格子の数学とその教育への応用

－　格子の基底と格子多角形の性質を中心として　－

２０１９年

兵庫教育大学大学院
連合学校教育学研究科
教科教育実践学専攻
（鳴門教育大学）
有　元　康　一

目 次

序論

本論文では, 格子の基底および格子多角形の性質を中心として, 格子の数学とその教育への応用について考察する. 格子を含む整数論の題材は, 児童生徒にとって馴染みやすく興味や関心をもって学習に取り組むことができるため, 数学教育への応用が期待できる. また, 格子は従来から数学の研究対象の 1 つであり, 格子理論は現代の情報社会を支える暗号技術に応用されることが期待されている. 従って, これからの社会を生きていく児童生徒にとっても興味を引くものとなり得ると考える. これらの理由により, 本論文では格子に関する話題を取り扱う.

文部科学省 ([18],[19],[20]) は新学習指導要領において, 「主体的・対話的で深い学び」の実現に向けた授業改善を通して, 創意工夫を生かした特色ある教育活動を展開する中で, 児童生徒に主体的に学ぶ力, すなわち自ら課題を見つけ学んでいく力, を中心とする生きる力を育むことを目指している.

秋田 ([1]) は, 小・中学校における算数・数学の授業において, 数学の学問的構成原理である公理に基づく手法を強く意識して, 既習事項を基に新しい知識や問題解決の方法を獲得させることに重点を置いた指導の重要性を指摘している. さらに, 算数・数学を担当する教員が, この手法をはっきり意識し, 児童生徒がこの手法を使って自分自身で新たな知識を創れるように仕組まなければ, 児童生徒が自分自身で自律的に算数・数学の理解を深めることは難しいだろうと指摘している. つまり, 生きる力の育成のためには, 教師自身が数学の本質である公理に基づく手法を強く意識する必要があることを主張している. また, 主体的に学ぶ力の育成のためには, 児童生徒の興味・関心や理解度に応じて関連する内容を授業において取り上げることができることも重要である. 松崎 ([17]) は, そのためには教師が大学数学までの内容を系統的かつ俯瞰的に捉えておくことが必要であることを指摘している.

以上で見たように, 学習指導要領で述べられている「主体的・対話的で深い学び」を実現するためには, 教師自身が数学を学び, 数学の特質や本質を実際に体験して理解してい

なければならない. また, 小学校から大学までの学習内容を系統的かつ俯瞰的に捉えたうえで, 既知の事実を活用して, 新しいものを生み出そうという姿勢が大切であると考える.

しかし, 実際の算数・数学の授業においては, 教師自身が公理に基づく数学の学問的構成原理を敬遠する傾向があることが否めない. さらに, 学力の向上を目的としながら, 目前にある演習問題の解き方の指導に陥りがちで, 授業の方法論のみが意識されているという現状がある. 方法論が重要であることは言うまでもないが, 内容論と方法論の両方が必要不可欠であり, それぞれが, 車の両輪のように作用することが大切である. 従って, 数学の内容も詳細に吟味した授業構成が必要不可欠であり, これらが互いに影響しあうことが肝要である.

本論文では, 第 I 部で格子の基底の性質とその教育への応用, 第 II 部で格子多角形の性質とその教育への応用について論じる. 各部の概要を述べる.

第 I 部では, 格子基底簡約理論について述べる. 情報セキュリティ分野では, 次世代暗号として有力な格子暗号が注目されている. 格子暗号とは, 格子の最短ベクトル問題など, 格子理論における解決困難な問題を安全性の根拠とする暗号方式である ([21]).

この最短ベクトル問題への基本的なアプローチの 1 つとして, LLL 格子基底簡約アルゴリズム (LLL Lattice basis reduction algorithm) がある. このアルゴリズムは，1982 年に, A.K.Lenstra, H.W.Lenstra, Jr., and L.Lovász ([15]) によって開発された. 基底簡約とは格子において簡約基底 (reduced basis) を求めることであり, 基底をうまく取りかえて，応用する際に都合の良い単純なものを構成することである. これは,「基底の選択」または「基底の標準化」とも言える. この研究は, 計算機への実装が実現され, 工学の分野等で応用されている. 応用例として, 有理数係数多項式の因子分解がある. これは, 多項式時間の計算量で因子分解を行うものである.

Lenstra, et al. による研究をはじめとする一連の研究では, ベクトル空間 $\mathbb{R}^n$ における, 有理整数環 $\mathbb{Z}$ 上の格子を考えていたが, H.Napias ([22]) は, このアルゴリズムをユークリッド環上の格子に一般化している.

本研究では, H.Napias と同様の観点により, LLL 格子基底簡約について, 有限次代数体 F 上における整数環 $\mathcal{O}_F$ 上の格子への一般化を試みた. その結果, 虚二次体に限り一般化可能であることを明らかにした. このように, 概念を一般化することにより, 本質的な要素が把握できたり, 新たな要素が見えてくることが多いが, 実際, 本研究により, 格子基底

簡約問題においては, 前提条件として, 考えている環で最小元の存在が必要であることが分かった. この他, 虚二次体における簡約基底の性質, およびガウスの数体 $\mathbb{Q}(\sqrt{-1})$ において簡約基底が常に存在する条件を明らかにした.

最後に, 格子基底簡約理論の教育への応用について述べた. 以下, 第 I 部を構成する内容を, 章ごとに述べる. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ はそれぞれ, 有理整数環, 有理数体, 実数体, 複素数体とする.

第 1 章では, 第 2 章から第 4 章で必要な格子の一般的な理論について説明する. K を体, V を n 次元 K-計量ベクトル空間, R を K に含まれる環として, ベクトル空間 V において, 環 R 上で格子を定義する. また, 格子の判別式とその性質について述べる.

第 2 章では, 環 R を $\mathbb{Z}$ としたときの格子を考え, LLL 基底簡約について述べる. まず, 環 R 上で定義された格子を $\mathbb{Z}$ 上で考える. Minkowski 簡約基底と LLL 簡約基底についてまとめた. Minkowski 簡約基底の計算は, 基底ベクトルのノルムに関する条件が強く, 多項式時間の計算量では終了しない. そのため, 現実的には計算が困難であり, 計算機にのせるまで整備されていない. 従って, さらに弱い条件での簡約基底を求める必要がある. 実際使用されている LLL 簡約基底は, それ自身十分によい性質をもっており, 他の計算の初期の基底としても使用されており, 現在使われている基底簡約で代表的なものの 1 つである. この章の後半は. LLL 格子基底簡約の理論について概要をまとめる.

第 3 章では, 有限次代数体 F における整数環 $\mathcal{O}_F$ の最小元について論じる. 虚二次体以外の代数体の場合, $\mathcal{O}_F$ に関して 0 が集積点となり, 自由 $\mathcal{O}_F$-加群においても 0 が集積点となることを証明する. このことにより, いくらでも 0 に近い元が存在することがわかる. 本論文では, この証明を 2 通り与えている. 1 つは, ディリクレの同時近似定理を適用した証明 ([3]) である. もう 1 つは, 群論の結果を適用した証明である.

第 4 章では, 虚二次体 $F = \mathbb{Q}(\sqrt{m})$, $m < 0$ における整数環 $\mathcal{O}_F$ を考え, $\mathcal{O}_F$-格子における LLL 基底簡約について述べる. まず $\mathcal{O}_F$-格子を定義し, LLL 簡約基底を定義して, その性質について明らかにする ([3]). その後, 簡約基底の存在性について検討し, ガウスの数体 $\mathbb{Q}(\sqrt{-1})$ 上で常に簡約基底が存在するように, 擬 LLL 簡約基底を定義してその性質を明らかにする ([5]). さらに, この擬 LLL 簡約基底について, 基底簡約アルゴリズムが有限回の計算で終了することを証明する ([6]).

第 5 章では, 前章までで議論された, 格子基底簡約理論の教材化に向けて考察した一例

として, 格子のしきつめ問題について論じる.

第 II 部では, 2 次元の格子について考える. 格子の数学については [14], [16] 等で述べられている. これらの文献では, 格子多角形, 格子多面体や円周上の格子点の個数などについて述べられているが, 3 辺の長さが整数で面積も整数であるヘロン三角形については記述がない. そこで, 正方格子において, ヘロン三角形の頂点となる格子点の性質を考察し, そのような無限個の格子点を構成する方法を見い出した. また, 和算家である菊池長良の公式で直接的に表現できないヘロン三角形の例を挙げた. これらの話題に関連するピックの定理, 格子正多角形, 円周上の有理点の個数, トレミーの定理, 格子ヘロン三角形の教材化の可能性について論じた. 以下, 第 II 部を構成する内容を, 章ごとに述べる.

第 6 章では, ピックの定理とその教材化について論じる. また, 格子点を頂点とする正多角形は正方形に限ることの証明を紹介する. この定理は, 単に数学の古典理論であるばかりでなく, 教育の観点からは, その証明には背理法が適用されており, また, 知的好奇心を引き出す教材化の可能性を多分に含んでいる.

第 7 章では, 円周上にある有理点の個数についての古典的な結果を述べ, その教材化について述べる. 円周上にある有理点の個数は, $0, 1, 2, \infty$ であることが知られている. もし, 円周上の有理点が少なくとも 3 個見つかった場合, この円の中心も有理点となることが分かる. このことを用いた無限個の有理点が存在することの証明を紹介する. このとき, 有理点が n 個見つかっている円を, 適当に拡大すれば, n 個の格子点をのせた円周が存在することが分かる. 有理点が 3 個以上存在する円の中心が有理点となることの証明は, 中学校では連立方程式の学習, 高等学校では円の方程式の学習の範囲でも可能であることを指摘し, 教材化が可能であることを述べる. また, 与えられた個数の格子点をもつ円を見つけさせる活動なども「主体的・対話的で深い学び」につながる教材として考えられる.

第 8 章では, トレミーの定理について述べる. トレミーの定理は初等幾何学において有名な定理で, 多数の証明が知られている. この定理を適用して, 相互の距離がすべて有理数となるような無限個の点を含む円が存在することを証明する.

第 9 章では, ヘロン三角形の 3 辺の長さを与える公式として, 菊池長良や Carmichael のものがあるが, 和算家である菊池長良の公式では直接的に表現できないヘロン三角形について述べた. 和算の話題は中学校の教科書でも多数取り上げられており, 生徒にとっても馴染みやすい話題である. 和算の教材化については多くの研究があるが, ここではヘロン

三角形に関する和算の研究成果を教材化する可能性を示した.

第 10 章では, 相互の距離がすべて有理数となるような無限個の有理点を含む円が存在することについて述べる. この結果により, これらの無限個の点から任意に 3 点を選択し, 適当に拡大をすれば, ヘロン三角形の頂点である 3 点の格子点を含む円が存在することも証明されたことになる. また, 実際にヘロン三角形の頂点となる格子点の求め方を 2 つ見出した.

最後に, 研究のまとめと今後の課題について述べた. 著者らによる結果は, 学校教育において数学の授業で活用できる教材となり得る. 例えば, 図形のしきつめや三角形は小学校の算数で取りあげられる題材であり, ヘロン三角形はその定義もわかりやすく, 小学校から大人まで誰にでも親しめる教材となる. 本論文で考察した数学の内容は, これからの新しい時代に展開される「主体的・対話的で深い学び」を実現する授業づくりの題材となることを指摘した.

第I部

格子基底簡約とその教育への応用

第1章　格子の理論

本章では, 以後必要になる基礎理論について述べる. 具体的には, ベクトル空間や加群, 格子についてまとめる. すべて標準的な内容であるため文献は示さない.

1.1　ベクトル空間および加群

K を複素数体 $\mathbb{C}$ の部分体, R を K に含まれる環とする.

定義 1.1　集合 V が次の条件をみたすとき, V を K 上の**ベクトル空間** (vector space) という.

(I) $\boldsymbol{x}, \boldsymbol{y} \in V$ に対して**和**と呼ばれる第三の元 (これを$\boldsymbol{x}+\boldsymbol{y}$で表す) が定まり, 次の法則が成り立つ.

(1) $(\boldsymbol{x}+\boldsymbol{y})+\boldsymbol{z} = \boldsymbol{x}+(\boldsymbol{y}+\boldsymbol{z})$,

(2) $\boldsymbol{x}+\boldsymbol{y} = \boldsymbol{y}+\boldsymbol{x}$,

(3) **零ベクトル**と呼ばれる特別な元 (これを$\boldsymbol{0}$であらわす) がただ 1 つ存在し, V のすべての元 $\boldsymbol{x}$ に対して, $\boldsymbol{0}+\boldsymbol{x} = \boldsymbol{x}$ が成り立つ,

(4) V の任意の元 $\boldsymbol{x}$ に対し, $\boldsymbol{x}+\boldsymbol{x}' = \boldsymbol{0}$ となる V の元 $\boldsymbol{x}'$ がただ 1 つ存在する. これを $\boldsymbol{x}$ の**逆ベクトル**といい, $-\boldsymbol{x}$ で表す.

(II) V の任意の元 $\boldsymbol{x}$ と任意の K の元 a に対し, $\boldsymbol{x}$ の a 倍と呼ばれるもう 1 つの V の元 (これを $a\boldsymbol{x}$で表す) が定まり, 次の法則が成り立つ.

(5) $(a+b)\boldsymbol{x} = a\boldsymbol{x}+b\boldsymbol{x}$,

(6) $a(\boldsymbol{x}+\boldsymbol{y}) = a\boldsymbol{x}+a\boldsymbol{y}$,

(7) $(ab)\boldsymbol{x} = a(b\boldsymbol{x})$,

(8) $1\boldsymbol{x} = \boldsymbol{x}$.

定義 1.2　K 上のベクトル空間 V が, 次の条件を満たすとき, V を K 上の**計量ベクトル空間** (metric vector space) という.

$\boldsymbol{x}, \boldsymbol{y} \in V$ に対して, 内積と称する K の元 (これを $\boldsymbol{x} \cdot \boldsymbol{y}$ で表す) が定まり, 次の性質をもつ.

(1) $\boldsymbol{x} \cdot (\boldsymbol{y}_1 + \boldsymbol{y}_2) = \boldsymbol{x} \cdot \boldsymbol{y}_1 + \boldsymbol{x} \cdot \boldsymbol{y}_2$,

$(\boldsymbol{x}_1 + \boldsymbol{x}_2) \cdot \boldsymbol{y} = \boldsymbol{x}_1 \cdot \boldsymbol{y} + \boldsymbol{x}_2 \cdot \boldsymbol{y}$,

(2) $c \in K$ に対して, $(c\boldsymbol{x}) \cdot \boldsymbol{y} = c(\boldsymbol{x} \cdot \boldsymbol{y})$, $\boldsymbol{x} \cdot (c\boldsymbol{y}) = \overline{c}(\boldsymbol{x} \cdot \boldsymbol{y})$,

(3) $\boldsymbol{x} \cdot \boldsymbol{y} = \overline{\boldsymbol{y} \cdot \boldsymbol{x}}$,

(4) $\boldsymbol{x} \cdot \boldsymbol{x}$ は 0 または正の実数であり, $\boldsymbol{x} \cdot \boldsymbol{x} = 0$ となるのは, $\boldsymbol{x} = \boldsymbol{0}$ のときに限る.

以後, V を K 上の n 次元計量ベクトル空間とする.

定義 1.3　1 つの演算, 例えば乗法の定義された集合 G が**群** (group) であるとは, 次の 3 つの条件がみたされていることである.

(1) 結合法則 :　$(ab)c = a(bc)$,

(2) 単位元の存在 :　G の元 1 で, G の任意の元 x に対して $1x = x1 = x$ をみたすものが存在する,

(3) 逆元の存在 :　G の任意の元 a に対して $aa^{-1} = a^{-1}a = 1$ をみたす元 $a^{-1} \in G$ が存在する.

群 G において, さらに次の条件

(4) 交換法則 :　$ab = ba$,

が満たされているとき, G は**アーベル群** (abelian group) という.

定義 1.4　群 G の空でない部分集合 H が, 次の 2 つの条件

(1) $a, b \in H \Longrightarrow ab \in H$,

(2) $a \in H \Longrightarrow a^{-1} \in H$,

をみたすとき, H は G の**部分群** (subgroup) であるという.

命題 1.5　定義 1.4 の 2 つの条件をみたす部分群 H は, 群の定義を満たしている.

定義 1.6　S を G の部分集合とするとき, S のいくつかの元のべき積 $a_1^{n_1} \cdots a_n^{n_r} (a_i \in S, n_i \in \mathbb{Z})$ の全体は G の部分群である. これを $< S >$ で表し, S で**生成される部分群**という.

特に 1 つの元 a で生成される部分群

$$< a > \quad = \{\ a^n \mid n \in \mathbb{Z}\ \} \tag{1.1}$$

を**巡回群** (cyclic group) とよび, a をその**生成元** (generator) という.

定義 1.7　群 G がアーベル群のときは, その演算を加法の形でかくことが多い. このとき G を**加法群** (additive group) とよび, その単位元を**零元**とよんで, 0 で表す. また, G の元 a の逆元を $-a$ で表す.

定義 1.8　R を環, M を加法群とし, 写像 $f : R \times M \to M$ が与えられているとする. いま $(r, m) \in R \times M$ の f による像を rm とかくことにし, これが次の条件をみたすとき M は R-**左加群**であるという.

(1) $r(m + m') = rm + rm'$,

(2) $(r + r')m = rm + r'm$,

(3) $(rr')m = r(r'm)$,

(4) $1m = m$.

ただし $r, r', 1 \in R,\ m, m' \in M$ とする.

R-右加群も同様に定義される. R が可換環のときは, R-左加群は自然に R-右加群と考えられる. この場合, 単に R-**加群** (R-module) という.

ここで, R は複素数体 $\mathbb{C}$ に含まれる環だから, 可換環である. 従って, R-左加群, R-右加群を区別しない.

定義 1.9　M を R-加群とする. 有限集合 $U = \{u_1, \cdots, u_n\} \subset M$ に対して, 次の 2 つの条件

$$(1) \quad \sum_{i=1}^{n} r_i u_i = 0\ (r_i \in R) \quad \Longrightarrow \quad r_i = 0\ (i = 1, \cdots, n), \tag{1.2}$$

$$(2) \quad M = \sum_{u \in U} Ru, \tag{1.3}$$

をみたすとき, M は R-**自由加群** (R-free module) といい, U を R-自由加群の**基底** (basis) とよぶ. また, U の元の個数を M の (R-自由加群としての) **階数** (rank) とよぶ.

1.2 格子

定義 1.10 Λ を R-加群とする. このとき, Λ が V 内における **格子**(lattice) であるとは, ある V のベクトル空間としての基底 $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ で,

$$\Lambda = R\boldsymbol{b}_1 + \cdots + R\boldsymbol{b}_n = \left\{ \sum_{i=1}^{n} r_i \boldsymbol{b}_i \;\middle|\; r_i \in R \ (1 \leq i \leq n) \right\} \tag{1.4}$$

を満たすものが存在することをいう. ここで, 1 つの基底を構成する n 個のベクトルの順序も考える.

定義 1.10 において, 有限集合 $U = \{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\} \subset \Lambda$ とすれば, 定義 1.9 の (1.2), (1.3) を満たすから, 次の命題を得る.

命題 1.11 格子 Λ は R-自由加群である.

定義 1.12 格子 Λ の R-自由加群としての基底 $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ を格子の**基底**とよぶ. また, 1 つの基底におけるベクトルの個数を, 格子 Λ の**階数** (rank) といい, rank Λ で表す.

以後, 格子 Λ の基底全体の集合を $\mathcal{B}_\Lambda$ で表す. 基底の選び方は一通りではないことを注意しておく. 以後 $K = \mathbb{R}$ または $\mathbb{C}$ とする.

定義 1.13 $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \in \mathcal{B}_\Lambda$ に対して,

$$d(\Lambda) := \sqrt{|\det(\boldsymbol{b}_i \cdot \boldsymbol{b}_j)|} \tag{1.5}$$

を Λ の **判別式**(discriminant) という. ここで $\cdot$ は 2 つのベクトルの内積を表す. $\det(\boldsymbol{b}_i \cdot \boldsymbol{b}_j)$ は, (i, j) 成分が $\boldsymbol{b}_i$, $\boldsymbol{b}_j$ の内積である n 次正方行列の行列式である.

以後, $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \in \mathcal{B}_\Lambda$ とする.

命題 1.14 次が成立する.

$$d(\Lambda) = |\det(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)| \tag{1.6}$$

が成り立つ. ここで $\det(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ は, $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ を横に並べてできる n 次正方行列の行列式である.

