\longrightarrow M_{i-1}\xrightarrow{f_i} M_i\xrightarrow{f_{i+1}} M_{i+1}\longrightarrow\cdots \tag{3.7}$$

が**完全**（exact）であるとは，任意の i に対して $\mathrm{Im}f_i=\mathrm{Ker}f_{i+1}$ を満たすことである．特に，3 項からなる完全列

$$0\to M_1\to M_2\to M_3\to 0 \tag{3.8}$$

を**短完全列**という.

補題 3.8.

- $0\to M_1\xrightarrow{f} M_2$ が完全である $\iff$ f は単射である
- $M_1\xrightarrow{g} M_2\to 0$ が完全である $\iff$ g は全射である
- $0\to M_1\xrightarrow{f} M_2\xrightarrow{g} M_3\to 0$ が完全である
  $\iff$ f は単射，g は全射かつ g は同型

$$\begin{array}{rccc} \bar{g}\colon & M_2/f(M_1) & \xrightarrow{\sim} & M_3 \\ & \cup & & \cup \\ & \bar{x} & \mapsto & g(x) \end{array} \tag{3.9}$$

を誘導する.

4　蛇の補題

この章では，蛇の補題について述べる．まず，余核を定義する．

定義 4.1 (余核)．$f\colon M \to N$ を A-準同型とする．N の剰余加群 $\mathrm{Coker} f := N/\mathrm{Im} f$ を f の**余核**という．

補題 4.2 (蛇の補題)．A-加群の短完全列による可換図式

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{u} & M_2 & \xrightarrow{v} & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & N_1 & \xrightarrow{s} & N_2 & \xrightarrow{t} & N_3 & \longrightarrow & 0 \end{array} \tag{4.1}$$

が与えられた時，次の長完全列が構成できる．

$$0 \to \mathrm{Ker} f \xrightarrow{\bar{u}} \mathrm{Ker}\, g \xrightarrow{\bar{v}} \mathrm{Ker}\, h \xrightarrow{d} \mathrm{Coker} f \xrightarrow{\bar{s}} \mathrm{Coker}\, g \xrightarrow{\bar{t}} \mathrm{Coker}\, h \to 0 \tag{4.2}$$

$d\colon \mathrm{Ker}\, h \to \mathrm{Coker} f$ は**連結準同型**と呼ばれ，次のように定義される．$x \in \mathrm{Ker}\, h$ とすれば，$x \in M_3$ である．この x に対して，v は全射より $v(y) = x$ なる $y \in M_2$ が存在する．$\beta := g(y)$ とすれば，$t(\beta) = t(g(y)) = h(v(y)) = h(x) = 0$ より，$\beta \in \mathrm{Ker}\, t = \mathrm{Im}\, s$ となる．ゆえに，$s(\alpha) = \beta$ なる $\alpha \in N_1$ が存在する．$d\colon \mathrm{Ker}\, h \to \mathrm{Coker} f$ を $d(x) = \alpha \pmod{\mathrm{Im} f}$ で定める．

蛇の補題において，$\bar{u}$，$\bar{v}$，$\bar{s}$，$\bar{t}$ はそれぞれ u，v，s，t から標準的に決まるので，連結準同型 d が well-defined であり，かつ列（4.2）が完全であることが主要な主張である．

Proof. 蛇の補題の証明は，[2] の 17 頁，例 1.8 を参照してほしい．　□

5　2 次体の整数環

この章では，2 次体の整数環についての定義及び性質を述べる．以降，$m \in \mathbb{Z}\backslash\{0\}$ は平方因子を持たないとする．

5.1　2 次体の整数環

まず，2 次体の定義を行う．

定義 5.1 (2 次体)．2 **次体**とは，$K = \mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\}$ で表される体のことである．$m > 0$ の時 K を**実 2 次体**，$m < 0$ の時 K を**虚 2 次体**という．

つまり，2 次体 $K = \mathbb{Q}(\sqrt{m})$ は $\mathbb{Q}$ の 2 次拡大体である．次に，2 次体の整数環を考察する上で重要な道具となるノルムを定義する．

定義 5.2 (ノルム)**.** $x = a + b\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ の $\mathbb{Q}$ 上のノルム $N(x)$ を次のように定める.

$$\begin{array}{rccc} \varphi_x\colon & \mathbb{Q}(\sqrt{m}) & \to & \mathbb{Q}(\sqrt{m}) \\ & \cup & & \cup \\ & y & \mapsto & xy \end{array} \tag{5.1}$$

を $\mathbb{Q}$ 線型写像としての表現行列を T_x として, $N(x) := \det_{\mathbb{Q}} T_x$ とおく.