命題 1.15　次が成立する (アダマールの不等式).

$$|\det(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)| \leq \prod_{i=1}^{n} \|\boldsymbol{b}_i\| \tag{1.7}$$

ただし, 行列 $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ が正則のときには, 等号は $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ がたがいに直交するときのみ成立する.

注 1.16　命題 1.15 において, (1.7) の不等式は, $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ が基底でなくても成立する. また, これらは格子 Λ の元でなくても, ベクトル空間 V の元であれば成立する.

以後, $K = \mathbb{R}$ とする.

定義 1.17　$(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \in \mathcal{B}_\Lambda$ に対して,

$$\Pi(\Lambda) := \left\{ \sum_{i=1}^{n} x_i \boldsymbol{b}_i \;\middle|\; 0 \leq x_i < 1 \right\} \tag{1.8}$$

を Λ の**基本平行体**という.

第2章　実数体における格子基底簡約

本章では, すでに明らかにされている格子基底簡約の理論を述べる. 簡約基底として, Minkowski 簡約基底および LLL 簡約基底がその代表例である. これらの基底の定義や例および性質を述べる. 特に, A.K.Lenstra, et al.([15]) による LLL 基底簡約の理論についてはそのアルゴリズムを最後に述べる. 既知の理論であるため, 証明を省略したものもある. 第 1 章における体 K は $\mathbb{R}$, 環 R は $\mathbb{Z}$ とする.

2.1　格子の定義

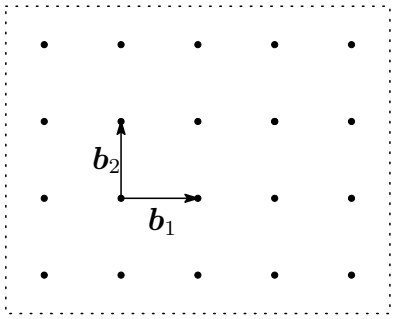
定義 2.1　定義 1.10 はこの場合, 次のようになる.
Λ を $\mathbb{Z}$-加群 (module) とする. このとき, Λ が $\mathbb{R}^n$ 内における **格子**(lattice) であるとは, ある $\mathbb{R}^n$ のベクトル空間としての基底 $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ で,

$$\Lambda = \mathbb{Z}\boldsymbol{b}_1 + \cdots + \mathbb{Z}\boldsymbol{b}_n = \left\{ \sum_{i=1}^{n} r_i \boldsymbol{b}_i \;\middle|\; r_i \in \mathbb{Z}\ (1 \leq i \leq n) \right\} \tag{2.1}$$

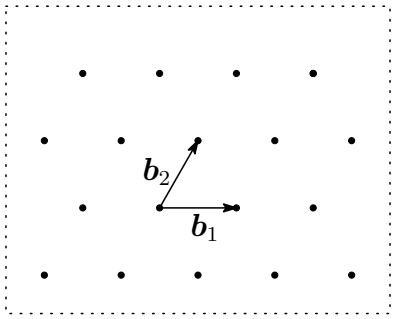
を満たすものが存在することをいう.

第 1 章と同様に, Λ の基底全体の集合を $\mathcal{B}_\Lambda$ で表す. また, 1 つの基底を構成する n 個のベクトルの順序も考える.

例 2.2　$n = 2$ のときの例を 2 つ挙げる.　このとき $\Lambda = \mathbb{Z}\boldsymbol{b}_1 + \mathbb{Z}\boldsymbol{b}_2$ と表され, 基底となる 2 つのベクトルはそれぞれ以下のようである :



正方格子 $\boldsymbol{b}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\boldsymbol{b}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$



六角格子 $\boldsymbol{b}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\boldsymbol{b}_2 = \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix}$

基底の選び方は一通りではないことを注意しておく.

2.2 最短ベクトル問題

格子内の最小ベクトルの 1 つ, また, より一般的に, 一定の定数以下のノルムをもつベクトルを見つける問題が重要である. ここでは, 最短ベクトル問題を定義する.

定義 2.3 n 個の線形独立なベクトル $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n \in \mathbb{R}^n$ に対して, これらのベクトルで生成される格子 $\Lambda = \mathbb{Z}\boldsymbol{b}_1 + \cdots + \mathbb{Z}\boldsymbol{b}_n$ のなかで, ノルムが 0 以外の最短なベクトルを求める問題を**最短ベクトル問題** (shortest vector problem, SVP) という.

この最短ベクトル問題を解く多項式時間アルゴリズムは知られておらず, この問題は, 格子についての計算量困難な問題の 1 つとしてよく知られている ([7]). 後で述べる格子基底簡約は, 最短ベクトル問題を効率的に解くための 1 つの方法となる.

2.3 格子における簡約基底

ここで, 格子 Λ の特別な性質を持つ基底について考える. 最短ベクトル問題へのアプローチの観点から, ノルムの小さいベクトルからなる基底について考えていく. このような基底の代表例である, Minkowski 簡約基底および LLL 簡約基底について述べる.

2.3.1 Minkowski 簡約基底

ベクトルのノルムによって, $\mathbb{R}^n$ のベクトルの順序をつけることは, 基底の集合上の半順序を導く.

定義 2.4 [*23*, (3.18a), p191] $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{R}^n$ に対して,

$$\boldsymbol{a} < \boldsymbol{b} \ :\Longleftrightarrow\ \|\boldsymbol{a}\| < \|\boldsymbol{b}\| \tag{2.2}$$

と定義する. ここで $\|\cdot\|$ はベクトルの長さ (ノルム) である.

これは次の定義により, n 次元の格子 Λ のすべての基底の集合上で半順序を引き起こす:

定義 2.5 [*23*, (3.18b), p191] 2 つの基底 $(\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n), (\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \in \mathcal{B}_\Lambda$ に対して,

$(\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n) < (\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) :\Longleftrightarrow$ ある番号 $j (1 \leq j \leq n)$ が存在し, $1 \leq i \leq j-1$ をみたす

任意の i に対して, $\|\boldsymbol{a}_i\| = \|\boldsymbol{b}_i\|$ かつ $\|\boldsymbol{a}_j\| < \|\boldsymbol{b}_j\|$ (2.3)

と定義する.

定義 2.5 で定義した順序 "<"は, $\boldsymbol{a}_1\boldsymbol{a}_2\cdots\boldsymbol{a}_n$ を単語とみなしたときの, ノルムの大きさに関する辞書式順序である.

定義 2.6 [*23*, Def(3.18c), p191] 格子 Λ の基底全体の集合において, $<$ に関しての極小元を **Minkowski 簡約基底** (Minkowski reduced basis) と呼ぶ.

以後, Minkowski 簡約基底全体の集合を $\mathcal{M}_\Lambda$ で表す.

注 2.7 [*23*, p191] Minkowski 簡約基底は一意には決まらない. 例えば, すべての $\pi \in \mathfrak{S}_n$(n 個の元の対称群) に対して $(\boldsymbol{e}_{\pi(1)}, \cdots, \boldsymbol{e}_{\pi(n)}) \in \mathcal{M}_{\mathbb{Z}^n}$ である. ここで $\boldsymbol{e}_i (i = 1, \cdots, n)$ は第 i 成分のみが 1 で他はすべて 0 である単位ベクトルである.

具体的に, 階数が 2 の場合の Minkowski 簡約基底の例を示す.

例 2.8 (正方格子の Minkowski 簡約基底)

$\Lambda = \mathbb{Z}\boldsymbol{b}_1 + \mathbb{Z}\boldsymbol{b}_2,\ \boldsymbol{b}_1 = (1,0),\ \boldsymbol{b}_2 = (0,1)$ のとき,

$$\mathcal{M}_\Lambda = \{(\boldsymbol{b}_1, \boldsymbol{b}_2), (\boldsymbol{b}_1, -\boldsymbol{b}_2), (-\boldsymbol{b}_1, \boldsymbol{b}_2), (-\boldsymbol{b}_1, -\boldsymbol{b}_2), (\boldsymbol{b}_2, \boldsymbol{b}_1), (\boldsymbol{b}_2, -\boldsymbol{b}_1), (-\boldsymbol{b}_2, \boldsymbol{b}_1), (-\boldsymbol{b}_2, -\boldsymbol{b}_1)\} \tag{2.4}$$

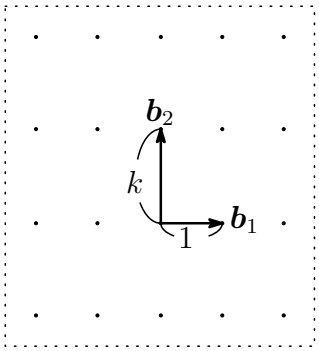
である.

例 2.9 (長方格子の Minkowski 簡約基底)

$\Lambda = \mathbb{Z}\boldsymbol{b}_1 + \mathbb{Z}\boldsymbol{b}_2,\ \boldsymbol{b}_1 = (1,0),\ \boldsymbol{b}_2 = (0,k),\ 1 < k$ のとき,

$$\mathcal{M}_\Lambda = \{(\boldsymbol{b}_1, \boldsymbol{b}_2), (\boldsymbol{b}_1, -\boldsymbol{b}_2), (-\boldsymbol{b}_1, \boldsymbol{b}_2), (-\boldsymbol{b}_1, -\boldsymbol{b}_2)\} \tag{2.5}$$

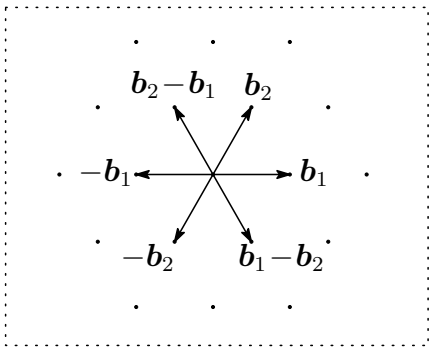
である.



例 2.10 (六角格子の Minkowski 簡約基底)

$\Lambda = \mathbb{Z}\boldsymbol{b}_1 + \mathbb{Z}\boldsymbol{b}_2,\ \boldsymbol{b}_1 = (1,0),\ \boldsymbol{b}_2 = (1/2, \sqrt{3}/2)$ のとき,

6 つのベクトル $\boldsymbol{b}_1, -\boldsymbol{b}_1, \boldsymbol{b}_2, -\boldsymbol{b}_2, \boldsymbol{b}_1 - \boldsymbol{b}_2, \boldsymbol{b}_2 - \boldsymbol{b}_1$ のなかから, 線形独立となるように任意に選んだベクトル列に限り, Minkowski 簡約基底となる.



Minkowski 簡約基底について, 本質的に違うものがあるかどうかは不明である. また, 次の性質がある.

命題 2.11　格子 Λ に対して, $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \in \mathcal{M}_\Lambda$ ならば

$$\|\boldsymbol{b}_1\| \leq \cdots \leq \|\boldsymbol{b}_n\| \tag{2.6}$$

が成立する.

定義 2.12　Λ の部分集合 S に対して, $S \setminus \{\mathbf{0}\}$ の最小元の集合を Min S で表す. すなわち

$$\text{Min } S := \{\boldsymbol{y} \in S \mid \boldsymbol{y} \neq \mathbf{0}, \|\boldsymbol{y}\| \leq \|\boldsymbol{x}\| \text{ for } {}^\forall \boldsymbol{x} \in S, \boldsymbol{x} \neq \mathbf{0}\} \tag{2.7}$$

とする.

定義 2.13　$\boldsymbol{x}_1, \cdots, \boldsymbol{x}_n \in \Lambda$ とする. Λ に対して, $\boldsymbol{x}_1 \in \text{Min } \Lambda$, $\boldsymbol{x}_i \in \text{Min } (\Lambda \setminus (\mathbb{Z}\boldsymbol{x}_1 + \cdots + \mathbb{Z}\boldsymbol{x}_{i-1}))$ $(i = 2, \cdots, n)$ と仮定し, $M_i := \|\boldsymbol{x}_i\|^2$ とおく. このとき $(M_1, \cdots, M_n)$ を Λ の**逐次最小** (successive minima) という.

定義 2.13 において, $\boldsymbol{x}_i$ $(i = 1, \cdots, n)$ は, $\boldsymbol{x}_1, \cdots, \boldsymbol{x}_{i-1}$ と線形独立になるベクトルのなかで, ノルムが最短となるベクトルである. 以下に長方格子における逐次最小の例を挙げる.

例 2.14 (長方格子の逐次最小)　$\Lambda = \mathbb{Z}\boldsymbol{b}_1 + \mathbb{Z}\boldsymbol{b}_2$, $\boldsymbol{b}_1 = (1, 0), \boldsymbol{b}_2 = (0, k)$, $1 < k$ のとき, Min $\Lambda = \{\boldsymbol{b}_1, -\boldsymbol{b}_1\}$ であり, 定義 2.13 における $\boldsymbol{x}_1$ を $\boldsymbol{b}_1$ とすると, $M_1 = \|\boldsymbol{x}_1\|^2 = 1$ である ($\boldsymbol{x}_1$を$-\boldsymbol{b}_1$としても同様).
Min $(\Lambda \setminus \mathbb{Z}\boldsymbol{b}_1) = \{\boldsymbol{b}_2, -\boldsymbol{b}_2\}$ だから, $\boldsymbol{x}_2$ を $\boldsymbol{b}_2$ とすると, $M_2 = \|\boldsymbol{x}_2\|^2 = k^2$ である ($\boldsymbol{x}_2$を$-\boldsymbol{b}_2$としても同様). 従って Λ の逐次最小は $(1, k^2)$ である.

注 2.15 [*23*, (3.31), p195]　格子 Λ の逐次最小を与えるベクトル列は, 基底となるとは限らない. 例えば, $\Lambda = \mathbb{Z}\boldsymbol{b}_1 + \mathbb{Z}\boldsymbol{b}_2 + \mathbb{Z}\boldsymbol{b}_3 + \mathbb{Z}\boldsymbol{b}_4 + \mathbb{Z}\boldsymbol{b}_5$, $\boldsymbol{b}_1 = (1, 0, 0, 0, 0), \boldsymbol{b}_2 = (0, 1, 0, 0, 0), \boldsymbol{b}_3 = (0, 0, 1, 0, 0), \boldsymbol{b}_4 = (0, 0, 0, 1, 0), \boldsymbol{b}_5 = (1/2, 1/2, 1/2, 1/2, 1/2)$ のとき, $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4, \boldsymbol{b}_5) \in \mathcal{M}_\Lambda$ である. 一方, 逐次最小となるベクトル列は $\boldsymbol{x}_1 = \boldsymbol{b}_1, \boldsymbol{x}_2 = \boldsymbol{b}_2, \boldsymbol{x}_3 = \boldsymbol{b}_3, \boldsymbol{x}_4 = \boldsymbol{b}_4, \boldsymbol{x}_5 = 2\boldsymbol{b}_5 - \boldsymbol{b}_4 - \boldsymbol{b}_3 - \boldsymbol{b}_2 - \boldsymbol{b}_1$ となり, $M_1 = \cdots = M_5 = 1$ である. ところが, $(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{x}_4, \boldsymbol{x}_5) \notin \mathcal{B}_\Lambda$ である.

補題 2.16　$(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \in \mathcal{M}_\Lambda$ とする. $1 \leq r \leq n-1$ をみたす r を固定して, $\boldsymbol{b}_i \in \mathrm{Min}\ (\Lambda \setminus (\mathbb{Z}\boldsymbol{b}_1 + \cdots + \mathbb{Z}\boldsymbol{b}_{i-1}))(i = 1, \cdots, r)$, $x_1\boldsymbol{b}_1 + \cdots + x_n\boldsymbol{b}_n \in \mathrm{Min}\ (\Lambda \setminus (\mathbb{Z}\boldsymbol{b}_1 + \cdots + \mathbb{Z}\boldsymbol{b}_r)), d := \gcd(x_{r+1}, \cdots, x_n)$ としたとき, 次が成立する.

(1)　$d = 1$ ならば,

$$\boldsymbol{b}_{r+1} \in \mathrm{Min}\ (\Lambda \setminus (\mathbb{Z}\boldsymbol{b}_1 + \cdots + \mathbb{Z}\boldsymbol{b}_r)), \tag{2.8}$$

(2)　$d \neq 1$ ならば,

$$M_{r+1} \leq \frac{r}{3} M_r, \tag{2.9}$$

ここで $(M_1, \cdots, M_n)$ は定義 2.13 で定義した Λ の逐次最小である.

この補題 2.16 より, 次の命題を得る.

命題 2.17　$1 \leq n \leq 3$ のとき, $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \in \mathcal{M}_\Lambda$ ならば, $\boldsymbol{b}_i \in \mathrm{Min}\ (\Lambda \setminus (\mathbb{Z}\boldsymbol{b}_1 + \cdots + \mathbb{Z}\boldsymbol{b}_{i-1}))(i = 1, \cdots, n)$ である.

命題 2.18　$\boldsymbol{b}_1 \in \mathrm{Min}\ \Lambda$, $\boldsymbol{b}_i \in \mathrm{Min}\ (\Lambda \setminus (\mathbb{Z}\boldsymbol{b}_1 + \cdots + \mathbb{Z}\boldsymbol{b}_{i-1}))$ $(i = 2, \cdots, n)$ かつ $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \in \mathcal{B}_\Lambda$ ならば $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \in \mathcal{M}_\Lambda$ である.

証明　$(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \notin \mathcal{M}_\Lambda$ と仮定すると, $(\boldsymbol{c}_1, \cdots, \boldsymbol{c}_n) \in \mathcal{M}_\Lambda$ で,

$$(\boldsymbol{c}_1, \cdots, \boldsymbol{c}_n) < (\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \tag{2.10}$$

となるものが存在する. このとき $\|\boldsymbol{c}_j\| = \|\boldsymbol{b}_j\|$ $(j = 1, \cdots, n)$ であることを, 以下で示すことにより, (2.10) に矛盾することを導く.

(2.10) より, $\|\boldsymbol{c}_1\| \leq \|\boldsymbol{b}_1\|$ である. 一方 $\boldsymbol{b}_1 \in \mathrm{Min}\ \Lambda$ だから $\|\boldsymbol{b}_1\| \leq \|\boldsymbol{c}_1\|$ である. 従って $\|\boldsymbol{c}_1\| = \|\boldsymbol{b}_1\|$ である.

次に, $k > 1$ に対して $\|\boldsymbol{c}_i\| = \|\boldsymbol{b}_i\|$ $(i = 1, \cdots, k-1)$ が成立するとき, $\|\boldsymbol{c}_k\| = \|\boldsymbol{b}_k\|$ となることを以下で示す. (2.10) より, $\|\boldsymbol{c}_k\| \leq \|\boldsymbol{b}_k\|$ である. いま $\|\boldsymbol{c}_k\| < \|\boldsymbol{b}_k\|$ とすると,

$$\boldsymbol{b}_k \in \mathrm{Min}\ (\Lambda \setminus (\mathbb{Z}\boldsymbol{b}_1 + \cdots + \mathbb{Z}\boldsymbol{b}_{k-1})) \tag{2.11}$$

より, $\boldsymbol{c}_k \in \mathbb{Z}\boldsymbol{b}_1 + \cdots + \mathbb{Z}\boldsymbol{b}_{k-1}$ である.

もし, $\boldsymbol{c}_1, \cdots, \boldsymbol{c}_k \in \mathbb{Z}\boldsymbol{b}_1 + \cdots + \mathbb{Z}\boldsymbol{b}_{k-1}$ とすると, 階数の関係から, $\boldsymbol{c}_1, \cdots, \boldsymbol{c}_k$ は線形従属となる. 従って, ある r $(1 \leq r < k)$ に対して $\boldsymbol{c}_r \notin \mathbb{Z}\boldsymbol{b}_1 + \cdots + \mathbb{Z}\boldsymbol{b}_{k-1}$, すなわち

$\boldsymbol{c}_r \in \Lambda \backslash (\mathbb{Z}\boldsymbol{b}_1 + \cdots + \mathbb{Z}\boldsymbol{b}_{k-1})$ となるものが存在する. これと (2.11) より $\|\boldsymbol{b}_k\| \leq \|\boldsymbol{c}_r\|$ である. 従って, $\|\boldsymbol{c}_k\| < \|\boldsymbol{b}_k\| \leq \|\boldsymbol{c}_r\|$ となり, $\|\boldsymbol{c}_k\| < \|\boldsymbol{c}_r\|$ である. 一方, $(\boldsymbol{c}_1, \cdots, \boldsymbol{c}_n) \in \mathcal{M}_\Lambda$, $r < k$ だから, 命題 2.11 より, $\|\boldsymbol{c}_r\| \leq \|\boldsymbol{c}_k\|$ である. これは, $\|\boldsymbol{c}_k\| < \|\boldsymbol{c}_r\|$ に矛盾する. 従って, $\|\boldsymbol{c}_k\| = \|\boldsymbol{b}_k\|$ が示された.

以上により, $\|\boldsymbol{c}_j\| = \|\boldsymbol{b}_j\|$ $(j = 1, \cdots, n)$ であるが, これははじめの仮定 (2.10) に反する. 従って, $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \in \mathcal{M}_\Lambda$ である. ■

2.3.2 LLL 簡約基底

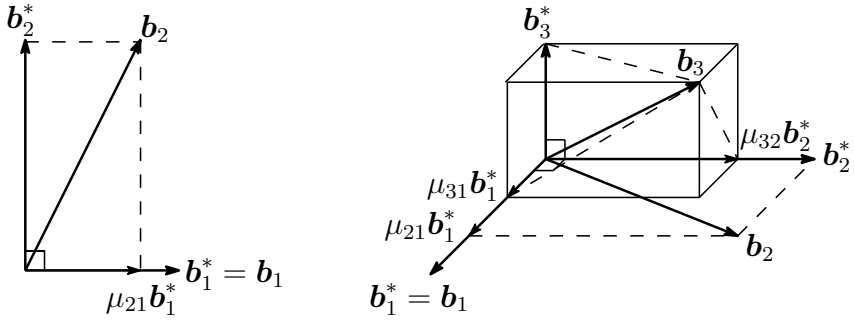
定義 2.6 で述べた, 格子の Minkowski 簡約基底のは, 2 つの基底の大小を, 各基底のベクトル列を単語とする辞書式順序で判断するため, 多項式時間の計算量では終了しない. そのため, 現実的には計算が困難であり, 計算機にのせるまで整備されていない. ゆえに, さらに弱い条件での基底簡約を求める必要がある. これから定義する LLL 簡約基底は, それ自身十分によい性質をもっている. この基底は, 現在使われている基底簡約のアルゴリズムで重要なものであり, A.K.Lenstra, et al. によって開発された. この論文では, アルゴリズムの応用例として, 有理整数係数をもつ多項式の因子分解についても紹介されている ([15]).

定義 2.19 $\Lambda = \mathbb{Z}\boldsymbol{b}_1 + \cdots + \mathbb{Z}\boldsymbol{b}_n$ とする. Λ の基底 $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ に対して,

$$\boldsymbol{b}_i^* := \boldsymbol{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \boldsymbol{b}_j^*, \quad \mu_{ij} := \frac{\boldsymbol{b}_i \cdot \boldsymbol{b}_j^*}{\boldsymbol{b}_j^* \cdot \boldsymbol{b}_j^*} \quad (1 \leq j < i \leq n) \tag{2.12}$$

とすると (Gram-Schmidt の直交化法).

例 2.20 定義 2.19 において, $n = 2$ のとき $\boldsymbol{b}_1^*, \boldsymbol{b}_2^*$ が, $n = 3$ のとき $\boldsymbol{b}_1^*, \boldsymbol{b}_2^*, \boldsymbol{b}_3^*$ が, 次の図のように順次決定される.



定義 2.21　$\Lambda = \mathbb{Z}\boldsymbol{b}_1 + \cdots + \mathbb{Z}\boldsymbol{b}_n$ とする. Λ の基底 $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ が **LLL 簡約基底**であるとは, 定義 2.19 における, 直交基底におけるベクトル $\boldsymbol{b}_1^*, \cdots, \boldsymbol{b}_n^*$ が次を満たすときである :

$$|\mu_{ij}| \leq \frac{1}{2} \quad (1 \leq j < i \leq n), \tag{2.13}$$

$$\|\boldsymbol{b}_i^* + \mu_{i,i-1}\boldsymbol{b}_{i-1}^*\|^2 \geq \frac{3}{4}\|\boldsymbol{b}_{i-1}^*\|^2. \tag{2.14}$$

以後, Λ の LLL 簡約基底全体の集合を $\mathcal{L}_\Lambda$ で表す.

注 2.22 [23, p200]　定義 2.21 の式 (2.14) における定数 $\frac{3}{4}$ は, $\frac{1}{4} < \alpha < 1$ を満たす任意の α で置き換えることができる. このとき, 後から述べる命題 2.28 などの評価は適切に変更しなければならない.

定数 α が大きいと LLL 簡約基底としての性質は良くなるが, 簡約基底の計算のための計算量も増える.

例 2.23　$n = 2$ のとき定義 2.21 は次の不等式で表せる :

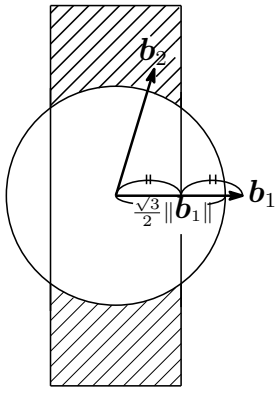
(2.13) 式については

$$|\mu_{21}| \leq \frac{1}{2}, \tag{2.15}$$

(2.14) 式については, 定義 2.19 (Gram-Schmidt の直交化法) より $\boldsymbol{b}_1^* = \boldsymbol{b}_1$, $\boldsymbol{b}_2^* = \boldsymbol{b}_2 - \mu_{21}\boldsymbol{b}_1^* = \boldsymbol{b}_2 - \mu_{21}\boldsymbol{b}_1$ であるから, $\boldsymbol{b}_2^* + \mu_{21}\boldsymbol{b}_1^* = (\boldsymbol{b}_2 - \mu_{21}\boldsymbol{b}_1) + \mu_{21}\boldsymbol{b}_1 = \boldsymbol{b}_2$ である. 従って

$$\|\boldsymbol{b}_2\|^2 \geq \frac{3}{4}\|\boldsymbol{b}_1\|^2, \quad \text{すなわち} \quad \|\boldsymbol{b}_2\| \geq \frac{\sqrt{3}}{2}\|\boldsymbol{b}_1\| \tag{2.16}$$

となる. (2.15), (2.16) 式より, 簡約基底 $(\boldsymbol{b}_1, \boldsymbol{b}_2)$ において, $\boldsymbol{b}_1$ と $\boldsymbol{b}_2$ を図示すると次のようになる. $\boldsymbol{b}_2$ の終点が図の斜線部分（帯状領域）に存在している.



$n = 2$ のときの $\boldsymbol{b}_2$ のとり得る範囲

上の図において, 帯状領域は上下方向に無限に伸びている. これより, ただちに次の例が得られる.

例 2.24 (正方格子の LLL 簡約基底)
$\Lambda = \mathbb{Z}\boldsymbol{b}_1 + \mathbb{Z}\boldsymbol{b}_2,\ \boldsymbol{b}_1 = (1,0),\ \boldsymbol{b}_2 = (0,1)$ のとき,

$$\mathcal{L}_\Lambda = \{(\boldsymbol{b}_1, \boldsymbol{b}_2), (\boldsymbol{b}_1, -\boldsymbol{b}_2), (-\boldsymbol{b}_1, \boldsymbol{b}_2), (-\boldsymbol{b}_1, -\boldsymbol{b}_2), (\boldsymbol{b}_2, \boldsymbol{b}_1), (\boldsymbol{b}_2, -\boldsymbol{b}_1), (-\boldsymbol{b}_2, \boldsymbol{b}_1), (-\boldsymbol{b}_2, -\boldsymbol{b}_1)\} \tag{2.17}$$

である. 従って, $\mathcal{M}_\Lambda = \mathcal{L}_\Lambda$ である.

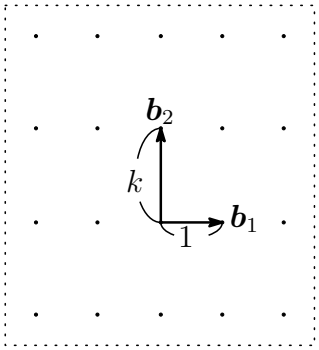
例 2.25 (長方格子の LLL 簡約基底)
$\Lambda = \mathbb{Z}\boldsymbol{b}_1 + \mathbb{Z}\boldsymbol{b}_2,\ \boldsymbol{b}_1 = (1,0),\ \boldsymbol{b}_2 = (0,k),\ 1 < k$ のとき,
(1) $k \leq \frac{2}{\sqrt{3}}$ のとき,

$$\mathcal{L}_\Lambda = \{(\boldsymbol{b}_1, \boldsymbol{b}_2), (\boldsymbol{b}_1, -\boldsymbol{b}_2), (-\boldsymbol{b}_1, \boldsymbol{b}_2), (-\boldsymbol{b}_1, -\boldsymbol{b}_2), (\boldsymbol{b}_2, \boldsymbol{b}_1), (\boldsymbol{b}_2, -\boldsymbol{b}_1), (-\boldsymbol{b}_2, \boldsymbol{b}_1), (-\boldsymbol{b}_2, -\boldsymbol{b}_1)\} \tag{2.18}$$

である. 従って, $\mathcal{M}_\Lambda \subsetneq \mathcal{L}_\Lambda$ である.
(2) $\frac{2}{\sqrt{3}} < k$ のとき,

$$\mathcal{L}_\Lambda = \{(\boldsymbol{b}_1, \boldsymbol{b}_2), (\boldsymbol{b}_1, -\boldsymbol{b}_2), (-\boldsymbol{b}_1, \boldsymbol{b}_2), (-\boldsymbol{b}_1, -\boldsymbol{b}_2)\} \tag{2.19}$$

である. 従って, $\mathcal{M}_\Lambda = \mathcal{L}_\Lambda$ である.



Minkowski 簡約基底と LLL 簡約基底の関係について, rank $\Lambda = 2$ のときには次の命題が得られる.

命題 2.26 rank $\Lambda = 2$ のとき, 次が成立する.

$$\mathcal{M}_\Lambda \subseteq \mathcal{L}_\Lambda. \tag{2.20}$$

証明　$(\boldsymbol{b}_1, \boldsymbol{b}_2) \in \mathcal{B}_\Lambda$ とする. このとき, 命題 2.17 と命題 2.18 により,

$$(\boldsymbol{b}_1, \boldsymbol{b}_2) \in \mathcal{M}_\Lambda \iff \boldsymbol{b}_1 \in \mathrm{Min}\ \Lambda,\ \boldsymbol{b}_2 \in \mathrm{Min}\ (\Lambda \setminus \mathbb{Z}\boldsymbol{b}_1) \tag{2.21}$$

である. まず, $\boldsymbol{b}_1 \in \mathrm{Min}\ \Lambda,\ \boldsymbol{b}_2 \in \mathrm{Min}\ (\Lambda \setminus \mathbb{Z}\boldsymbol{b}_1)$ のとき, (2.15) が成り立つことを以下で証明する.

$\mu_{21} > \frac{1}{2}$ かつ $\boldsymbol{b}_1 \in \mathrm{Min}\ \Lambda$ のとき, $\|\boldsymbol{b}_2 - \boldsymbol{b}_1\|^2 < \|\boldsymbol{b}_2\|^2$ であり, $\boldsymbol{b}_2 \notin \mathrm{Min}\ (\Lambda \setminus \mathbb{Z}\boldsymbol{b}_1)$ となる. また, $\mu_{21} < -\frac{1}{2}$ かつ $\boldsymbol{b}_1 \in \mathrm{Min}\ \Lambda$ のとき, 同様に $\|\boldsymbol{b}_1 + \boldsymbol{b}_2\|^2 < \|\boldsymbol{b}_2\|^2$ であり, $\boldsymbol{b}_2 \notin \mathrm{Min}\ (\Lambda \setminus \mathbb{Z}\boldsymbol{b}_1)$ となる. 従って, $|\mu_{21}| \leq \frac{1}{2}$ が得られる.

(2.16) が成り立つことについては, 命題 2.11 より, $(\boldsymbol{b}_1, \boldsymbol{b}_2) \in \mathcal{M}_\Lambda$ ならば, $\|\boldsymbol{b}_1\|^2 \leq \|\boldsymbol{b}_2\|^2$ だから, $\frac{3}{4}\|\boldsymbol{b}_1\|^2 \leq \|\boldsymbol{b}_2\|^2$ が得られる. ■

次に, Λ の基底が与えられたときに, Λ の元のノルムについて, 次の命題が得られる. この命題の証明では, 本質的には, 0 でない有理整数環 $\mathbb{Z}$ の任意の元の絶対値が 1 以上であること, すなわち, 最小元が存在していることが重要である.

命題 2.27 [*15*, p518]
$(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \in \mathcal{B}_\Lambda$ とする. また, $\boldsymbol{b}_i^*\ (i = 1, 2, \cdots, n)$ は定義 2.19 で定義した通りとする. このとき, $\boldsymbol{0} \neq {}^\forall\boldsymbol{x} \in \Lambda$ に対して,

$$\|\boldsymbol{x}\|^2 \geq \|\boldsymbol{b}_i^*\|^2 \quad \text{for } {}^\exists i \leq n. \tag{2.22}$$

ただし i は $\boldsymbol{x} = \sum_{j=1}^n r_j\boldsymbol{b}_j\ (r_j \in \mathbb{Z})$ と表したときの, $r_j \neq 0$ を満たす最大の j である.

次に, LLL 簡約基底においてノルムについての重要な性質を述べる.

命題 2.28 [*15*, p517 − 518]　$(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \in \mathcal{L}_\Lambda$ とする. また, $\boldsymbol{b}_i^*\ (i = 1, 2, \cdots, n),\ \mu_{ij}$ は定義 2.19 で定義した通りとする. このとき次が成立する :

$$(1) \quad \|\boldsymbol{b}_j\|^2 \leq 2^{i-1}\|\boldsymbol{b}_i^*\|^2 \ \ (1 \leq j \leq i \leq n), \tag{2.23}$$

$$(2) \quad d(\Lambda) \leq \prod_{i=1}^n \|\boldsymbol{b}_i\| \leq 2^{\frac{n(n-1)}{4}} d(\Lambda), \tag{2.24}$$

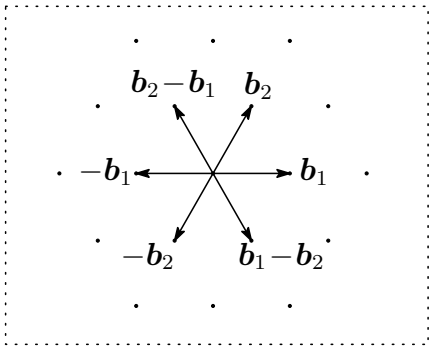
(3) $\|\boldsymbol{b}_1\| \leq 2^{\frac{n-1}{4}} d(\Lambda)^{\frac{1}{n}}$, (2.25)

(4) $\|\boldsymbol{b}_1\|^2 \leq 2^{n-1}\|\boldsymbol{x}\|^2$ for $^\forall \boldsymbol{x} \in \Lambda,\ \boldsymbol{x} \neq \boldsymbol{0}$, (2.26)

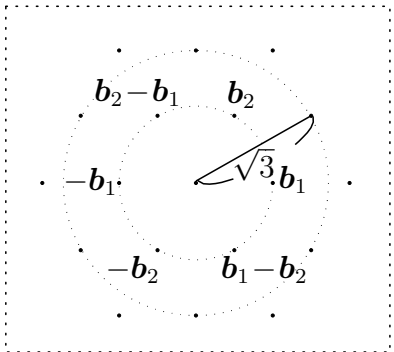
(5) $\|\boldsymbol{b}_j\|^2 \leq 2^{n-1}\max\{\|\boldsymbol{x}_1\|^2, \cdots, \|\boldsymbol{x}_t\|^2\}$ ($1 \leq j \leq t \leq n$ で, $\boldsymbol{x}_1, \cdots, \boldsymbol{x}_t$ は線型独立). (2.27)

最後に, この命題 2.28 を適用して, rank $\Lambda = 2$ のときの六角格子の LLL 簡約基底の例を求める.

例 2.29 (六角格子の LLL 簡約基底)
$\Lambda = \mathbb{Z}\boldsymbol{b}_1 + \mathbb{Z}\boldsymbol{b}_2,\ \boldsymbol{b}_1 = (1, 0),\ \boldsymbol{b}_2 = (1/2, \sqrt{3}/2)$ のとき,
6 つのベクトル $\boldsymbol{b}_1, -\boldsymbol{b}_1, \boldsymbol{b}_2, -\boldsymbol{b}_2, \boldsymbol{b}_1 - \boldsymbol{b}_2, \boldsymbol{b}_2 - \boldsymbol{b}_1$ のなかから, 線形独立となるように任意に選んだベクトル列に限り, LLL 簡約基底となる. 従って, $\mathcal{M}_\Lambda = \mathcal{L}_\Lambda$ である.



解 求める LLL 簡約基底を $(\boldsymbol{x}_1, \boldsymbol{x}_2)$ とする. $d(\Lambda) = \frac{\sqrt{3}}{2}$ であり, 命題 2.28(3) より, $\boldsymbol{x}_1 > \frac{\sqrt[4]{6}}{\sqrt{2}}$ ならば, $(\boldsymbol{x}_1, \boldsymbol{x}_2) \notin \Lambda$ となる. $1 < \frac{\sqrt[4]{6}}{\sqrt{2}} < \sqrt{3}$ より, $\boldsymbol{x}_1$ の候補は, $\pm\boldsymbol{b}_1, \pm\boldsymbol{b}_2, \pm(\boldsymbol{b}_1 - \boldsymbol{b}_2)$ に限る.



次に $\|\boldsymbol{b}_1\| = 1$ であることと, 命題 2.28(2) より, $\boldsymbol{x}_2 > \frac{\sqrt{6}}{2}$ ならば, $(\boldsymbol{x}_1, \boldsymbol{x}_2) \notin \Lambda$ となる. ゆえに, $\boldsymbol{x}_2$ の候補はノルムが $\frac{\sqrt{6}}{2}$ 以下のベクトルであり, $\pm\boldsymbol{b}_1, \pm\boldsymbol{b}_2, \pm(\boldsymbol{b}_1 - \boldsymbol{b}_2)$ に限る.

これらの 6 個のベクトルから, $\boldsymbol{x}_1 \in \mathrm{Min}\ \Lambda, \boldsymbol{x}_2 \in \mathrm{Min}\ (\Lambda \setminus \mathbb{Z}\boldsymbol{b}_1)$ となるように選ぶと, どの場合も $(\boldsymbol{x}_1, \boldsymbol{x}_2) \in \mathcal{B}_\Lambda$ であるから, 命題 2.18 より $(\boldsymbol{x}_1, \boldsymbol{x}_2) \in \mathcal{M}_\Lambda$ である. rank $\Lambda = 2$ の場合, 命題 2.26 より, $\mathcal{M}_\Lambda \subseteq \mathcal{L}_\Lambda$ であるが, これらの 6 個のベクトル以外は LLL 簡約基底にならないから, $\mathcal{M}_\Lambda = \mathcal{L}_\Lambda$ となる. ■

2.4 基底簡約アルゴリズム

A.K.Lenstra, et al. による LLL 格子基底簡約アルゴリズムについて紹介する. 基本的な考え方や詳細については [15] に記述されている. まず, アルゴリズムの停止, 終了について次のように定義する.

定義 2.30 アルゴリズムにおいて, 所定の演算をすべて行い, 目的とする値が得られた場合 **終了**するという. また, 途中の演算において, 求められる値が存在せずに, 次のステップに進むことができないとき**停止**するという.

このアルゴリズムの概要を [23] の記述に従って紹介する.

はじめに定数 μ_{ij}, ベクトル空間 $\mathbb{R}^n$ の直交基底のベクトル $\boldsymbol{b}_i^*$ を (2.12) により計算する. このとき, LLL-簡約基底が帰納的に構成される. その帰納法は簡約基底のベクトルの個数 n による. 最初の変数は $m = 2$ とする. $m > n$ の場合, その手続きは終了する. このアルゴリズムの手順は次の 3 つである:

(Step A_m) $\mu_{m,m-1}$ の値が $|\mu_{m,m-1}| \leq \frac{1}{2}$ となるようにする. もし $|\mu_{m,m-1}| > \frac{1}{2}$ ならば, $\boldsymbol{b}_m - \{\mu_{m,m-1}\}\boldsymbol{b}_{m-1}$ をあらたに $\boldsymbol{b}_m$ とする. ここで $\{x\}$ は実数 x に一番近い整数 $\mathbb{Z}$ の元である. $x+\frac{1}{2} \in \mathbb{Z}$ のときは, $\{x\}$ は $x+\frac{1}{2}$ とする ($x-\frac{1}{2}$ でもよい). このとき, $\mu_{m,m-1} - \{\mu_{m,m-1}\}$ があらたな $\mu_{m,m-1}$ となり, $|\mu_{m,m-1}| \leq \frac{1}{2}$ とすることができる. すべての $\boldsymbol{b}_i^*$ は不変のままである.