補題 5.3. ノルムは次の性質をもつ.

1. $N(a + b\sqrt{m}) = a^2 - mb^2 \quad (a + b\sqrt{m} \in \mathbb{Q}(\sqrt{m}))$,
2. $m < 0$ (虚 2 次体) ならば $N(x) = |x|^2 = x\bar{x} \geq 0 \quad (x \in \mathbb{Q}(\sqrt{m}))$,
3. $N(xy) = N(x)N(y) \quad (x, y \in \mathbb{Q}(\sqrt{m}))$.

定義 5.4. $K = \mathbb{Q}(\sqrt{m})$ を 2 次体とする.

$$\mathcal{O}_K = \{x \in K \mid \text{ある } f(t) \in \mathbb{Z}[t] : \text{モニック が存在して } f(x) = 0\} \tag{5.2}$$

を K の**整数環**という. $\mathcal{O}_K$ は K における $\mathbb{Z}$ の整閉包である.

命題 5.5. ([5] 定理 4.18) 2 次体の整数環は $\mathcal{O}_K = \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ である. ただし, ω は次で定める.

$$\omega = \begin{cases} \frac{1+\sqrt{m}}{2} & (m \equiv 1 \pmod 4) \\ \sqrt{m} & (m \equiv 2, 3 \pmod 4) \end{cases} \tag{5.3}$$

例 5.6.

- $\mathbb{Q}(\sqrt{-1})$ の整数環はガウス整数環 $\mathbb{Z}[\sqrt{-1}]$ である.
- $\mathbb{Q}(\sqrt{-3})$ の整数環はアイゼンシュタイン整数環 $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ である.
- $\mathbb{Q}(\sqrt{-7})$ の整数環はクライン整数環 $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ と呼ばれる.

5.2 2 次体の整数環の性質

命題 5.7. ([5] 定理 5.39) 2 次体 K の整数環 $\mathcal{O}_K$ に対して UFD ならば PID である. 即ち

$$\text{ユークリッド整域} \implies \text{PID} \iff \text{UFD} \tag{5.4}$$

が成り立つ.

定理 5.8 (ベイカー・ヘーグナー・スターク)**.** $K = \mathbb{Q}(\sqrt{m})$ $(m < 0)$ を虚 2 次体とする. このとき次が成り立つ.

$$\mathcal{O}_K\text{が UFD} \iff -m = 1, 2, 3, 7, 11, 19, 43, 67, 163 \tag{5.5}$$

6　蛇の補題の 2 次体の整数環への応用

この章では，本研究の主結果について述べる．以降，$A = \mathcal{O}_K = \mathbb{Z}[\omega]$ を虚 2 次体 K の整数環とし，$\mathbb{Z}/n\mathbb{Z}$ を $\mathbb{Z}_n$ で表す．ω は式 (5.3) で与えられているものとする．まず，主結果のために必要な命題及び補題を述べる．

命題 6.1.

$$c \in \mathbb{Z} \implies A/(c) \simeq \mathbb{Z}_c \oplus \mathbb{Z}_c \quad \text{（加法群としての同型）} \tag{6.1}$$

が成り立つ．

Proof. 写像 φ を

$$\begin{array}{rccc} \varphi\colon & A & \to & \mathbb{Z}_c \oplus \mathbb{Z}_c \\ & \cup & & \cup \\ & a + b\omega & \mapsto & (a + c\mathbb{Z}, b + c\mathbb{Z}) \end{array} \tag{6.2}$$

とすれば，これは全射群準同型である．この準同型の核は $\mathrm{Ker}\varphi = Ac = (c)$ なので，準同型定理から主張が得られる． □

補題 6.2. $x \in A\backslash\{0\}$ を A の単元でない元とし，(x) を A の単項イデアルとする．このとき

$$\#(A/(x)) = N(x) \tag{6.3}$$

が成り立つ．つまり，$A/(x)$ の（群としての）位数はノルム $N(x)$ である．

Proof. $N(x)$ を素因数分解して，

$$N(x) = {p_1}^{e_1}{p_2}^{e_2}\cdots{p_k}^{e_k} \tag{6.4}$$

とする．$l := \frac{N(x)}{p_1}$ とする．次のような短完全列による可換図式を考える．

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{u} & A & \xrightarrow{v} & A/(p_1) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A & \xrightarrow{s} & A & \xrightarrow{t} & A/(\bar{x}) & \longrightarrow & 0 \end{array} \tag{6.5}$$