(Step B_m) $i = m$ に対して, (2.14) が成立するならば (Step C_m) に進む. そうでなければ, $\boldsymbol{b}_{m-1}$ と $\boldsymbol{b}_m$ を入れ替える. $m > 2$ の場合は (Step A_{m-1}) に, $m = 2$ の場合は (Step A_2) に

行く.

(Step C_m) ((Step A_m) と同様に) $j = m-2, m-3, \cdots, 1$ に対して, μ_{mj} の値が $|\mu_{mj}| \leq \frac{1}{2}$ となるようにする. その後, (Step A_{m+1}) に行く. $m+1 > n$ ならばアルゴリズムは終了する.

アルゴリズムのなかで, $\boldsymbol{b}_i^*$ は成分を使って表す必要はない. そのノルムの 2 乗 $\|\boldsymbol{b}_i\|^2 = \boldsymbol{b}_i^* \cdot \boldsymbol{b}_i^*$ のみ使用される. このアルゴリズムが終了することを以下で示す.

$$D_i := \det(\boldsymbol{b}_\mu \cdot \boldsymbol{b}_\nu)_{1 \leq \mu, \nu \leq i} \quad (1 \leq i \leq n) \tag{2.28}$$

を, $d(\Lambda)^2 (= D_n)$ の小行列式とし, また,

$$D := \prod_{j=1}^{n-1} D_j \tag{2.29}$$

とする. (1.5), (2.12) によって,

$$D_i = \prod_{j=1}^{i} \|\boldsymbol{b}_j^*\|^2 \quad (1 \leq i \leq n) \tag{2.30}$$

を得る. (Step B_m) において, $\boldsymbol{b}_{m-1}$ と $\boldsymbol{b}_m$ を交換するたびに, 他のすべての D_i は不変のままであるが, D_{m-1} の値は $\frac{3}{4}$ 未満になる. 従って, D の値も $\frac{3}{4}$ 未満になる. しかし, D_i に対し,

$$S_i := (3/4)^{i(i-1)/2} \cdot m(\Lambda)^i \tag{2.31}$$

$$m(\Lambda) := \min \left\{ \ \|\boldsymbol{x}\|^2 \ \middle| \ \boldsymbol{x} \in \Lambda, \boldsymbol{x} \neq \boldsymbol{0} \ \right\}, \tag{2.32}$$

とする. このとき, 次が成立する,

$$D_i \geq S_i > 0 \ \ (1 \leq i \leq n). \tag{2.33}$$

従って, アルゴリズムは有限回のステップで終了する.

第3章　代数体における格子基底簡約

本章では, 有限次代数体における格子基底簡約について論じる. 第 1 節で代数体について, 第 2 節で代数体における整数環についての古典理論を述べる. これらはすべて代数的整数論の基礎理論である.

第 3 節では, 著者らによる結果を述べる. 前章で述べた格子基底簡約の実数体における既知の理論を, 代数体へ一般化することを試みる. 著者らは, 有限次代数体 F に対して, 絶対値が 0 以外の最小元をもつ整数環 $\mathcal{O}_F$ は, 有理整数環 $\mathbb{Z}$ および虚二次体における整数環に限ることを明らかにした. この証明を 2 通り述べる. 1 つは, ディリクレの同時近似定理を適用した証明 ([3]) である. もう 1 つは, 群論の結果を適用した証明である.

3.1　代数体

定義 3.1　$\alpha \in \mathbb{C}$ が有理数を係数とする, ある多項式の根であるとき, いいかえると $a_0(\neq 0), a_1, \cdots, a_m \in \mathbb{Q}$ があって

$$a_0\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0 \tag{3.1}$$

が成り立つとき, α は**代数的数** (algebraic number) であるという.

定義 3.2　1 つの代数的数 α について, α を根にもち $\mathbb{Q}$ の元を係数とするような多項式のうち, 次数が最小で, 最高次係数が 1 であるものを α の ($\mathbb{Q}$ 上の) **最小多項式** (minimal polynomial) という. 最小多項式の次数が n のとき, α を n 次の代数的数 (αの次数は n) という.

定義 3.3　代数的数全体のつくる体 Ω の部分体を**代数体** (あるいは**代数的数体**) (algebraic number field) という. 代数体 F を $\mathbb{Q}$ 上の線型空間とみなしたとき, この次元が有限であるとき F は**有限次代数体**であるといい, 次元が無限のときは**無限次代数体**という. もっ

とくわしく, $\dim_{\mathbb{Q}} F = n < \infty$ のとき, F を n 次の代数体 (また, F の次数は n) といい, $[F : \mathbb{Q}] = n$ とかく. さらに, F の $\mathbb{Q}$ 上の線形空間としての基底を F の ($\mathbb{Q}$ 上の) **基底** (basis) という.

以後, 簡単のために, 有限次代数体のことを**代数体**ということにする.

定義 3.4　2 次の代数体, 3 次の代数体をそれぞれ**二次体** (quadratic field), **三次体** (cubic field) という.

定義 3.5　$\alpha \in \Omega$ にたいして, 複素数体 $\mathbb{C}$ の部分体で, α をふくむ最小のものを $\mathbb{Q}(\alpha)$ とかき, 有理数体 $\mathbb{Q}$ に α を**添加してえられる**代数体とよぶ.

命題 3.6　$\alpha \in \Omega$ にたいして, α の次数が n のとき, $\mathbb{Q}(\alpha)$ は n 次の代数体である.

定理 3.7　任意の有限次代数体 F は, 有理数体 $\mathbb{Q}$ に 1 つの代数的数 α を添加してえられる. すなわち, 有限次代数体 F は適当な $\alpha \in \Omega$ によって $F = \mathbb{Q}(\alpha)$ となる.

定義 3.8　定義 3.7 における α を F の**原始元** (primitive element) という.

定義 3.9　n 次代数体 $F = \mathbb{Q}(\alpha)$ について, $F \subset \mathbb{R}$ のとき, F は**実代数体** (real algebraic field) という. 一方, $F \not\subset \mathbb{R}$ のとき, F は**虚代数体** (imaginary algebraic field) であるという.

定義 3.10　2 次の実代数体を**実二次体** (real quadratic field), 虚代数体を**虚二次体** (imaginary quadratic field) とよぶ.

命題 3.11　n 次代数体 $F = \mathbb{Q}(\alpha)$ において, F が実な代数体であることと $\alpha \in \mathbb{R}$ であることは同値である.

3.2　整数環

実数体における有理整数環は, 代数体における整数環となる.

定義 3.12　$\omega \in \mathbb{C}$ が有理整数を係数とする最高次係数 1 のある多項式の根であるとき, ω は**代数的整数** (algebraic integer) であるという.

定義 3.13　代数的整数全体の集合を Γ とする. 代数体 F にふくまれている代数的整数全体の集合 $\mathcal{O}_F := \Gamma \cap F$ を F の**整数環**という. $\mathcal{O}_F$ の元を F の**整数** (integer) という.

命題 3.14　$\mathcal{O}_F$ は F の部分環であり, $\mathcal{O}_F \cap \mathbb{Q} = \mathbb{Z}$ である.

定理 3.15　F を n 次代数体とすると, F の整数環 $\mathcal{O}_F$ は n 個の基底をもつ自由加群である. すなわち, F の n 個の整数 $\{\omega_1, \cdots, \omega_n\} \subset \mathcal{O}_F$ に対して,

$$c_1\omega_1 + \cdots + c_n\omega_n = 0 \ (c_i \in \mathbb{Z}) \quad \Longrightarrow \quad c_1 = \cdots = c_n = 0, \tag{3.2}$$

であり, さらに

$$\mathcal{O}_F = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n = \left\{ \sum_{i=1}^{n} c_i\omega_i \;\middle|\; c_i \in \mathbb{Z},\ \omega_i \in \mathcal{O}_F \ (1 \le i \le n) \right\} \tag{3.3}$$

である.

定義 3.16　n 次代数体 F の整数環 $\mathcal{O}_F$ の自由加群としての一組の基底 $\omega_1, \cdots, \omega_n$ を F の**整数基** (integral basis) という.

3.3　整数環の最小元

代数体 F の整数環 $\mathcal{O}_F$ が最小元をもつのは, F が有理数体と虚二次体の 2 種類であることを 2 通りの方法で証明する. 証明にあたって [25], [26] を参考にした. 2 通りとも, F が有理数体および虚二次体以外の場合は, 最小元をもたないことを示す. F が有理数体の場合は, 整数環 $\mathbb{Z}$ は最小元 1 をもつことは明らかである. F が虚二次体の場合, 整数環 $\mathcal{O}_F$ が最小元をもつことは次章で証明する.

1 つめは, ディリクレの同時近似定理を適用した証明であり, もう 1 つは群論等の結果を適用した証明である.

3.3.1　ディリクレの同時近似定理を適用した証明

補題 3.17 [3, Lemma 4.1]　$\alpha, \beta \in \mathbb{R}$ とし, α, β のうち, 少なくとも 1 つは無理数であるとする. このとき, 無限個の整数の 3 つ組 (x, y, z) で, $|x - z\alpha| < 1/\sqrt{z}$, $|y - z\beta| < 1/\sqrt{z}$ を満たすものが存在する.

証明　ある大きな正整数 k をとり, 次のような積を考える.

$$0(\alpha,\beta),\ 1(\alpha,\beta),\ 2(\alpha,\beta),\ \cdots,\ k^2(\alpha,\beta), \tag{3.4}$$

ここで $n(\alpha,\beta)=(n\alpha,n\beta)$ とする. これらはいずれも, 整数部分の組 (m_i,n_i) と, 小数部分の組 (f_i,g_i) $(i=0,1,\cdots,k^2)$ との和に表せ, 以下のようになる.

$0(\alpha,\beta)=(m_0,n_0)+(f_0,g_0)$, $(m_0,n_0)=(0,0)$ かつ $(f_0,g_0)=(0,0)$,
$1(\alpha,\beta)=(m_1,n_1)+(f_1,g_1)$, $(m_1,n_1)\in\mathbb{Z}^2$, $0\le f_1<1$ かつ $0\le g_1<1$,
$2(\alpha,\beta)=(m_2,n_2)+(f_2,g_2)$, $(m_2,n_2)\in\mathbb{Z}^2$, $0\le f_2<1$ かつ $0\le g_2<1$,
$\cdots\cdots\cdots$
$k^2(\alpha,\beta)=(m_{k^2},n_{k^2})+(f_{k^2},g_{k^2})$, $(m_{k^2},n_{k^2})\in\mathbb{Z}^2$, $0\le f_{k^2}<1$ かつ $0\le g_{k^2}<1$.

k^2+1 個の数の組, (f_0,g_0), $(f_1,g_1),\cdots,(f_{k^2},g_{k^2})$ はすべて $\mathbb{R}^2$ 内で, 領域 $[0,1)\times[0,1)$ 内に存在する. ここで, この領域を次のように k^2 個の正方形に分割する.

領域 $(1,1)$: $[0,1/k)\times[0,1/k)$,
$\cdots\cdots\cdots$
領域 (i,j) : $[(i-1)/k,i/k)\times[(j-1)/k,j/k)$,
$\cdots\cdots\cdots$
領域 (k,k) : $[(k-1)/k,1)\times[(k-1)/k,1)$,

k^2+1 個の数の組が k^2 個の領域に存在するから, ある領域で, 数の組が少なくとも 2 個存在するものがある. その 2 個の数の組を, $(f_p,g_p),(f_q,g_q)$ $(p<q)$ とする. このとき, $|f_p-f_q|<1/k$, $|g_p-g_q|<1/k$ である. いま, $p(\alpha,\beta)=(m_p,n_p)+(f_p,g_p)$, $q(\alpha,\beta)=(m_q,n_q)+(f_q,g_q)$ だから, 我々は $|(q-p)\alpha-(m_q-m_p)|<1/k$, $|(q-p)\beta-(n_q-n_p)|<1/k$ を得る. そこで, $z:=q-p$, $x:=m_q-m_p$, $y:=n_q-n_p$ とおくと, $x,y,z\in\mathbb{Z}$ であり, $|x-z\alpha|<1/k$, $|y-z\beta|<1/k$ となる. そのうえに, さらに k を大きくとるたびに, 新たな x と z が自動的に得られる. なぜなら, x と z を定めたとき, $\alpha\in\mathbb{R}\setminus\mathbb{Q}$ に対して, 不等式 $|x-z\alpha|<1/k$ は k が十分に大きいと成り立たなくなるからである. ここで, $0\le p,q\le k^2$ だから, 我々は $0<z=q-p\le k^2$, 従って $1/k<1/\sqrt{z}$ を得る. ■

命題 3.18 [3, Proposition 4.2]　$\mathcal{O}_F \not\subset \mathbb{R}$ とし, 階数 n は 3 以上とする. 任意の正の数 $\epsilon \in \mathbb{R}$ に対して, $z \in \mathcal{O}_F,\ z \neq 0$ で, $|z| < \epsilon$ となるものが存在する.

証明　階数 $n = 3$ とし, $\mathcal{O}_F = \mathbb{Z}\boldsymbol{a} + \mathbb{Z}\boldsymbol{b} + \mathbb{Z}\boldsymbol{e}$ と仮定してよい. 複素数体 $\mathbb{C}$ は $\mathbb{R}$ 上の 2 次のベクトル空間だから,　$\alpha, \beta \in \mathbb{R}$ で, $\boldsymbol{e} = \alpha\boldsymbol{a} + \beta\boldsymbol{b}$ をみたすものが存在する. そして, $\alpha,\ \beta$ のうち少なくとも 1 つは無理数である. 上の補題 3.17 より, 0 でない整数 $p,\ q,\ r$ で $|p\alpha + q| < \epsilon/(\|\boldsymbol{a}\| + \|\boldsymbol{b}\|)$, $|p\beta + q| < \epsilon/(\|\boldsymbol{a}\| + \|\boldsymbol{b}\|)$ となるものが存在する. そのとき, 我々は $\|p\boldsymbol{e} + q\boldsymbol{a} + r\boldsymbol{b}\| = \|(p\alpha + q)\boldsymbol{a} + (p\beta + r)\boldsymbol{b}\| \leq |(p\alpha + q)|\|\boldsymbol{a}\| + |(p\beta + r)|\|\boldsymbol{b}\| < \epsilon$ を得る. ■

同様にして, 次の命題を得る.

命題 3.19 [3, Proposition 4.3]　$\mathcal{O}_F \subset \mathbb{R}$ とし, 階数 n は 2 以上とする. 任意の正の数 $\epsilon \in \mathbb{R}$ に対して, $z \in \mathcal{O}_F,\ z \neq 0$ で, $|z| < \epsilon$ となるものが存在する.

以上により, 次の定理を得る.

定理 3.20 [3, Theorem 4.4]　代数体 F における整数環 $\mathcal{O}_F$ が最小元をもつのは, F が有理数体または虚二次体のときに限る.

3.3.2　群論の結果を適用した証明

次に 2 つめの証明を挙げる. これは群論等の結果を適用した証明であり, 本小節の内容は著者らによる結果である. まず, F が実代数体, すなわち, $F \subset \mathbb{R}$ のときの整数環 $\mathcal{O}_F$ について考える.

定義 3.21　G を加法群とする. γ が G の**集積点** (accumulation point) であるとは, 任意の $\varepsilon > 0$ に対して, γ の ε-近傍を

$$U_\varepsilon(\gamma) := \left\{ a \in G \;\middle|\; |a - \gamma| < \varepsilon \right\} \tag{3.5}$$

とすると,

$$U_\varepsilon(\gamma) \cap G \neq \{0\} \tag{3.6}$$

となることである.

定義 3.22　G, G' を加法群とし, $G \subset G'$ とする. G が G' で**稠密** (dense) であるとは, 任意の $\gamma \in G'$, $\varepsilon > 0$ に対して,

$$(\gamma - \varepsilon, \gamma + \varepsilon) \cap G \neq \emptyset \tag{3.7}$$

であるときをいう.

補題 3.23　$G \neq \{0\}$ を加法群 $\mathbb{R}$ の部分群とする. このとき, G は $\mathbb{R}$ 内で稠密か巡回群になる.

証明　$a := \inf\{g \in G \mid g > 0\}$ とする. $\{g \in G \mid g > 0\} \neq \emptyset$ だから, $0 \leq a < \infty$ である.

まず $a \notin G$ の場合, 任意の $\varepsilon > 0$ に対して, $g \in G$ で $a < g < a + \varepsilon$ をみたすものが存在する. 同じ議論より, $g' \in G$ で $a < g' < g < a + \varepsilon$ をみたすものが存在する. ここで, $h_\varepsilon := g - g'$ とおくと, $h_\varepsilon \in G$ であり, $0 < h_\varepsilon < \varepsilon$ をみたす.

いま, $\cup_{\varepsilon > 0}\{z \cdot h_\varepsilon \mid z \in \mathbb{Z}\}$ が $\mathbb{R}$ 内で稠密であることがわかり, これは G の部分集合である. 任意の $b \in \mathbb{R}$ に対して, 開区間 $(b - \varepsilon, b + \varepsilon)$ を考えれば, この区間は 2ε の距離をもつ. 従って, この区間には $z \cdot h_\varepsilon$ の形の元が存在する. なぜなら, この形の 2 元の差は ε より小さいからである. 従って, G は $\mathbb{R}$ 内で稠密である.

$a \in G$ かつ $a = 0$ の場合, 同様にして G は $\mathbb{R}$ 内で稠密であることが証明できる.

$a \in G$ かつ $a > 0$ の場合, $a \in \{g \in G \mid g > 0\}$ だから, $a = \min\{g \in G \mid g > 0\}$ である. この場合, $G = a\mathbb{Z}$ だから G には最小元 a があり, G は巡回群である. ■

補題 3.24　G を加法群 $\mathbb{R}$ の部分群とするとき, 次が成立する.

(1)　0 が G の集積点ならば, G は $\mathbb{R}$ で稠密である.

(2)　0 が G の集積点でなければ, $s \in G$ で $G = \{ns \mid n \in \mathbb{Z}\}$ となるものが存在する.

命題 3.19 より, 代数体 F の整数環 $\mathcal{O}_F \subset \mathbb{R}$ を加法群とみると, 0 が $\mathcal{O}_F$ の集積点であることがわかる. これと, 補題 3.24 (1) より, 次の命題を得る.

命題 3.25　$G = \mathcal{O}_F \subset \mathbb{R}$ とし, 階数 n は 2 以上とする. このとき, G は $\mathbb{R}$ で稠密である.

次に F が虚代数体, すなわち, $F \not\subset \mathbb{R}$ のときの整数環 $\mathcal{O}_F$ について考える. 整数環 $\mathcal{O}_F$ の階数が 2 のとき, 線形独立な 2 つのベクトルによってはられる空間は離散的に存在する. これは F が虚二次体のときである. $\mathcal{O}_F$ の階数が 3 以上の場合について以下で述べる.

定理 3.26 [ボルツァーノ・ワイエルシュトラス]　$\mathbb{R}^n$ の有界な無限集合は, 集積点をもつ.

命題 3.27　$G(\subset \mathbb{C})$ を $\mathbb{Z}$-自由加群とし, 階数 n は 3 以上とする. このとき, 0 が $\mathbb{C}$ で G の集積点となる.

証明　仮定より, G は rank 3 の部分 $\mathbb{Z}$-加群 S を含む. $S = \mathbb{Z}\boldsymbol{a}_1 + \mathbb{Z}\boldsymbol{a}_2 + \mathbb{Z}\boldsymbol{a}_3$ とする. ここで $\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3 \in \mathbb{C}$ である.

$\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3$ のうち 2 つ, 例えば $\boldsymbol{a}_1$ と $\boldsymbol{a}_2$ が $\mathbb{R}$ 上線形従属であるとする. ここで, $\mathbb{R}\boldsymbol{a}_1$ を $\mathbb{R}$ と同一視すると, 補題 3.23 より直線 $\mathbb{R}\boldsymbol{a}_1$ のなかで $\mathbb{Z}\boldsymbol{a}_1 + \mathbb{Z}\boldsymbol{a}_2$ は稠密になり, 原点にいくらでも近いベクトルがとれる.

次に $\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3$ は $\mathbb{R}$ 上線形独立であるとする. このとき, $\boldsymbol{a}_1$ と $\boldsymbol{a}_2$ ではられた平行四辺形のなかに $\mathbb{Z}\boldsymbol{a}_3$ の元を引き戻すことにより, この平行四辺形のなかに無限個の異なる $\mathbb{Z}\boldsymbol{a}_1 + \mathbb{Z}\boldsymbol{a}_2 + \mathbb{Z}\boldsymbol{a}_3$ の元が存在することになる. よって定理より, この平行四辺形のなかに $\mathbb{Z}\boldsymbol{a}_1 + \mathbb{Z}\boldsymbol{a}_2 + \mathbb{Z}\boldsymbol{a}_3$ の集積点がある. この集積点を $\boldsymbol{b}$ とするとき, $\boldsymbol{b}$ を中心とし, 半径 $\frac{\varepsilon}{2}$ の円内に, $\mathbb{Z}\boldsymbol{a}_1 + \mathbb{Z}\boldsymbol{a}_2 + \mathbb{Z}\boldsymbol{a}_3$ の元が無数に存在する. これらの異なる 2 つを, $\boldsymbol{e} = e_1\boldsymbol{a}_1 + e_2\boldsymbol{a}_2 + e_3\boldsymbol{a}_3$, $\boldsymbol{f} = f_1\boldsymbol{a}_1 + f_2\boldsymbol{a}_2 + f_3\boldsymbol{a}_3$, とすると, $\|\boldsymbol{e} - \boldsymbol{f}\| \leq \|\boldsymbol{e} - \boldsymbol{b}\| + \|\boldsymbol{b} - \boldsymbol{f}\| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$ となり, $\boldsymbol{e} - \boldsymbol{f} \neq \boldsymbol{0}$, $\boldsymbol{e} - \boldsymbol{f} \in \mathbb{Z}\boldsymbol{a}_1 + \mathbb{Z}\boldsymbol{a}_2 + \mathbb{Z}\boldsymbol{a}_3$ である. ε は任意であるから, この集積点 $\boldsymbol{b} = \boldsymbol{0}$ であることが分かる. 従って, 0 が $\mathbb{C}$ で G の集積点であることが証明された. ■

系 3.28　$G = \mathcal{O}_F$ を階数 $n \geq 3$ の F の整数環とする. このとき, 0 は $\mathbb{C}$ 内での集積点である.

G が階数 3 の $\mathbb{Z}$-自由加群の場合, G が $\mathbb{C}$ で稠密になる条件を以下で述べる. 以下で, そのための準備をする.

定義 3.29　A を $\mathbb{C}$ の部分集合とする. $b \in \mathbb{C}$, 任意の $\varepsilon > 0$ に対して, $U_\varepsilon(b) \cap A \neq \emptyset$ であるとき, b を A の**触点** (point of osculation) という. A の触点全体の集合 $\overline{A}$ を A の**閉包** (closure) という.

定義 3.30　$A \subset \mathbb{C}$ は, 任意の $x \in A$ に対しある $\varepsilon > 0$ が存在して $U_\varepsilon(x) \subset A$ となるとき, $\mathbb{C}$ の**開集合** (open set) という.

定義 3.31　$A \subset \mathbb{C}$ は, $\overline{A} = A$ をみたすとき, $\mathbb{C}$ の**閉集合** (closed set) という.

定義 3.32　$A, B, X \in C$ に対して,

$$X = A \cup B, \quad A \cap B = \emptyset \tag{3.8}$$

のとき, X は A, B の**直和** (direct sum) であるといい,

$$X = A \dot{+} B \tag{3.9}$$

で表す.

定義 3.33　$\mathbb{C}$ の開集合 U は, 空でない 2 つの開集合の直和とならないとき, **連結** (connection) という. また, $\mathbb{C}$ の閉集合 F は, 空でない 2 つの閉集合の直和とならないとき, 連結であるという.

定義 3.34　$A(\subset \mathbb{C})$ の一点 x に対し, x を含む A の連結部分集合全体の合併 C を x を含む A の**連結成分** (connected component) という.

以上の準備により, 次の命題を得る.

補題 3.35　G が $\mathbb{C}$ の部分自由 $\mathbb{Z}$-加群であり, rank $n = 3$, $G \not\subset \mathbb{R}$ とする. 0 を含む G の閉包 $\overline{G}$ の連結成分が直線になるための必要十分条件は, 2 つの $\mathbf{0}$ でない $\boldsymbol{b}_1, \boldsymbol{b}_2 \in G$ と $\gamma \in \mathbb{R} \setminus \mathbb{Q}$ で, $\boldsymbol{b}_1 = \gamma \boldsymbol{b}_2$ を満たすようなものが存在することである.

証明　0 を含む G の閉包の連結成分が直線であると仮定する. そのとき, $G \cap \ell$ は無限集合であり, $G \cap \ell$ の閉包は ℓ である. $G = \mathbb{Z}\boldsymbol{a}_1 + \mathbb{Z}\boldsymbol{a}_2 + \mathbb{Z}\boldsymbol{a}_3$ で表し, $\boldsymbol{x} = x_1\boldsymbol{a}_1 + x_2\boldsymbol{a}_2 + x_3\boldsymbol{a}_3, \boldsymbol{x}' = x_1'\boldsymbol{a}_1 + x_2'\boldsymbol{a}_2 + x_3'\boldsymbol{a}_3$ を 2 つの異なる 0 でない $G \cap \ell$ の元とする. $\boldsymbol{a}_1,\ \boldsymbol{a}_2,\ \boldsymbol{a}_3$ は $\mathbb{Z}$ 上線形独立だから, もし $\boldsymbol{x} \in \mathbb{Q}\boldsymbol{x}'$ ならば, $x_1 : x_2 : x_3 = x_1' : x_2' : x_3'$ である. ここで, x_1, x_2, x_3 の最大公約数を d で表す. もし, $G \cap \ell \subseteq \mathbb{Q}\boldsymbol{x}$ ならば $G \cap \ell = \mathbb{Z}(1/d)\boldsymbol{x}$ である. この場合, $G \cap \ell$ の閉包はそれ自身となり矛盾する. ゆえに $G \cap \ell \not\subseteq \mathbb{Q}\boldsymbol{x}$ である. $\ell = \mathbb{R}\boldsymbol{x}$ だから, $\gamma \in \mathbb{R} \setminus \mathbb{Q}$ で $\boldsymbol{b}_1 = \gamma\boldsymbol{x} \in G \cap \ell$ となるものが存在する.

次に, 2 つの $\mathbf{0}$ でない元 $\boldsymbol{b}_1, \boldsymbol{b}_2 \in G$ と $\gamma \in \mathbb{R} \setminus \mathbb{Q}$ で, $\boldsymbol{b}_1 = \gamma\boldsymbol{b}_2$ となるものが存在すると仮定する. F を G の商体とする. このとき, ある $\boldsymbol{a} \in G$ に対し, $F = \mathbb{Q}\boldsymbol{b}_1 + \mathbb{Q}\boldsymbol{b}_2 + \mathbb{Q}\boldsymbol{a}$ となるものが存在する. ゆえに, 正整数 n で $G \subseteq \mathbb{Z}(1/n)\boldsymbol{b}_1 + \mathbb{Z}(1/n)\boldsymbol{b}_2 + \mathbb{Z}(1/n)\boldsymbol{a}$ となるものが存在する. 0 を含む $\mathbb{Z}(1/n)\boldsymbol{b}_1 + \mathbb{Z}(1/n)\boldsymbol{b}_2 + \mathbb{Z}(1/n)\boldsymbol{a}$ の閉包の連結成分は直線 $\mathbb{R}\boldsymbol{b}_1$ であることが分かる. ゆえに, 0 を含む G の閉包の連結成分もまた直線 $\mathbb{R}\boldsymbol{b}_1$ である. ■

系 3.36　$G = \mathcal{O}_F$ を rank $n = 3$, $\mathcal{O}_F \not\subset \mathbb{R}$ の整数環とする. 0 を含む G の閉包 $\overline{G}$ の連結成分が直線になるための必要十分条件は, 2 つの $\mathbf{0}$ でない $\boldsymbol{b}_1, \boldsymbol{b}_2 \in G$ と $\gamma \in \mathbb{R} \setminus \mathbb{Q}$ で, $\boldsymbol{b}_1 = \gamma \boldsymbol{b}_2$ を満たすようなものが存在することである.

命題 3.37　G が $\mathbb{C}$ の部分自由 $\mathbb{Z}$-加群であり, rank $n = 3$, $G \not\subset \mathbb{R}$ とする. このとき, G の閉包 $\overline{G}$ が $\mathbb{C}$ となるための必要十分条件は, 任意の 2 つの $\mathbf{0}$ でない $\boldsymbol{b}_1, \boldsymbol{b}_2 \in G$ と $\gamma \in \mathbb{R} \setminus \mathbb{Q}$ に対して, $\boldsymbol{b}_1 \neq \gamma \boldsymbol{b}_2$ が成り立つことである.

証明　$G = \mathbb{Z}\boldsymbol{a}_1 + \mathbb{Z}\boldsymbol{a}_2 + \mathbb{Z}\boldsymbol{a}_3$ と表す. 2 つの $\mathbf{0}$ でない $\boldsymbol{b}_1, \boldsymbol{b}_2 \in G$ と, $\gamma \in \mathbb{R} \setminus \mathbb{Q}$ で $\boldsymbol{b}_1 = \gamma \boldsymbol{b}_2$ となるものが存在することを仮定する. このとき, 補題 3.35 より, $\mathbb{C}$ で G の閉包 $\overline{G}$ は等間隔に配置された平行線となる. 従って, $\overline{G} \neq \mathbb{C}$ である.

次に, 任意の $\mathbf{0}$ でない 2 つの元 $\boldsymbol{b}_1, \boldsymbol{b}_2 \in G$ および, 任意の $\gamma \in \mathbb{R} \setminus \mathbb{Q}$ に対して, $\boldsymbol{b}_1 \neq \gamma \boldsymbol{b}_2$ であると仮定する. いま, 任意の $\boldsymbol{a} \in \mathbb{C}$ および任意の $\varepsilon > 0$ に対して, $U_\varepsilon(\boldsymbol{a}) := \{\boldsymbol{x} \in \mathbb{C} \mid \|\boldsymbol{a} - \boldsymbol{x}\| < \varepsilon\}$ とおく. 仮定より, もし $\boldsymbol{x} = x_1\boldsymbol{a}_1 + x_2\boldsymbol{a}_2 + x_3\boldsymbol{a}_3$, $\boldsymbol{x}' = x_1'\boldsymbol{a}_1 + x_2'\boldsymbol{a}_2 + x_3'\boldsymbol{a}_3 \in U_\varepsilon(\boldsymbol{a}) \cap G$ が $\boldsymbol{x} \in \mathbb{R}\boldsymbol{x}'$ を満たすなら, $x_1 : x_2 : x_3 = x_1' : x_2' : x_3'$ である. ゆえに, $\boldsymbol{x} \in U_\varepsilon(\boldsymbol{a}) \cap G$ に対して, $\{\boldsymbol{x}' \in U_\varepsilon(\boldsymbol{a}) \cap G \mid \boldsymbol{x} \in \mathbb{R}\boldsymbol{x}'\}$ は有限集合である. 命題 3.27 によって $\mathbf{0}$ は $\mathbb{C}$ で G の集積点となるから, $\mathbf{0}$ でない元 $\boldsymbol{u}_1, \boldsymbol{u}_2 \in U_{\varepsilon/2}(\mathbf{0}) \cap G$ で $\boldsymbol{u}_1 \notin \mathbb{R}\boldsymbol{u}_2$ となるものが存在する. 従って $(\mathbb{Z}\boldsymbol{u}_1 + \mathbb{Z}\boldsymbol{u}_2) \cap U_\varepsilon(\boldsymbol{a}) \neq \emptyset$, $(\mathbb{Z}\boldsymbol{u}_1 + \mathbb{Z}\boldsymbol{u}_2) \subset G$ であり, $G \cap U_\varepsilon(\boldsymbol{a}) \neq \emptyset$ を得る. ■

系 3.38　$G = \mathcal{O}_F$ を rank $n = 3$, $\mathcal{O}_F \not\subset \mathbb{R}$ の整数環とする. このとき, G の閉包 $\overline{G}$ が $\mathbb{C}$ となるための必要十分条件は, 任意の 2 つの $\mathbf{0}$ でない $\boldsymbol{b}_1, \boldsymbol{b}_2 \in G$ と $\gamma \in \mathbb{R} \setminus \mathbb{Q}$ に対して, $\boldsymbol{b}_1 \neq \gamma \boldsymbol{b}_2$ が成り立つことである.

いま, $G = \mathbb{Z}i + \mathbb{Z}\sqrt{2} + \mathbb{Z}\sqrt{3}(1+i)$ とする. このとき, 任意の 2 つの元 $\boldsymbol{b}_1, \boldsymbol{b}_2 \in G$ および任意の $\gamma \in \mathbb{R} \setminus \mathbb{Q}$ に対して, $\boldsymbol{b}_1 \neq \gamma \boldsymbol{b}_2$ となることが分かる. 従って, 次を得る.

例 3.39　$G = \mathbb{Z}i + \mathbb{Z}\sqrt{2} + \mathbb{Z}\sqrt{3}(1+i)$ とする. このとき, $\mathbb{C}$ 内で $\overline{G} = \mathbb{C}$ である.

今まで, 有限次代数体 F における整数環 $\mathcal{O}_F$ の最小元について述べた. 定理 3.20 より, $\mathcal{O}_F$ が最小元をもつのは, F が有理数体または虚二次体のときに限ることが分かった.

次章では, F を虚二次体として格子を考え, 基底簡約について考えていく.

第4章　虚二次体における格子基底簡約

本章では, 著者らによって一般化された虚二次体における格子基底簡約について論じる. 第 1 節では, 二次体とその整数環について具体的に表示する. これはすでに知られている古典理論である. 標準的なものなので特に文献は示さない. 第 2 節では, 虚二次体上で格子を定義する. 虚二次体は前章でみたように最小元をもつことが保証されていることが重要である. 第 3 節では, 虚二次体上で格子を考えるときに必要となる基礎理論について述べる. 実数体の範囲を超えるため, 複素数のなかで内積を考えなければならない. 第 4 節では, 著者ら ([3]) によって得られた LLL 簡約基底の性質について述べる. 第 5 節では, 常に簡約基底が存在するような擬簡約基底について述べ, その基底が常に存在し, 有限回の計算でアルゴリズムが終了することを証明する. この節の結果は著者 ([5]) によって明らかにされた.

第 1 章における体 K は F(有限次代数体), 環 R は $\mathcal{O}_F$(F の整数環) とする.

4.1　二次体とその整数環の表示

命題 4.1　定義 3.4 で定義された二次体 F は, 平方因子をもたない適当な $m \in \mathbb{Z}, m \neq 0$ によって,

$$F = \mathbb{Q}(\sqrt{m}) \tag{4.1}$$

と表せる. ここで $\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\}$ である.

命題 4.2　命題 4.1 において, $m > 0$ のとき, F は定義 3.10 で定義された実二次体になる. また $m < 0$ のとき, F は虚二次体となる.

定理 4.3　F を二次体とし, その整数環を $\mathcal{O}_F$ とする. このとき $\mathcal{O}_F$ は, m の値によって次のように表せる.

(i) $m \equiv 2, 3 \pmod 4$ のとき,

$$\mathcal{O}_F = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}, \tag{4.2}$$

(ii) $m \equiv 1 \pmod 4$ のとき,

$$\mathcal{O}_F = \left\{ \frac{a + b\sqrt{m}}{2} \;\middle|\; a, b \in \mathbb{Z}, \quad a \equiv b \pmod 2 \right\}. \tag{4.3}$$

4.2 $\mathcal{O}_F$-格子の定義

F を虚二次体, $\mathcal{O}_F$ を F の整数環, V を F 上の n 次元線形空間とする.

定義 4.4 Λ を $\mathcal{O}_F$-加群 (module) とする. このとき, Λ が F^n 内における **格子**(lattice) であるとは, ある F^n のベクトル空間としての基底 $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ で,

$$\Lambda = \mathcal{O}_F\boldsymbol{b}_1 + \cdots + \mathcal{O}_F\boldsymbol{b}_n = \left\{ \sum_{i=1}^{n} r_i\boldsymbol{b}_i \;\middle|\; r_i \in \mathcal{O}_F \ (1 \le i \le n) \right\} \tag{4.4}$$

を満たすものが存在することをいう.

4.3 内積とノルムの定義

有限次代数体 F に対して, $F \subset \mathbb{C}$ だから, 複素数体上のベクトル空間内で内積とノルムを定義する.

定義 4.5 $z \in F$ に対して, $z = x + yi$ $(x, y \in \mathbb{R})$ とする. このとき z の **絶対値** (absolute value)$|z|$ を

$$|z| = \sqrt{x^2 + y^2} \tag{4.5}$$

によって定義する.

命題 4.6 $z \in F$ に対して,

$$|z|^2 = |\overline{z}|^2 = z \cdot \overline{z} \tag{4.6}$$

が成り立つ.

定義 4.7　$\boldsymbol{a}, \boldsymbol{b} \in F^n$ とする. ここで, $\boldsymbol{a} = (a_1, \cdots, a_n), \boldsymbol{b} = (b_1, \cdots, b_n)$ としたとき, **内積** $\boldsymbol{a} \cdot \boldsymbol{b}$ を

$$\boldsymbol{a} \cdot \boldsymbol{b} = a_1\overline{b}_1 + \cdots + a_n\overline{b}_n \tag{4.7}$$

で定義する. 従って $\boldsymbol{a} \cdot \boldsymbol{b} \in \mathbb{C}$ である. 特に $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{R}^n$ (実ベクトル) ならば,

$$\boldsymbol{a} \cdot \boldsymbol{b} = a_1 b_1 + \cdots + a_n b_n \tag{4.8}$$

である. 一般の複素ベクトルの内積を, 実ベクトルの内積と区別するために, 特に**エルミート積**と言うこともある.

このように内積を定義すると, 定義 1.2 における (1)-(4) の公理を満たしている.

定義 4.8　$\boldsymbol{x} \in F^n$ に対して, $\boldsymbol{x} \cdot \boldsymbol{x}$ の負でない平方根を $\boldsymbol{x}$ の**ノルム** (norm) といい, $\|\boldsymbol{x}\|$ で表わす. すなわち,

$$\|\boldsymbol{x}\| = \sqrt{\boldsymbol{x} \cdot \boldsymbol{x}} \tag{4.9}$$

である.

命題 4.9　定義 4.8 の 式 (4.9) より,

$$\|\boldsymbol{x}\|^2 = \boldsymbol{x} \cdot \boldsymbol{x} = |x_1|^2 + \cdots + |x_n|^2 \tag{4.10}$$

が成り立つ. ここで, $x_i (\in F)$ は $\boldsymbol{x}$ の第 i 成分である.

4.4　LLL 簡約基底

以後, 第 2 章で定義された LLL 簡約基底を, F が虚二次体の場合でも同様に定義していく. 定義 2.19 はこの場合, 次のようになる.

定義 4.10　$(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \in \mathcal{B}_\Lambda$ に対して,

$$\boldsymbol{b}_i^* := \boldsymbol{b}_i - \sum_{j=1}^{i-1} \mu_{ij}\boldsymbol{b}_j^*, \quad \mu_{ij} := \frac{\boldsymbol{b}_i \cdot \boldsymbol{b}_j^*}{\boldsymbol{b}_j^* \cdot \boldsymbol{b}_j^*} \quad (1 \leq j < i \leq n) \tag{4.11}$$

とする (Gram-Schmidt の直交化法). ここで, 複素ベクトル空間における内積 (定義 4.7 の式 (4.7)) は複素数だから, $\mu_{ij} \in \mathbb{C}$ である.

例 4.11　$\boldsymbol{b}_1 = (i, 0, 1),\ \boldsymbol{b}_2 = (1, i, 0),\ \boldsymbol{b}_3 = (0, -1, i)$ $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3 \in \mathbb{Q}(i))$　に対して, $\boldsymbol{b}_1^*,\ \boldsymbol{b}_2^*,\ \boldsymbol{b}_3^*$ を求めると,

$$\boldsymbol{b}_1^* = (i,\ 0,\ 1)\,,\quad \boldsymbol{b}_2^* = \left(\frac{1}{2},\ i,\ \frac{i}{2}\right),\quad \boldsymbol{b}_3^* = \left(\frac{1-i}{3},\ -\frac{1+i}{3},\ \frac{1+i}{3}\right) \tag{4.12}$$

である.

次に, 定義 2.21 は次のようになる,

定義 4.12 [3]　$(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \in \mathcal{B}_\Lambda$ が Λ の **LLL 簡約基底**であるとは, 定義 4.10 における, 直交基底におけるベクトル $\boldsymbol{b}_1^*, \cdots, \boldsymbol{b}_n^*$ が次を満たすときである :

$$|\mu_{ij}| \leq \frac{1}{2}\ \ (1 \leq j < i \leq n), \tag{4.13}$$

$$\|\boldsymbol{b}_i^* + \mu_{i,i-1}\boldsymbol{b}_{i-1}^*\|^2 \geq \frac{3}{4}\|\boldsymbol{b}_{i-1}^*\|^2. \tag{4.14}$$

第 2 章と同様に, 以後, Λ の LLL-reduced basis 全体を $\mathcal{L}_\Lambda$ で表す.