ただし，準同型は次のように構成される．$z \in A$ に対して，

$$\begin{gathered} u\colon z \mapsto p_1 z,\ v\text{: 自然な準同型}, \\ s\colon z \mapsto \bar{x}z,\ t\text{: 自然な準同型}, \\ f\colon z \mapsto xz,\ g\colon z \mapsto lz,\ h\colon z + (p_1) \mapsto lz + (\bar{x}) \end{gathered}$$

とする．f，g は単射なので

$$\mathrm{Ker} f = 0, \mathrm{Ker}\, g = 0, \mathrm{Coker} f = A/(x), \mathrm{Coker}\, g = A/(l)$$

である．これに蛇の補題を用いると長完全列

$$0 \to 0 \xrightarrow{\bar{u}} 0 \xrightarrow{\bar{v}} \mathrm{Ker}\, h \xrightarrow{d} A/(x) \xrightarrow{\bar{s}} A/(l) \xrightarrow{\bar{t}} \mathrm{Coker}\, h \to 0 \tag{6.6}$$

が得られる．$\alpha := \#\mathrm{Ker}\, h$，$\beta := \#(A/(x))$，$\gamma := \#(A/(l))$，$\delta := \#\mathrm{Coker}\, h$ と置くと，完全列 (6.6) から

$$\frac{\alpha}{\beta}\frac{\gamma}{\delta} = 1 \tag{6.7}$$

即ち

$$\alpha\gamma = \beta\delta \tag{6.8}$$

が成り立つ．一方 h についての準同型定理と $A/(\bar{x})$ が複素共役により $\mathbb{Z}$-加群として $A/(x)$ と同型であることを用いると，

$$\delta = \frac{\beta}{\frac{\#(A/(p_1))}{\alpha}} = \frac{\alpha\beta}{{p_1}^2} \tag{6.9}$$

である．式 (6.9) を式 (6.8) に代入して，

$$\alpha\gamma = \beta\frac{\alpha\beta}{{p_1}^2}$$

となるので，$\gamma = l^2$ に注意すると，

$$\beta^2 = {p_1}^2\gamma = {p_1}^2 \cdot l^2 = N(x)^2$$

となる．よって $\beta = N(x)$，即ち $\#(A/(x)) = N(x)$ が得られる． □

補題 6.3. $x \in A\backslash\{0\}$ を A の単元でない元，(x) を A の単項イデアルとする．$A/(x)$ は

$$A/(x) \simeq \mathbb{Z}_{N(x)} \quad \text{または} \quad \mathbb{Z}_l \oplus \mathbb{Z}_{l'} \tag{6.10}$$

の形で表せる．但し，l，l' は

$$\begin{cases} l \cdot l' = N(x) \\ l' \mid l \\ 1 < l' \leq l < N(x) \end{cases} \tag{6.11}$$

を満たす正の整数である．

Proof. 補題 6.2 より $A/(x)$ は有限群である．$A \simeq \mathbb{Z} \oplus \mathbb{Z}$ より，$A/(x) \simeq (\mathbb{Z} \oplus \mathbb{Z})/N$（但し，$N$ は $\mathbb{Z} \oplus \mathbb{Z}$ のある加法部分群）と表せる．つまり $\mathbb{Z}$-加群の全射準同型

$$\phi\colon \mathbb{Z} \oplus \mathbb{Z} \twoheadrightarrow A/(x) \tag{6.12}$$

が存在する．$e_1 = (1, 0)$，$e_2 = (0, 1)$ と置けば $\{e_1, e_2\}$ は $\mathbb{Z} \oplus \mathbb{Z}$ の生成系である．従って，$\{\phi(e_1), \phi(e_2)\}$ は $A/(x)$ の生成系である．よって $A/(x)$ は高々2 元生成である．補題 6.2 より $A/(x)$ の位数は $N(x)$ なので，1 元生成のときは

$$A/(x) \simeq \mathbb{Z}_{N(x)} \tag{6.13}$$

となり，2 元生成のときは，$l \cdot l' = N(x)$ かつ $1 < l, l' < N(x)$ なる正の整数 l, l' を用いて，

$$A/(x) \simeq \mathbb{Z}_l \oplus \mathbb{Z}_{l'} \tag{6.14}$$

となる．ここで

$$\begin{cases} l = {p_1}^{e_1} {p_2}^{e_2} \cdots {p_k}^{e_k} \\ l' = {p_1}^{f_1} {p_2}^{f_2} \cdots {p_j}^{f_j} \end{cases} \tag{6.15}$$