補題 4.13 [3, Lemma 3.1]　$F = \mathbb{Q}(\sqrt{m}),\ m < 0$ のとき 0 でない任意の $r \in \mathcal{O}_F$ に対し, $|r|^2 \geq 1$ である.

証明　$m \not\equiv 1 \pmod 4$ のとき, $r = a + b\sqrt{m}\ (a, b \in \mathbb{Z})$ と表せる. $r = a + b\sqrt{-m}i$ だから, $|r|^2 = a^2 - mb^2$. となる. いま $a \neq 0$ とすると, $|r|^2 \geq 1$ である. また, $b \neq 0$ とすると, $|r|^2 \geq -m \geq 1$ である. 従って, $a \neq 0$ または $b \neq 0$ のとき, $|r|^2 \geq 1$ である.

$m \equiv 1 \pmod 4$ のとき, $r = \frac{a+b\sqrt{m}}{2}(a, b \in \mathbb{Z})$ と表せる. ここで $a \equiv b \pmod 2$ である. $r = \frac{a+b\sqrt{-m}i}{2} = \frac{a}{2} + \frac{b\sqrt{-m}}{2}i$ だから, $|r|^2 = (\frac{a}{2})^2 + (\frac{b\sqrt{-m}}{2})^2 = \frac{a^2-mb^2}{4}$.
$a \neq 0$ または $b \neq 0$ のとき, $|r|^2 \geq 1$ であることを示す. $m < 0,\ m \equiv 1 \pmod 4$ をみたす m で, $-m(> 0)$ が最小となる $m = -3$. このとき $|r|^2 = \frac{a^2+3b^2}{4}$ である.
(i) $a \equiv b \equiv 0 \pmod 2$ のとき, $a^2 + 3b^2$ の最小値は 4 ($a = \pm 2,\ b = 0$ のとき) である.
(ii) $a \equiv b \equiv 1 \pmod 2$ のとき, $a^2 + 3b^2$ の最小値は 4 ($a = \pm 1,\ b = \pm 1$ のとき) である.
以上より, $|r|^2 \geq \frac{a^2+3b^2}{4} \geq 1$ である. ■

命題 4.14 [3, Proposition 3.2]　F を虚二次体 $\mathbb{Q}(\sqrt{m})$ とし, その整数環を $\mathcal{O}_F$ とする. また $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \in \mathcal{B}_\Lambda$ とし, $\boldsymbol{b}_i^*\ (i = 1, \cdots, n)$ は定義 4.10 で定義した通りとする. このとき, $\boldsymbol{0}$ でない任意の $\boldsymbol{x} \in \Lambda$ に対して,

$$\|\boldsymbol{x}\|^2 \geq \|\boldsymbol{b}_i^*\|^2 \tag{4.15}$$

となる $i \leq n$ が存在する. ここで, i は $\boldsymbol{x} = \sum_{j=1}^{n} r_j \boldsymbol{b}_j$ $(r_j \in \mathcal{O}_F)$ と表したときの, $r_j \neq 0$ を満たす最大の j である.

証明　Λ の任意の元 $\boldsymbol{x}$ に対して, $\boldsymbol{x} = \sum_{j=1}^{n} r_j \boldsymbol{b}_j = \sum_{j=1}^{n} s_j \boldsymbol{b}_j^*$ と表せる. ここで, $r_j \in \mathcal{O}_F$, $s_j \in \mathbb{Q}(\sqrt{m})$ $(j = 1, \cdots, n)$ である. i を $r_i \neq 0$ となる最大の添字とする. このとき, $r_{i+1} = \cdots = r_n = 0$ である. このとき, $r_i = s_i$ および $\boldsymbol{x} = \sum_{j=1}^{i} s_j \boldsymbol{b}_j^*$ が成立することを以下で示す.

定義 4.10 の (4.11) 式 より, $\boldsymbol{b}_i = \boldsymbol{b}_i^* + \sum_{j=1}^{i-1} \mu_{ij} \boldsymbol{b}_j^*$ だから, $\boldsymbol{b}_j^*$ $(j = 1, 2, \cdots, i)$ の線形結合の形に整理すると,

$$\begin{aligned} \boldsymbol{x} &= \sum_{j=1}^{i} r_j \boldsymbol{b}_j && (4.16) \\ &= \sum_{j=1}^{i} \left\{ r_j \left(\sum_{k=1}^{j-1} \mu_{jk} \boldsymbol{b}_k^* + \boldsymbol{b}_j^* \right) \right\} && (4.17) \\ &= \sum_{j=1}^{i} \left(r_j + \sum_{k=j+1}^{i} r_k \mu_{kj} \right) \boldsymbol{b}_j^* && (4.18) \end{aligned}$$

いま, (4.18) で $j = i$ のとき, $r_i = s_i$, $\boldsymbol{x} = \sum_{j=1}^{i} s_j \boldsymbol{b}_j^*$ である. 次に, $i \neq j$ に対して $\boldsymbol{b}_i^* \cdot \boldsymbol{b}_j^* = 0$ だから

$$\begin{aligned} \|\boldsymbol{x}\|^2 &= \|s_1 \boldsymbol{b}_1^* + \cdots + s_i \boldsymbol{b}_i^*\|^2 && (4.19) \\ &= \|s_1 \boldsymbol{b}_1^*\|^2 + \cdots + \|s_i \boldsymbol{b}_i^*\|^2 && (4.20) \\ &\geq \|s_i \boldsymbol{b}_i^*\|^2 && (4.21) \\ &= |s_i|^2 \|\boldsymbol{b}_i^*\|^2 && (4.22) \end{aligned}$$

$s_i = r_i$ であり, また補題 4.13 より $|r_i|^2 \geq 1$ である. 従って,

$$\begin{aligned} \|\boldsymbol{x}\|^2 &\geq |r_i|^2 \|\boldsymbol{b}_i^*\|^2 && (4.23) \\ &\geq \|\boldsymbol{b}_i^*\|^2 && (4.24) \end{aligned}$$

となり, 証明された. ■

虚二次体における LLL 簡約基底の性質として, 以下の命題が得られる :

定理 4.15 [3, Theorem 3.3]　$F=\mathbb{Q}(\sqrt{m}),\ m<0,\ m$ は平方因数をもたない有理整数. また $(\boldsymbol{b}_1,\cdots,\boldsymbol{b}_n)\in\mathcal{L}_\Lambda$ とし, $\boldsymbol{b}_i^*\ (i=1,2,\cdots,n),\ \mu_{ij}$ は定義 4.10 で定義した通りとする. このとき次が成立する :

$$(1)\quad \|\boldsymbol{b}_j\|^2\le 2^{i-1}\|\boldsymbol{b}_i^*\|^2\ \ (1\le j\le i\le n), \tag{4.25}$$

$$(2)\quad d(\Lambda)\le\prod_{i=1}^{n}\|\boldsymbol{b}_i\|\le 2^{\frac{n(n-1)}{4}}d(\Lambda), \tag{4.26}$$

$$(3)\quad \|\boldsymbol{b}_1\|\le 2^{\frac{n-1}{4}}d(\Lambda)^{\frac{1}{n}}, \tag{4.27}$$

$$(4)\quad \|\boldsymbol{b}_1\|^2\le 2^{n-1}\|\boldsymbol{x}\|^2\ \ \text{for}\ {}^{\forall}\boldsymbol{x}\in\Lambda,\ \boldsymbol{x}\neq\boldsymbol{0}, \tag{4.28}$$

$$(5)\quad \|\boldsymbol{b}_j\|^2\le 2^{n-1}\max\{\|\boldsymbol{x}_1\|^2,\cdots,\|\boldsymbol{x}_t\|^2\}\ (1\le j\le t\le n\ \text{で},\ \boldsymbol{x}_1,\cdots,\boldsymbol{x}_t\ \text{は線型独立}). \tag{4.29}$$

証明　(1)　(4.13) と (4.14) より, $1<i\le n$ に対して

$$\|\boldsymbol{b}_i^*\|^2\ge\left(\frac{3}{4}-|\mu_{i,i-1}|^2\right)\|\boldsymbol{b}_{i-1}^*\|^2\ge\frac{1}{2}\|\boldsymbol{b}_{i-1}^*\|^2 \tag{4.30}$$

である. これを順次適用すれば, $1\le j\le i\le n$ に対して,

$$\|\boldsymbol{b}_j^*\|^2\le 2^{i-j}\|\boldsymbol{b}_i^*\|^2 \tag{4.31}$$

が成立する. (4.11), (4.13) より,

$$\begin{aligned}\|\boldsymbol{b}_i\|^2 &= \|\boldsymbol{b}_i^*\|^2+\sum_{j=1}^{i-1}|\mu_{ij}|^2\|\boldsymbol{b}_j^*\|^2 &(4.32)\\ &\le \|\boldsymbol{b}_i^*\|^2+\sum_{j=1}^{i-1}\frac{1}{4}\cdot 2^{i-j}\|\boldsymbol{b}_i^*\|^2 &(4.33)\\ &= \left(1+\frac{1}{4}(2^i-2)\right)\|\boldsymbol{b}_i^*\|^2 &(4.34)\\ &\le 2^{i-1}\|\boldsymbol{b}_i^*\|^2, &(4.35)\end{aligned}$$

を得る. 従って, $1\le j\le i\le n$ に対して,

$$\|\boldsymbol{b}_j^*\|^2\le 2^{j-1}\|\boldsymbol{b}_j^*\|^2\le 2^{i-1}\|\boldsymbol{b}_i^*\|^2 \tag{4.36}$$

であり (1) が証明された.

(2)　(1.6), (4.11) より,

$$d(\Lambda)=|\det(\boldsymbol{b}_1^*,\cdots,\boldsymbol{b}_n^*)| \tag{4.37}$$

である. また $i \neq j$ に対して $\boldsymbol{b}_i^*, \boldsymbol{b}_j^*$ は直交するから,

$$d(\Lambda) = \prod_{i=1}^{n} \|\boldsymbol{b}_i^*\| \tag{4.38}$$

となる. ここで, $\|\boldsymbol{b}_i^*\| \leq \|\boldsymbol{b}_i\|$ と $\|\boldsymbol{b}_i\| \leq 2^{(i-1)/2}\|\boldsymbol{b}_i^*\|$ より (2) が証明された.

(3)　(1) で $j = 1$ とし, $i = 1, \cdots, n$ として, 辺々かけると

$$\|\boldsymbol{b}_1\|^{2n} \leq 2^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} \|\boldsymbol{b}_i^*\|^2 \tag{4.39}$$

であり, 両辺を $\frac{1}{2n}$ 乗すると,

$$\|\boldsymbol{b}_1\| \leq 2^{\frac{n-1}{4}} \prod_{i=1}^{n} \|\boldsymbol{b}_i^*\|^{\frac{1}{n}} \tag{4.40}$$

ここで (4.38) より, (3) が得られる.

(4)　命題 4.14 より, $\boldsymbol{0}$ でない任意の $\boldsymbol{x} \in \Lambda$ に対し, ある $i(\leq n)$ が存在して $\|\boldsymbol{x}\|^2 \geq \|\boldsymbol{b}_i^*\|^2$ である. (1) で $j = 1$ とすれば,

$$\|\boldsymbol{b}_1\|^2 \leq 2^{i-1}\|\boldsymbol{b}_i^*\|^2 \leq 2^{n-1}\|\boldsymbol{b}_i^*\|^2 \leq 2^{n-1}\|\boldsymbol{x}\|^2 \tag{4.41}$$

であり (4) が証明された.

(5)　$\boldsymbol{x}_j = \sum_{i=1}^{n} r_{ij}\boldsymbol{b}_i$ と表せる. ここで $r_{ij} \in \mathcal{O}_F (1 \leq i \leq n, 1 \leq j \leq t)$ である. ここで, j を固定して, $i(j)$ を $r_{ij} \neq 0$ を満たす最大の i とする. 従って, $r_{i(j)+1,j} = \cdots = r_{nj} = 0$ である. このとき, 命題 4.14 より, $1 \leq j \leq t$ に対して,

$$\|\boldsymbol{x}_j\|^2 \geq \|\boldsymbol{b}_{i(j)}^*\|^2 \tag{4.42}$$

である. ここで $\boldsymbol{x}_j$ を $i(1) \leq \cdots \leq i(t)$ となるように並びかえて, 改めて $\boldsymbol{x}_j$ とする. このとき $1 \leq j \leq t$ に対して, $j \leq i(j)$ である. もし $j > i(j)$ となる j があれば, $j - 1 \geq i(j)$ であるから, $\boldsymbol{x}_1, \cdots, \boldsymbol{x}_j$ はすべて $\mathcal{O}_F\boldsymbol{b}_1 + \cdots + \mathcal{O}_F\boldsymbol{b}_{j-1}$ の元となり, 線形独立であることに反する.

ここで, $j = 1, \cdots, t$ に対して, $j \leq i(j)$, (1) , (4.42) より,

$$\|\boldsymbol{b}_j\|^2 \leq 2^{i(j)-1} \cdot \|\boldsymbol{b}_{i(j)}^*\|^2 \leq 2^{n-1} \cdot \|\boldsymbol{b}_{i(j)}^*\|^2 \leq 2^{n-1} \cdot \|\boldsymbol{x}_j\|^2 \tag{4.43}$$

であり, (5) が証明された. ■

虚二次体における LLL 簡約基底は, いつも存在するとは限らない. これについて, 次節で述べる.

4.5 擬 LLL 簡約基底

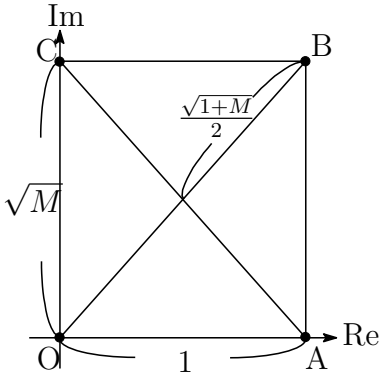
LLL 簡約基底が存在するための十分条件を調べる. 有理整数環 $\mathbb{Z}$ の場合, 任意の実数との差の絶対値は $\frac{1}{2}$ 以下である. しかし, 虚二次体の整数環 $\mathcal{O}_F$ の場合, 任意の複素数との差の絶対値は $\frac{1}{2}$ 以下とはならないことに注意しなければならない.

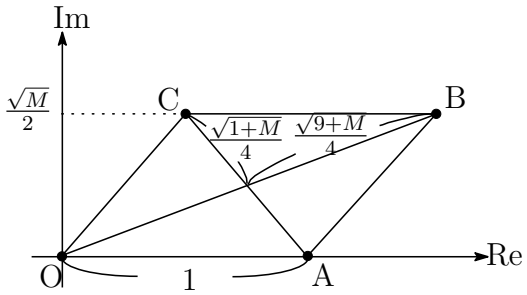
4.5.1 虚二次体の整数と複素数との差の絶対値

虚二次体 $\mathbb{Q}(\sqrt{m})(m<0, m$ は平方因子をもたない) に対して, $M := -m$ とおくと, M は平方因子をもたない正整数となる. 虚二次体の整数環は $\bmod 4$ で 2 つの場合に分けられるので, それぞれに対して, 複素数との差の絶対値について以下で述べる.

$m \not\equiv 1 \pmod 4$ すなわち $M \not\equiv 3 \pmod 4$ の場合, $\Pi := \{a + b\sqrt{m} \mid 0 \le a, b \le 1\} \subset \mathbb{R}^2$ とすると, 任意の $\mu \in \Pi$ に対して, $\{\alpha \in \mathbb{R}^2 \mid |\mu - \alpha| \le \frac{\sqrt{1+M}}{2}\} \cap \mathcal{O}_F \neq \emptyset$ である. すなわち $\{\mu\}$ を複素数 μ に一番近い整数 $\mathcal{O}_F$ の元とすると, $|\mu - \{\mu\}| \le \frac{\sqrt{1+M}}{2}$ である.

$m \equiv 1 \pmod 4$ すなわち $M \equiv 3 \pmod 4$ の場合, $\Pi := \{\frac{a+b\sqrt{m}}{2} \mid 0 \le a, b \le 1\} \subset \mathbb{R}^2$ とすると, 任意の $\mu \in \Pi$ (for $1 \le j < i \le n$) に対して, $\{\alpha \in \mathbb{R}^2 \mid |\mu - \alpha| \le \frac{\sqrt{9+M}}{4}\} \cap \mathcal{O}_F \neq \emptyset$ である. すなわち $|\mu - \{\mu\}| \le \frac{\sqrt{9+M}}{4}$ である.





命題 4.16 虚二次体 $F = \mathbb{Q}(\sqrt{m})(m<0, m$ は平方因子をもたない) に対して, $M := -m$ とおく. このとき, 任意の複素数と F の整数との差の絶対値について, $\{\mu\}$ を複素数 μ に一番近い整数 $\mathcal{O}_F$ の元とすると, 次が成立する.

(1) $m \not\equiv 1 \pmod 4$ すなわち $M \not\equiv 3 \pmod 4$ の場合,

$$\left|\mu - \{\mu\}\right| \le \frac{\sqrt{1+M}}{2}, \tag{4.44}$$

(2) $m \equiv 1 \pmod 4$ すなわち $M \equiv 3 \pmod 4$ の場合,

$$\left|\mu - \{\mu\}\right| \leq \frac{\sqrt{9+M}}{4}. \tag{4.45}$$

4.5.2 基底簡約アルゴリズム

はじめに定数 μ_{ij}, ベクトル空間 F^n の直交基底のベクトル $\boldsymbol{b}_i^*$ を (4.11) により計算する. このとき, LLL 簡約基底が帰納的に構成される. その帰納法は簡約基底のベクトルの個数 n による. 最初の変数は $m = 2$ とする. $m > n$ の場合, その手続きは終了する. このアルゴリズムの手順は次の 3 つである:

(Step A_m) $\mu_{m,m-1}$ の値が $|\mu_{m,m-1}| \leq \frac{1}{2}$ となるようにする. もし $|\mu_{m,m-1}| > \frac{1}{2}$ ならば, $\boldsymbol{b}_m - \{\mu_{m,m-1}\}\boldsymbol{b}_{m-1}$ をあらたに $\boldsymbol{b}_m$ とする. ここで $\{x\}$ は複素数 x に一番近い整数 $\mathcal{O}_F$ の元である. このとき, $\mu_{m,m-1} - \{\mu_{m,m-1}\}$ があらたな $\mu_{m,m-1}$ となり, $|\mu_{m,m-1}| \leq \frac{1}{2}$ とする. すべての $\boldsymbol{b}_i^*$ は不変のままである.

(Step B_m) $i = m$ に対して, (4.14) が成立するならば (Step C_m) に進む. そうでなければ, $\boldsymbol{b}_{m-1}$ と $\boldsymbol{b}_m$ を入れ替える. $m > 2$ の場合は (Step A_{m-1}) に, $m = 2$ の場合は (Step A_m) に行く.

(Step C_m) ((Step A_m) と同様に) $j = m-2, m-3, \cdots, 1$ に対して, μ_{mj} の値が $|\mu_{mj}| \leq \frac{1}{2}$ となるようにする. その後, (Step A_{m+1}) に行く. $m+1 > n$ ならばアルゴリズムは終了する.

(Step A_m) において, 常に $|\mu_{m,m-1}| \leq \frac{1}{2}$ となるとは限らない. 同様に, (Step C_m) において, 常に $|\mu_{mj}| \leq \frac{1}{2}$ となるとは限らない. これらにより, LLL 簡約基底は常に存在するとは限らないことが分かる. そこで, これらのステップの条件を満たすように定義を改良する必要がある.

注 4.17 2.4 節 (26 ページ) で示した $\mathbb{R}^n$ 内における格子での基底簡約アルゴリズムとの相違点は, (Step A_m) と (Step C_m) で, 複素数 x に対してそれに一番近い整数の元を $\{x\}$

とすることである. これ以外は同じである.

命題 4.16 により, 次の命題を得る.

命題 4.18　定義 4.12 における (4.13) は, 次のように改良すれば, 基底簡約アルゴリズムの (Step A_m) と (Step C_m) においても同様に修正することにより, 1 回の計算で, これらのステップにおける条件を満足させることができる.

(1)　$m \not\equiv 1 \pmod 4$ すなわち $M \not\equiv 3 \pmod 4$ の場合,

$$\left|\mu_{ij}\right| \leq \frac{\sqrt{1+M}}{2}, \tag{4.46}$$

(2)　$m \equiv 1 \pmod 4$ すなわち $M \equiv 3 \pmod 4$ の場合,

$$\left|\mu_{ij}\right| \leq \frac{\sqrt{9+M}}{4}. \tag{4.47}$$

4.5.3　擬 LLL 簡約基底

LLL 簡約基底の定義 (定義 4.12) における (4.14) は次と同値である.

$$\|\boldsymbol{b}_i^*\|^2 \geq \left(\frac{3}{4} - |\mu_{i,i-1}|^2\right) \|\boldsymbol{b}_{i-1}^*\|^2. \tag{4.48}$$

この不等式において, $\frac{3}{4} - |\mu_{i,i-1}|^2 \leq 0$ となると, この不等式がいつでも成立することになり, 意味をもたなくなる. 従って, 以降

$$\frac{3}{4} > |\mu_{i,i-1}|^2, \tag{4.49}$$

の下で考えていく.

$m \not\equiv 1 \pmod 4$ すなわち $M \not\equiv 3 \pmod 4$ の場合, (4.46), (4.49) を同時にみたす $M = 1$ である. $m \equiv 1 \pmod 4$ すなわち $M \equiv 3 \pmod 4$ の場合, (4.47), (4.49) を同時にみたす M は存在しない. 従って, $M = 1$ のときについて常に存在する簡約基底を以下で定義する.

定義 4.19 [6, p178]　$F = \mathbb{Q}(\sqrt{-1})$ とする. また, $\Lambda = \mathcal{O}_F\boldsymbol{b}_1 + \cdots + \mathcal{O}_F\boldsymbol{b}_n$ とする. Λ の基底 $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ が**擬 LLL 簡約基底**であるとは, 定義 4.10 における, 直交基底におけるベクトル $\boldsymbol{b}_1^*, \cdots, \boldsymbol{b}_n^*$ が, 条件 (4.14) および次の不等式を満たすときである.

$$|\mu_{ij}| \leq \frac{\sqrt{2}}{2} \quad (1 \leq j < i \leq n). \tag{4.50}$$

系 4.20　$F=\mathbb{Q}(\sqrt{-1})$ とする. 定理 4.3 で $m=-1$ とすると, 次が得られる.

$$\mathcal{O}_F=\mathbb{Z}[\sqrt{-1}]=\{a+b\sqrt{-1}\mid a,b\in\mathbb{Z}\}. \tag{4.51}$$

命題 4.21 [5]　$F=\mathbb{Q}(\sqrt{-1})$ とする. $(\boldsymbol{b}_1,\cdots,\boldsymbol{b}_n)$ を Λ の擬 LLL 簡約基底とし, また, $\boldsymbol{b}_i^*$ $(i=1,2,\cdots,n)$, μ_{ij} は定義 4.10 で定義した通りとする. このとき次が成立する :

$$(1)\quad \|\boldsymbol{b}_j\|^2\le 4^{i-1}\|\boldsymbol{b}_i^*\|^2\ \ (1\le j\le i\le n), \tag{4.52}$$

$$(2)\quad d(\Lambda)\le\prod_{i=1}^{n}\|\boldsymbol{b}_i\|\le(2^n-1)d(\Lambda), \tag{4.53}$$

$$(3)\quad \|\boldsymbol{b}_1\|\le\left(\frac{4^n-1}{3}\right)^{\frac{1}{2n}}d(\Lambda)^{\frac{1}{n}}, \tag{4.54}$$

$$(4)\quad \|\boldsymbol{b}_1\|^2\le 4^{n-1}\|\boldsymbol{x}\|^2\ \ \text{for}\ {}^{\forall}\boldsymbol{x}\in\Lambda,\ \boldsymbol{x}\neq\boldsymbol{0}, \tag{4.55}$$

$$(5)\quad \|\boldsymbol{b}_j\|^2\le 4^{n-1}\max\{\|\boldsymbol{x}_1\|^2,\cdots,\|\boldsymbol{x}_t\|^2\}\ (1\le j\le t\le n\ \text{で},\ \boldsymbol{x}_1,\cdots,\boldsymbol{x}_t\ \text{は線型独立}). \tag{4.56}$$

4.6　擬 LLL 簡約基底の存在性

虚二次体 $F=\mathbb{Q}(\sqrt{m})$ $(m<0, m$ は平方因子をもたない$)$ の場合, 4.5.2 で述べたように, LLL 簡約基底を求めるアルゴリズムが停止してしまう場合がある. そのため, $F=\mathbb{Q}(\sqrt{-1})$ のとき, アルゴリズムを次のように変更する.

はじめに定数 μ_{ij}, ベクトル空間 F^n の直交基底のベクトル $\boldsymbol{b}_i^*$ を (4.11) により計算する. このとき, 擬 LLL 簡約基底が帰納的に構成される. その帰納法は簡約基底のベクトルの個数 n による. 最初の変数は $m=2$ とする. $m>n$ の場合, その手続きは終了する. このアルゴリズムの手順は次の 3 つである. (Step A_m における $|\mu_{m,m-1}|$, Step C_m における $|\mu_{mj}|$ のとり得る値の範囲が変わっている.):

(Step A_m) $\mu_{m,m-1}$ の値が $|\mu_{m,m-1}|\le\frac{\sqrt{2}}{2}$ となるようにする. もし $|\mu_{m,m-1}|>\frac{\sqrt{2}}{2}$ ならば, $\boldsymbol{b}_m-\{\mu_{m,m-1}\}\boldsymbol{b}_{m-1}$ をあらたに $\boldsymbol{b}_m$ とする. ここで $\{x\}$ は複素数 x に一番近い整数 $\mathcal{O}_F$ の

元である. このとき, $\mu_{m,m-1} - \{\mu_{m,m-1}\}$ があらたな $\mu_{m,m-1}$ となり, $|\mu_{m,m-1}| \leq \frac{\sqrt{2}}{2}$ とすることができる. すべての $\boldsymbol{b}_i^*$ は不変のままである.

(Step B_m) $i = m$ に対して, (4.14) が成立するならば (Step C_m) に進む. そうでなければ, $\boldsymbol{b}_{m-1}$ と $\boldsymbol{b}_m$ を入れ替える. $m > 2$ の場合は (Step A_{m-1}) に, $m = 2$ の場合は (Step A_m) に行く.

(Step C_m) ((Step A_m) と同様に) $j = m-2, m-3, \cdots, 1$ に対して, μ_{mj} の値が $|\mu_{mj}| \leq \frac{\sqrt{2}}{2}$ となるようにする. その後, (Step A_{m+1}) に行く. $m+1 > n$ ならばアルゴリズムは終了する.

アルゴリズムが有限回の計算で終了することについて以下で述べる. (Step A_m), (Step C_m) は, 1 回の計算で, 必ず条件を満たす. (Step B_m) が有限回の計算で実現できることを証明すれば, このアルゴリズムは有限回の計算で終了し, 擬 LLL 簡約基底の存在が証明されることになる. 以下でこれを証明する.

アルゴリズムのなかで, $\boldsymbol{b}_i^*$ は成分を使って表す必要はない. そのノルムの 2 乗 $\|\boldsymbol{b}_i\|^2 = (\boldsymbol{b}_i^*, \boldsymbol{b}_i^*)$ のみ使用される. このアルゴリズムが終了することを以下で示す. (2.28) と同様に

$$D_i := \det(\boldsymbol{b}_\mu \cdot \boldsymbol{b}_\nu)_{1 \leq \mu, \nu \leq i} \quad (1 \leq i \leq n) \tag{4.57}$$

を, $d(\Lambda)^2 (= D_n)$ の小行列式とし, また (2.29) と同様に

$$D := \prod_{j=1}^{n-1} D_j \tag{4.58}$$

とする. (1.5), (4.10) によって,

$$D_i = \prod_{j=1}^{i} \|\boldsymbol{b}_j^*\|^2 \quad (1 \leq i \leq n) \tag{4.59}$$

を得る. (Step B_m) において, $\boldsymbol{b}_{m-1}$ と $\boldsymbol{b}_m$ を交換するたびに, 他のすべての D_i は不変のままであるが, D_{m-1} の値は $\frac{3}{4}$ 未満になる. 従って, D の値も $\frac{3}{4}$ 未満になる. しかし, D_i に対し,

$$S_i = 2^{-i(i-1)/2} \cdot m(\Lambda), \tag{4.60}$$

また, (2.32) と同様に

$$m(\Lambda) := \min\left\{ \ \|\boldsymbol{x}\|^2 \ \middle|\ \boldsymbol{x} \in \Lambda, \boldsymbol{x} \neq \boldsymbol{0} \ \right\}, \tag{4.61}$$

とする. このとき, 次が成立する.

$$D_i \geq S_i > 0 \ \ (1 \leq i \leq n). \tag{4.62}$$

以下で, S_i を求めていく.

定義 4.22　格子 $\Lambda = \sum_{i=1}^{n} \mathcal{O}_F \boldsymbol{b}_i$, $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \in \mathcal{B}_\Lambda$ に対して, **ハミルトン行列** (Hermitian matrix) $B = (b_{ij}) \in M_n(\mathbb{C})$ および**ハミルトン形式** (Hermitian form) を次で定義する.

$$b_{ij} = \boldsymbol{b}_i \cdot \boldsymbol{b}_j, \tag{4.63}$$

$$f(\boldsymbol{x}) = \sum_{1 \leq i,j \leq n} b_{ij} x_i \overline{x}_j. \tag{4.64}$$

ここで, $\boldsymbol{x} = (x_1, \cdots, x_n) \in F^n$ であり, $\overline{x}_i$ は x_i の共役な複素数とする.

命題 4.23　$\boldsymbol{x} \in \Lambda$, $\boldsymbol{x} = x_1\boldsymbol{b}_1 + \cdots + x_n\boldsymbol{b}_n$ に対して, 次が成立する.

$$f(\boldsymbol{x}) = \|\boldsymbol{x}\|^2. \tag{4.65}$$

従って, f は正定値となる.

以下で, 古典的な正定値二次形式の結果をガウスの数体への一般化を行う. 従って, エルミート形式を考える必要がある. 以後, この形式の最小値を考える. $\mathcal{O}_F$-格子の判別式の 2 乗の下界 S_n の具体的な表示を明らかにした. 以後述べる内容や証明の考え方は [9] による.

(4.7) によるエルミート積の性質を適用したり, 複素数の絶対値の基本的な性質を考えることにより, 次の補題を得る.

補題 4.24

$$f(x_1, x_2) = b_{11}|x_1|^2 + b_{12}x_1\overline{x}_2 + b_{21}\overline{x}_1x_2 + b_{22}|x_2|^2 \tag{4.66}$$

を正定値エルミート形式とする. このとき,

$$f(x_1, x_2) = b_{11}\left|x_1 + \frac{b_{21}}{b_{11}}x_2\right|^2 + \frac{b_{11}b_{22} - |b_{12}|^2}{b_{11}}|x_2|^2. \tag{4.67}$$

が成立する.

補題 4.25　$F=\mathbb{Q}(\sqrt{-1})$, $\mathcal{O}_F$ を F の整数環とする. $\alpha\in F$ に対して, $u\in\mathcal{O}_F$ で

$$|u+\alpha|\leq\frac{\sqrt{2}}{2}. \tag{4.68}$$

を満たすものが存在する.

これらにより, 次の補題を得る.

補題 4.26　f を (4.66) により得られる正定値エルミート形式とする. このとき, $(u_1,u_2)\neq(0,0)$ で

$$f(u_1,u_2)\leq(2D_2)^{\frac{1}{2}}, \tag{4.69}$$

をみたすものが存在する. ここで,

$$D_2=b_{11}b_{22}-|b_{12}|^2, \tag{4.70}$$

である.

証明　必要ならば同値な形式を考えることにより,

$$M(f)=\inf_{u_1,u_2\in\mathcal{O}_F}f(u_1,u_2)=b_{11}, \tag{4.71}$$

としてよい. ここで $(u_1,u_2)\neq(0,0)$ であり, (4.67) より,

$$f(x_1,x_2)=b_{11}\left|x_1+\frac{b_{21}}{b_{11}}x_2\right|^2+\frac{D_2}{b_{11}}|x_2|^2. \tag{4.72}$$

を得る. $u_2=1$ とおいて, 補題 4.25 より, $u_1\in\mathcal{O}_F$ で

$$\left|u_1+\frac{b_{21}}{b_{11}}\right|\leq\frac{\sqrt{2}}{2}. \tag{4.73}$$

を満たすものをとることができる. このとき,

$$f(u_1,1)\geq b_{11}, \tag{4.74}$$

であり, 一方で,

$$f(u_1,1)\leq\frac{1}{2}b_{11}+\frac{D_2}{b_{11}}. \tag{4.75}$$

であるから,

$$\frac{D_2}{b_{11}}\geq\frac{1}{2}b_{11}, \tag{4.76}$$

すなわち

$$b_{11}^2 \leq 2D_2, \tag{4.77}$$

を得る. また, (4.71) により, $f(u_1, u_2) \leq (2D_2)^{\frac{1}{2}}$ を得る. ■

この議論は, 次の命題に拡張できる.

命題 4.27　正定値エルミート形式

$$f(\boldsymbol{x}) = \sum_{1 \leq i,j \leq n} b_{ij} x_i \overline{x}_j \tag{4.78}$$

は, 任意の $\boldsymbol{u} \in {\mathcal{O}_F}^n, \boldsymbol{u} \neq \boldsymbol{0}$ に対して,

$$|f(\boldsymbol{u})| \leq 2^{(n-1)/2} {D_n}^{1/n}, \tag{4.79}$$

を満たす. ここで,

$$D_n = \det(b_{ij})_{1 \leq i,j \leq n} \tag{4.80}$$

である.

証明　補題 4.26 の証明の通り, 任意の $\boldsymbol{u} \in \mathcal{O}_F, \boldsymbol{u} \neq \boldsymbol{0}$ に対して

$$b_{11} \leq f(\boldsymbol{u}) \tag{4.81}$$

としてよい. このとき,

$$f(\boldsymbol{x}) = b_{11} \left| x_1 + \frac{b_{21}}{b_{11}} x_2 + \cdots + \frac{b_{n1}}{b_{11}} x_n \right|^2 + g(x_2, \cdots, x_n), \tag{4.82}$$

を表せる. ここで $g(x_2, \cdots, x_n)$ は判別式 D_n/b_{11} である定値エルミート形式である. $n-1$ 個の変数の形式に対して, すでに証明されているとしてよい, このとき, すべてが 0 ではない $u_2, \cdots, u_n \in \mathcal{O}_F$ で,

$$g(u_2, \cdots, u_n) \leq 2^{(n-2)/2} \left(\frac{D_n}{b_{11}} \right)^{1/(n-1)}. \tag{4.83}$$

を満たすものが存在する. 補題 4.25 により, $u_1 \in \mathcal{O}_F$ を

$$\left| u_1 + \frac{b_{21}}{b_{11}} u_2 + \cdots + \frac{b_{n1}}{b_{11}} u_n \right| \leq \frac{\sqrt{2}}{2}, \tag{4.84}$$

を満たすようにとると,

$$b_{11} \leq f(\boldsymbol{u}) \leq \frac{b_{11}}{2} + 2^{(n-2)/2} \left(\frac{D_n}{b_{11}} \right)^{1/(n-1)}, \tag{4.85}$$

となるから,

$$b_{11} \leq 2^{(n-1)/2} {D_n}^{1/n}. \tag{4.86}$$

を得る.

いま, $d(\Lambda)$ は (1.5) によって定義されており, $D_n = \{d(\Lambda)\}^2$ である. (4.57) によって得られる D_n が下界をもつことを証明するために, $m(\Lambda)$ を (4.61) 式で定義すると, これは正の実数である. $i > 0$ に対して, D_i をベクトル空間 $\sum_{j=1}^{i} F\boldsymbol{b}_j$ 内で, $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_i$ で張られる階数 i の $\mathcal{O}_F$-格子の判別式の 2 乗である.

命題 4.27 により, この格子は $\|\boldsymbol{x}\|^2 \leq 2^{(n-1)/2} {D_n}^{1/n}$ である $\boldsymbol{x} \neq \boldsymbol{0}$ が存在するから, 次の定理を得る.

定理 4.28 [6, p180] S_i を $\mathcal{O}_F$-格子の判別式の 2 乗 D_i の下界とする. このとき,

$$2^{-i(i-1)/2} \cdot m(\Lambda)^i \leq D_i, \tag{4.87}$$

すなわち, (4.60) 式が成立する.

この定理 4.28 で $n = 1, 2, \cdots$ とすると, $D = \prod_{i=1}^{n} D_i$ に対して, D は下界 $S = \prod_{i=1}^{n} S_i$ をもつことが分かる. 従って, 格子基底簡約アルゴリズムは有限回の計算により終了することが分かる. よって, 次の定理を得る.

定理 4.29 $F = \mathbb{Q}(\sqrt{-1})$ のとき, 擬 LLL 簡約基底は常に存在する.

第5章　格子基底簡約の教材化に向けて

本章では, 第2章から第4章までで議論した, 格子基底簡約の教材化について考察し, 格子基底簡約を教育に応用するための見方を提示する. まず, Λ の基底に対して, 格子しきつめが一対一に対応することを述べる. 次に, Λ の簡約基底に対応する格子しきつめを, 格子簡約しきつめと定義し, このしきつめが「効率的」であることを示す.

図形のしきつめについては, 小学校の算数から課題学習等で取りあげられいる. また, 中学校の数学においても, 関連する話題として, 図形の移動 (平行移動, 対称移動, 回転移動) があり, 児童生徒にとっても馴染みのある内容であり, 教材化が期待できる. また, しきつめの手順も考えることは, 児童・生徒の思考力の育成に役立つと考えられる.

5.1　格子しきつめ

n 次元ユークリッド空間 $\mathbb{R}^n$ を, 格子の基本領域でしきつめる問題を考える. Λ の1つの基底を与えることと, しきつめを与えることが同値であることを示す. つまり, 基底を与えることは, 基本的な移動を与えることになる. 特に, 第2章で考えた簡約基底を与えれば, 「効率的に」しきつめができることを示す. これを格子簡約しきつめと定義する. 同様の考え方で, $F^n(\subset \mathbb{C}^n)$ において, 著者らが構築した虚二次体における簡約基底に対応する簡約しきつめを提示することができる.

定義 5.1　格子 Λ に対して, $(\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n) \in \mathcal{M}_\Lambda$ とする. このとき

$$\Pi_{\boldsymbol{0}}(\Lambda) := \left\{ \ k_1\boldsymbol{e}_1 + \cdots + k_n\boldsymbol{e}_n \ \middle| \ 0 \leq k_1, \cdots, k_n < 1 \ \right\} \tag{5.1}$$

を Λ の**基本領域**という. また, この基本領域を $\boldsymbol{x} \in \Lambda$ だけ平行移動した領域を $\Pi_{\boldsymbol{x}}(\Lambda)$ で表す. すなわち,

$$\Pi_{\boldsymbol{x}}(\Lambda) = \left\{ \ \boldsymbol{x} + k_1\boldsymbol{e}_1 + \cdots + k_n\boldsymbol{e}_n \ \middle| \ 0 \leq k_1, \cdots, k_n < 1 \ \right\} \tag{5.2}$$

である.

定義 5.2　格子 Λ に対して, $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \in \mathcal{B}_\Lambda$ とする. (5.1) 式で定義された Λ の基本領域 $\Pi_0(\Lambda)$ を $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ に対して, それぞれ整数倍の和の方向に平行移動して, 重なる部分がなく平面全体を覆いつくすことを**格子しきつめ**という.

また, 格子しきつめができる, すなわち, 任意の $\boldsymbol{x}_1, \boldsymbol{x}_2 \in \Lambda$, $\boldsymbol{x}_1 \neq \boldsymbol{x}_2$ に対して,

$$\Pi_{\boldsymbol{x}_1}(\Lambda) \cap \Pi_{\boldsymbol{x}_2}(\Lambda) \neq \emptyset \tag{5.3}$$

であり, かつ,

$$\bigcup_{\boldsymbol{x} \in \Lambda} \Pi_{\boldsymbol{x}}(\Lambda) = \Lambda, \tag{5.4}$$

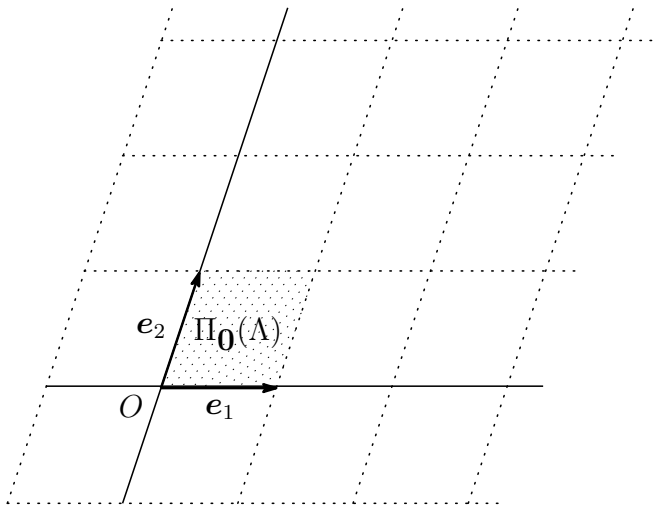
であるとき, **格子しきつめ可能**であるという.