と素因数分解して表し，

$$\begin{cases} c_i = \min\{e_i, f_i\} \\ d_i = \max\{e_i, f_i\} \end{cases} \tag{6.16}$$

と置いて，

$$\begin{cases} n_1 = \prod {p_i}^{c_i} \\ n_2 = \prod {p_i}^{d_i} \end{cases} \tag{6.17}$$

と決める．すると，$n_1 \mid n_2$ であって，

$$\mathbb{Z}_l \oplus \mathbb{Z}_{l'} \simeq \sum (\mathbb{Z}_{{p_i}^{e_i}} \oplus \mathbb{Z}_{{p_i}^{f_i}}) \simeq \sum (\mathbb{Z}_{{p_i}^{c_i}} \oplus \mathbb{Z}_{{p_i}^{d_i}}) \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \tag{6.18}$$

となる．n_1, n_2 を改めて l', l と置けば，主張が得られる． □

以下では，本論文の主目標である，蛇の補題を使った，ある条件のもとでの $A/(x)$ の $\mathbb{Z}$-加群としての構造の決定について述べる．

定理 6.4. $a, b \in \mathbb{Z}$ として，$x = a + b\omega \in A \backslash \{0\}$ を A の単元でない元とし，(x) を A の単項イデアルとする．このとき次が成り立つ．

1. $x \in \mathbb{Z}$ のとき，$A/(x) \simeq \mathbb{Z}_x \oplus \mathbb{Z}_x$,
2. $a, b \neq 0$ かつ $\gcd(a, b) = 1$ のとき，

$$A/(x) \simeq \mathbb{Z}_{N(x)}. \tag{6.19}$$

Proof. 1 の場合は，命題 6.1 で示したから 2 の場合を示す．補題 6.3 により

$$A/(x) \simeq \mathbb{Z}_{N(x)} \quad \text{または} \quad \mathbb{Z}_l \oplus \mathbb{Z}_{l'} \tag{6.20}$$

の形のものしかあり得ない．但し，l, l' は

$$\begin{cases} l \cdot l' = N(x) \\ l' \mid l \\ 1 < l' \leq l < N(x) \end{cases} \tag{6.21}$$

を満たす正の整数である．$A/(x) \simeq \mathbb{Z}_l \oplus \mathbb{Z}_{l'}$ として矛盾を導く．
この時，任意の $\alpha \in A/(x)$ は $l\alpha = 0$，即ち $l\alpha \in (x)$ を満たす．特に $\alpha = 1$ として $l \in (x)$ となる．つまり

$$\frac{l}{x} = \frac{l\bar{x}}{N(x)} = \frac{la}{N(x)} + \frac{lb}{N(x)}\bar{\omega} \in A \tag{6.22}$$

となり，$\omega = \frac{1+\sqrt{m}}{2}$ のとき $\bar{\omega} = 1 - \omega$，$\omega = \sqrt{m}$ のとき $\bar{\omega} = -\omega$ に注意すると，

$$\frac{la}{N(x)}, \frac{lb}{N(x)} \in \mathbb{Z} \tag{6.23}$$

が成り立つ．ここで $l_1 := \gcd(l, N(x))$ として $l = l_1 l_2$，$N(x) = l_1 a_1$ と書くと，

$$\frac{la}{N(x)} = \frac{l_1 l_2 a}{l_1 a_1} = \frac{l_2 a}{a_1} \in \mathbb{Z} \tag{6.24}$$

となる．l_1 のとり方より $a_1 \nmid l_2$ であるから $a_1 \mid a$ となる．同様にも $a_1 \mid b$ 分かる．仮定より $\gcd(a, b) = 1$ だったから $a_1 = 1$ となり，$N(x) = l_1$ となる．つまり $l = l_1 l_2 = N(x) l_2 \geq N(x)$ となる．これは $l < N(x)$ に矛盾する．以上により，

$$A/(x) \simeq \mathbb{Z}_{N(x)} \tag{6.25}$$

の形であることが分かった． □

次に，$N(x) = pq$ $(p, q$ は相異なる素数$)$ の場合を考える．これは補題 6.2 と有限生成アーベル群の基本定理より，

$$A/(x) \simeq \mathbb{Z}_{pq} \tag{6.26}$$

となることが分かるが，蛇の補題のみを使うことによって直接導くことができる．重複にはなるが，蛇の補題の応用例を考えることが目的なので，以下ではこれを示す．

命題 6.5. $x \in A \backslash \{0\}$ を A の単元でない元とし，(x) を A の単項イデアルとする．このとき次が成り立つ．

$$N(x) = pq \quad (p, q \text{ は相異なる素数}) \implies A/(x) \simeq \mathbb{Z}_{pq}. \tag{6.27}$$

Proof. 補題 6.2 と同様に，次のような短完全列による可換図式を考える．

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{u} & A & \xrightarrow{v} & A/(p) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A & \xrightarrow{s} & A & \xrightarrow{t} & A/(\bar{x}) & \longrightarrow & 0 \end{array} \tag{6.28}$$

ただし，準同型は次のように構成される．$z \in A$ に対して，

$$\begin{gathered} u\colon z \mapsto pz,\ v\text{: 自然な準同型}, \\ s\colon z \mapsto \bar{x}z,\ t\text{: 自然な準同型}, \\ f\colon z \mapsto xz,\ g\colon z \mapsto qz,\ h\colon z + (p) \mapsto qz + (\bar{x}) \end{gathered}$$

とする．f，g は単射なので

$$\mathrm{Ker} f = 0, \mathrm{Ker}\, g = 0, \mathrm{Coker} f = A/(x), \mathrm{Coker}\, g = A/(q)$$

である．これに蛇の補題を用いると長完全列

$$0 \to 0 \xrightarrow{\bar{u}} 0 \xrightarrow{\bar{v}} \mathrm{Ker}\, h \xrightarrow{d} A/(x) \xrightarrow{\bar{s}} A/(q) \xrightarrow{\bar{t}} \mathrm{Coker}\, h \to 0 \tag{6.29}$$

が得られる．$A/(x)$ を B とおく．
$\mathrm{Ker}\, h \subseteq A/(p) \simeq \mathbb{Z}_p \oplus \mathbb{Z}_p$ は部分加群なので，(i) $\mathrm{Ker}\, h = 0$ と (ii) $\mathrm{Ker}\, h \simeq \mathbb{Z}_p \oplus \mathbb{Z}_p$ と (iii) $\mathrm{Ker}\, h \simeq \mathbb{Z}_p$ の場合しか起こり得ない．そこで以下，場合分けして考える．
(i) $\mathrm{Ker}\, h = 0$ のとき．これは h が単射ということなので，

$$A/(p) \simeq \mathbb{Z}_p \oplus \mathbb{Z}_p \subseteq A/(\bar{x}) \tag{6.30}$$

となる．複素共役をとることで，$A/(\bar{x}) \simeq A/(x) = B$ であることに注意する．しかし列（6.29）の完全性から，$\bar{s}$ は単射であるから，

$$\mathbb{Z}_p \oplus \mathbb{Z}_p \subseteq A/(\bar{x}) \simeq B \subseteq \mathbb{Z}_q \oplus \mathbb{Z}_q \tag{6.31}$$

となる．これは矛盾である．よって $\mathrm{Ker}\, h \neq 0$ である．
(ii) $\mathrm{Ker}\, h \simeq \mathbb{Z}_p \oplus \mathbb{Z}_p$ のとき．これは h が零写像ということなので，

$$\mathrm{Coker}\, h = A/(\bar{x}) \simeq B \tag{6.32}$$

となる．列（6.29）の完全性から，$\bar{t}$ は全射で，

$$\bar{t} \colon \mathbb{Z}_q \oplus \mathbb{Z}_q \twoheadrightarrow \mathrm{Coker}\, h \simeq B \tag{6.33}$$

となる．しかし，再度列（6.29）の完全性から，d は単射より

$$\mathbb{Z}_p \oplus \mathbb{Z}_p \subseteq B \tag{6.34}$$

となる．これは矛盾である．よって $\mathrm{Ker}\, h \subsetneq \mathbb{Z}_p \oplus \mathbb{Z}_p$ である．
(iii) $\mathrm{Ker}\, h \simeq \mathbb{Z}_p$ のとき．h に対する準同型定理より，

$$\mathrm{Im}\, h \simeq (A/(p))/\mathrm{Ker}\, h \simeq \mathbb{Z}_p \tag{6.35}$$

なので $\mathrm{Coker}\, h \simeq B/\mathbb{Z}_p$ となる．列（6.29）の完全性から，d は単射で，

$$\mathrm{Ker}\, \bar{s} = \mathrm{Im}\, d = \mathrm{Ker}\, h \simeq \mathbb{Z}_p \tag{6.36}$$

となる．$\bar{s}$ に対する準同型定理を用いると，

$$B/\mathbb{Z}_p \simeq (A/(x))/\mathrm{Ker}\, \bar{s} \simeq \mathrm{Im}\, \bar{s} \subseteq A/(q) \simeq \mathbb{Z}_q \oplus \mathbb{Z}_q \tag{6.37}$$

は部分加群である．$B/\mathbb{Z}_p \neq 0$ であることを背理法で示す．$B/\mathbb{Z}_p = 0$ とすると $B \simeq \mathbb{Z}_p$ となって，d は全単射である．従って $\bar{s}$ は零写像となる．ゆえに $\bar{t}$ は全単射となり，

$$\mathbb{Z}_q \oplus \mathbb{Z}_q \simeq \mathrm{Coker}\, h \simeq B/\mathbb{Z}_p = 0 \tag{6.38}$$

となる．これは矛盾である．
次に $B/\mathbb{Z}_p \not\simeq \mathbb{Z}_q \oplus \mathbb{Z}_q$ を示す．そこで同型であるとすると $\mathrm{Im}\,\bar{s} \simeq B/\mathbb{Z}_p \simeq \mathbb{Z}_q \oplus \mathbb{Z}_q$ が成り立つ．ここで $\mathrm{Coker}\,h \simeq B/\mathbb{Z}_p \simeq \mathbb{Z}_q \oplus \mathbb{Z}_q$ より，$\bar{t}$ は全単射となるので，$\bar{s}$ は零写像となる．これも矛盾である．
よって，$B/\mathbb{Z}_p \simeq \mathbb{Z}_q$ しかあり得ない．ゆえに，

$$A/(x) \simeq B \simeq \mathbb{Z}_{pq} \tag{6.39}$$

である． □

7　まとめと今後の課題

A が虚 2 次体の整数環のとき，次の定理を蛇の補題を応用して証明した．蛇の補題が強力であることが実感できた．

定理 7.1. $a, b \in \mathbb{Z}$ として，$x = a + b\omega \in A\backslash\{0\}$ を A の単元でない元とし，(x) を A の単項イデアルとする．このとき次が成り立つ．

1. $x \in \mathbb{Z}$ のとき，$A/(x) \simeq \mathbb{Z}_x \oplus \mathbb{Z}_x$,
2. $a, b \neq 0$ かつ $\gcd(a, b) = 1$ のとき，

$$A/(x) \simeq \mathbb{Z}_{N(x)}. \tag{7.1}$$

また p, q を相異なる素数として $N(x) = pq$ とノルムが表されるときに $A/(x) \simeq \mathbb{Z}_{pq}$ となることを，より直接的な形で蛇の補題を用いることにより証明できた．今後の課題として，

- 超関数など他の分野での蛇の補題の応用を考える
- 可換環論やそれを応用する分野を学ぶ

が挙げられる．

参考文献

[1] M.F.Atiyah and I.G.MacDonald. 可換代数入門. 共立出版, 2006.

[2] 河田敬義. ホモロジー代数 1. 岩波書店, 1982.

[3] 高木貞治. 初等整数論講義. 共立出版, 1971.

[4] 志甫淳. 層とホモロジー代数. 共立出版, 2016.

[5] 青木昇. 数学のかんどころ 15，素数と 2 次体の整数論. 共立出版, 2012.

[6] 飯高茂. 数学のかんどころ 17，環論，これはおもしろい，素因数分解と循環小数への応用. 共立出版, 2013.

[7] 堀田良之. 代数入門 —群と加群— 新装版. 裳華房, 2021.