この定義より, Λ の基底に対して, 格子しきつめが一対一に対応している.

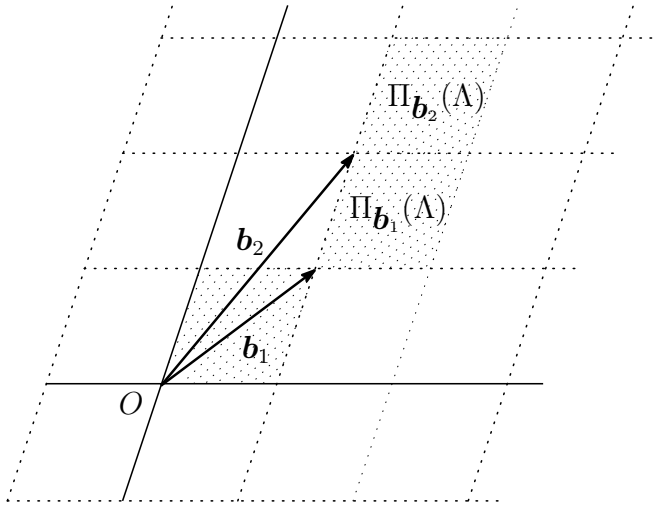
例 5.3　$\Lambda = \mathbb{Z}\boldsymbol{b}_1 + \mathbb{Z}\boldsymbol{b}_2$, $\boldsymbol{b}_1 = (4,3), \boldsymbol{b}_2 = (5,6)$ とする. このとき, $\boldsymbol{e}_1 = 2\boldsymbol{b}_1 - \boldsymbol{b}_2 = (3,0), \boldsymbol{e}_2 = -\boldsymbol{b}_1 + \boldsymbol{b}_2 = (1,3)$ に対して,

$$\begin{bmatrix} \boldsymbol{e}_1 \\ \boldsymbol{e}_2 \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{bmatrix} \tag{5.5}$$

であり, $\det \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} = 1 \in \mathbb{Z}$ より, この行列は逆行列をもつ. 従って, $(\boldsymbol{e}_1, \boldsymbol{e}_2) \in \mathcal{B}_\Lambda$ となる. 実際, $(\boldsymbol{e}_1, \boldsymbol{e}_2) \in \mathcal{M}_\Lambda$ である. この場合, 基本領域 $\Pi_{\mathbf{0}}(\Lambda)$ は次の図のようになる.



さらに, $\Pi_{\boldsymbol{b}_1}(\Lambda)$, $\Pi_{\boldsymbol{b}_2}(\Lambda)$ は次の図のようになる.



命題 5.4　格子 Λ に対して, $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \in \mathcal{B}_\Lambda$ とする. (5.1) 式で定義された Λ の基本領域 $\Pi_{\mathbf{0}}(\Lambda)$ で格子しきつめが可能である.

証明　Λ に属する点 $\boldsymbol{x} \in \mathbb{Z}\boldsymbol{b}_1 + \cdots + \mathbb{Z}\boldsymbol{b}_n$ に対して, 領域 $\Pi_{\boldsymbol{x}}(\Lambda)$ を対応させれば, この対応は一対一であるから格子しきつめが可能であることがわかる. ■

5.2　格子簡約しきつめ

格子しきつめでは, 1 つの基底を構成する n 個のベクトルそれぞれの方向に整数倍だけ平行移動した領域に, 基本領域である平行四辺形を貼り付けていけば, 平面全体を覆うことになるが, 貼るための移動距離が長く「効率が悪い」しきつめになる.

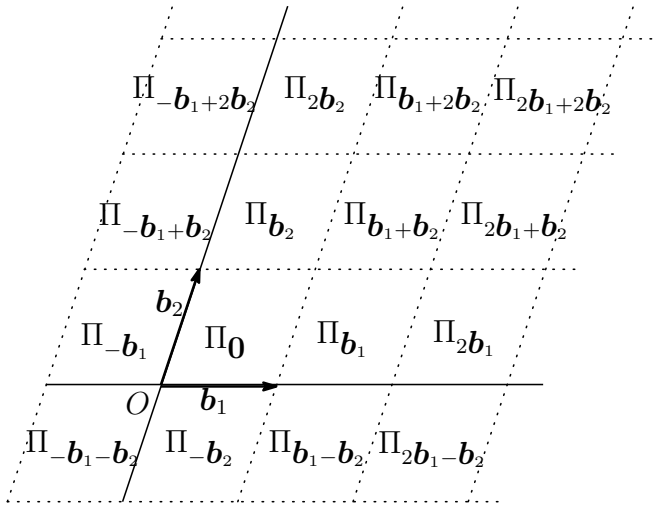
この問題を解決するには, 基底として簡約基底を用いればよいことを以下で説明する. 簡約基底は定義 2.6 で定義した Minkowski 簡約基底と, 定義 2.21 で定義した LLL 簡約基底がある. それぞれの簡約基底に対応した格子しきつめを次で定義する. 計算機で計算して基底を求めるには, すでに述べたように, LLL 簡約基底が実用的である.

簡約基底に対応する格子しきつめは, 効率的なしきつめの例となる. 効率的なしきつめの手順を考えることは, 児童生徒の思考力の育成に役立つと考えられる.

定義 5.5　格子 Λ に対して, $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \in \mathcal{M}_\Lambda$ とする. (5.1) 式で定義された Λ の基本領域 $\Pi_0(\Lambda)$ を $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ に対して, それぞれ整数倍の和の方向に平行移動して, 重な

る部分がなく平面全体を覆いつくすことを**格子 Minkowski 簡約しきつめ**という．また，$(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n) \in \mathcal{L}_\Lambda$ のとき，**格子 LLL 簡約しきつめ**という．これらを総称して**格子簡約しきつめ**という．

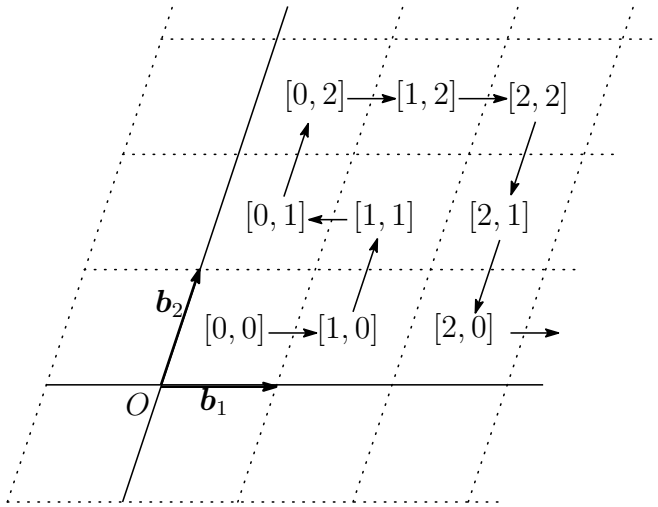
例 5.6　$\Lambda = \mathbb{Z}\boldsymbol{b}_1 + \mathbb{Z}\boldsymbol{b}_2$, $\boldsymbol{b}_1 = (3,0), \boldsymbol{b}_2 = (1,3)$ とすると $(\boldsymbol{b}_1, \boldsymbol{b}_2) \in \mathcal{M}_\Lambda$ である．このとき，領域 $\Pi_{\boldsymbol{x}}(\Lambda)$ $(\boldsymbol{x} \in \Lambda)$ を図示すると以下のようになる．ただし $\Pi_{\boldsymbol{x}}(\Lambda)$ を単に $\Pi_{\boldsymbol{x}}$ と表示している．



以下，簡単のために領域 $\Pi_{k_1\boldsymbol{b}_1+k_2\boldsymbol{b}_2}$ を $[k_1, k_2]$ と書くことにする．移動距離が最小となる手順の例として，

$[0,0] \to [1,0] \to [1,1] \to [0,1] \to [0,2] \to [1,2] \to [2,2] \to [2,1] \to [2,0] \to [3,0] \to \cdots$

が挙げられる．



第 4 章で示された, 著者らの研究により, 虚二次体への一般化によって得られた結果は, 格子 LLL 簡約しきつめにも応用できる. $\mathbb{C}^n$ 空間となるため, 図では表すことができないが, $\mathbb{R}$ 上 $2n$ 次元の空間内で格子 LLL 簡約しきつめを考えることができる.

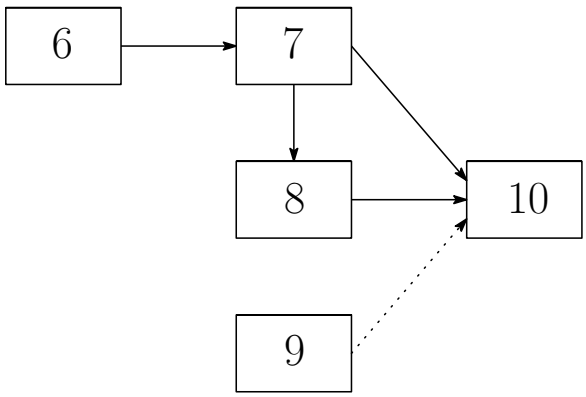
5.3 格子しきつめの教材化

本章で取り上げた平行四辺形による平面のしきつめは，学校でもよく取り上げられるテーマであるが, しきつめの手順, すなわち, どのような順番で平行四辺形をしきつめていくかについては考慮されていない. しきつめの手順, 特に効率的な手順を探る活動は, 「主体的・対話的で深い学び」の格好の素材を与えるものと思われる. 本論文における格子基底簡約の研究成果は, その教材化に寄与するものであると考える. この素材により, 中学校では, 図形の移動の 1 つである平行移動の概念を理解させること. 高等学校では, 平面上の任意のベクトルは線形独立な 2 つのベクトルの線形結合で一意的に表すことができることの理解を深めること等が期待される.

第II部

格子多角形とその教育への応用

第 II 部における, 各章の数学の内容の部分の関係は下の図のようになる.



第 6 章は第 7 章の準備であり, 定理 6.5(Scherrer) を第 7 章の補題 7.2 に使用する. 第 7 章は第 8 章の準備であり, 補題 7.2 を第 8 章の定理 8.2(Euler) に使用する. 第 7 章と第 8 章は第 10 章の準備であり, 補題 7.5 と定理 8.2(Euler) を定理 10.4 に使用する. 第 10 章には著者らによって得られた結果が含まれている. 第 6 章から第 8 章までは, [10] を参考にしてまとめた. 第 9 章は第 10 章の一般化である.

第6章　格子多角形とその教材化に向けて

第 II 部である本章以降は, $\mathbb{R}^2$ 内の格子 $\mathbb{Z}^2$ を考える. 格子の数学については [14], [16] 等で述べられている. これらの文献では, 格子多角形や円周上の格子点の個数などについて述べられているが, ヘロン三角形については記述がない. ヘロン三角形については, 第 9 章および第 10 章で考察する.

本章では, 格子多角形について述べる. まず, 古典的な結果であり有名なピックの定理を紹介する. この定理は, 格子多角形の面積を, 周上の格子点の数および内部にある格子点の数を使って表現するものである. この定理は, 小学校から大学, 一般まで幅広く, 「主体的・対話的で深い学び」を実現できる題材となり得ることを指摘する.

次に, 格子正多角形についての古典的な結果 (定理 6.5) を述べ, それを証明する. この定理は次章の議論に適用される. この定理は, 複数の補題からなるが, 証明はすべて背理法を用いている. 従って, これらの補題の証明は, 数学的な見方や考え方を育むのに適した例といえる.

6.1　ピックの定理

ここで述べる結果は, 古典的な結果である. 詳細は [10] などで述べられている.

定義 6.1　平面上の点 $(x, y) \in \mathbb{R}^2$ について, $x, y \in \mathbb{Q}$ であるとき, (x, y) を**有理点** (rational point) であるという. また, $x, y \in \mathbb{Z}$ であるとき, (x, y) を**格子点** (lattice point) であるという.

定義 6.2　格子点を頂点とする多角形を**格子多角形**といい, 特に, 格子点を頂点とする正多角形を**格子正多角形**という.

定義 6.3　2 つの格子多角形 P_1, P_2 が, 1 本の折れ線だけを共通の境界としてもつとき, これらをあわせて得られる格子多角形を $P_1 + P_2$ で表す.

格子多角形 P の面積は次の公式 (ピックの定理) で与えられる.

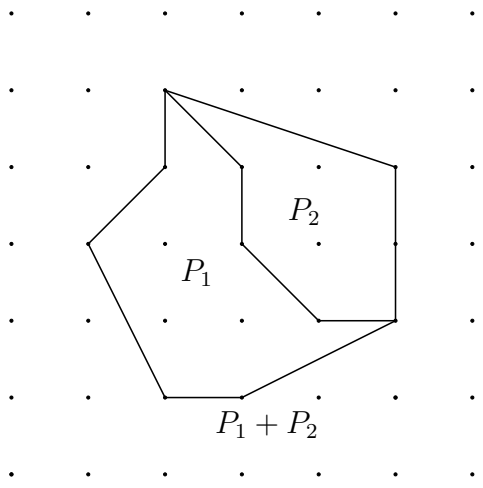
定理 6.4 [Pick, 1899]　P を格子多角形 (凸とは限らない) とする. このとき P の面積 $A(P)$ は次の式で与えられる:

$$A(P) = \frac{1}{2}B(P) + I(P) - 1, \tag{6.1}$$

ここで $B(P)$ は多角形の周上の格子点の数, $I(P)$ は内部にある格子点の数である.

証明　(i) 格子三角形が周上にも内部にも他の格子点を含まなければ, この三角形を面積は $\frac{1}{2}$ である. 従って, 内部に格子点を含まない三角形について (6.1) 式が成り立つ.

(ii) 2 つの格子多角形 P_1, P_2 が 1 本の折れ線だけを共通の境界としてもつとき, $P_1, P_2, P_1 + P_2$ に対して (6.1) 式が成り立つと仮定する. このとき, $A(P_1) + A(P_2) = A(P_1 + P_2)$ が成り立つことを証明する.



P_1 と P_2 の共通の境界である折れ線の両端以外の格子点は, $P_1 + P_2$ の内部の格子点であり, P_1, P_2 の周上にある格子点でもある. いずれの見方をしても (6.1) 式の右辺において, $\frac{1}{2} + \frac{1}{2} = 1$ に対応している.

P_1 と P_2 の共通の境界である折れ線の両端の格子点については, P_1, P_2 の両方で数えることなり, 重複する分を引けば, (6.1) 式の右辺の -1 に対応する.

格子多角形は, 周上の格子点, 内部の格子点を適当に線分で結んで, 内部に格子点をもたないようないくつかの三角形に分割できる. 従って, (i), (ii) から, 格子多角形の面積が (6.1) 式で得られることが示された. ■

6.2　ピックの定理の教材化

このピックの定理は, 教材化に適した題材である. 例えば, 面積の概念の理解を深めることをねらいとした授業設計が考えられる. 具体的な活動例として, 小学校では, 児童に好きな格子多角形を書かせ, その面積を求めた後, この定理の結果を使って改めて面積を求める活動が考えられる. 中学校では, 面積が $1/2$ である四角形が存在するかどうかを考えたり, 格子四角形で一番面積が小さいものを見つけたりする活動が考えられる. このような活動を通して, 児童生徒に数学の面白さや不思議さを感じさせることができる.

6.3　格子正多角形

次に, 格子正多角形にはどんなものがあるかを考える. 実際, 正方形しかないことが知られている.

定理 6.5 $[24, \text{Scherrer}, 1946]$　格子点を頂点とする正多角形は正方形に限る.

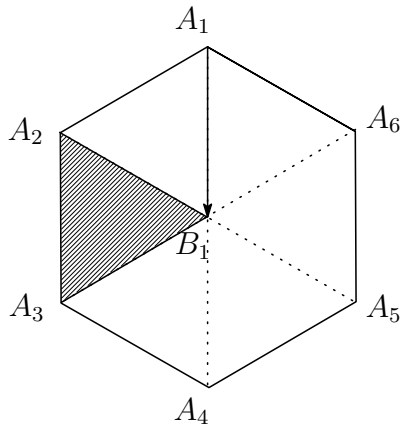
この定理の証明を, 補題 6.6〜補題 6.8 として述べる. 背理法により証明するが, 証明に用いる数学的発想が面白く生徒にも理解可能で, 証明自身が論理的な思考力を養うための教材となり得るため, その過程を示す.

補題 6.6　格子正三角形は存在しない.

証明　1 辺の長さが a である格子正三角形があるとする. この面積は $\frac{\sqrt{3}}{4}a^2$ である. a^2 は正の整数であるから, 面積 $\frac{\sqrt{3}}{4}a^2$ は無理数である. 一方, 定理 6.4 より, 格子多角形の面積は有理数であるから矛盾が生じる. 従って, 格子正三角形は存在しない. ■

補題 6.7　格子正六角形は存在しない.

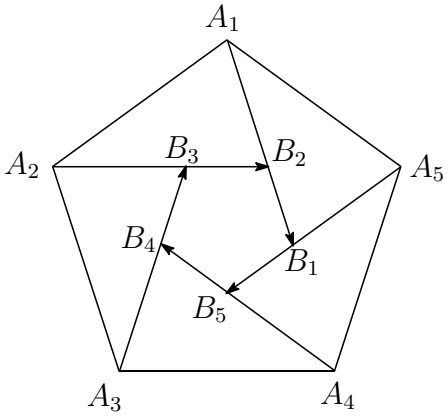
証明　格子正六角形が存在すると仮定する. 格子正多角形の 1 辺の長さは $\sqrt{m^2+n^2}\,(m, n \in \mathbb{Z})$ の形で表されるから, このような格子正六角形のうち, 1 辺の長さが最小のものが存在する. その 1 つを $A_1A_2A_3A_4A_5A_6$ とする.



点 A_1 を $\overrightarrow{A_2A_3}$ によって平行移動した点を B_1 とすると, 点 B_1 も格子点となる. このとき, 格子正三角形が存在することになり, 補題 6.6 に矛盾する. ■

補題 6.8　格子正 n 角形 $(n = 5, n \geq 7)$ は存在しない.

証明　格子正 n 角形 $(n = 5, n \geq 7)$ が存在すると仮定する. 補題 6.7 における格子正六角形の場合と同様に, 1 辺の長さが最小のものを考え, $A_1 \cdots A_n$ とする. $n \geq 5$ より, $\angle A_iA_{i+1}A_{i+2} > \frac{\pi}{2}$ $(i = 1, \cdots n,$ ただし $i+1, i+2$ が n を超える場合は n を引いた数とし, 以下同様とする.) だから, 点 B_i $(i = 1, \cdots, n)$ を内部に $\overrightarrow{A_iB_i} = \overrightarrow{A_{i+1}A_{i+2}}$ であるようにとれる. このとき, $B_1 \cdots B_n$ は $A_1 \cdots A_n$ の内部にある格子正 n 角形であり矛盾する. 例えば, $n = 5$ のとき次の図のようになり, 1 辺の長さが最小な格子正五角形を $A_1A_2A_3A_4A_5$ とすると, この内部に格子正五角形 $B_1B_2B_3B_4B_5$ が存在することとなり矛盾する. ■



6.4　格子正多角形の教材化

前節で考察した格子正多角形について, 定理 6.5 の証明は複数の補題からなるが, これらの証明は, 数学的な見方や考え方を育むのに適した例といえる. 育成したい数学的な見方として

- 格子点を頂点にもつ多角形で, 各辺の長さがすべて等しい図形に着目する.
- 格子正三角形の面積が, 有理数か無理数のいずれかであるという点に着目する.

が挙げられる. 次に, 育成したい数学的な考え方として

- 格子正 n 角形において, n の値のそれぞれに対して個々に調べようとする.
- 格子正 n 角形において, n の値によって統合的に考える.
- 証明しようとしている結論が成立しないと仮定して矛盾を導くことにより証明する (背理法の考え方).
- すでに証明された補題の結果を, 他の議論に適用できないかを考える.

が挙げられる.

第7章　円周上の有理点とその教材化に向けて

本章では, 第6章の定理6.5を適用して, ピタゴラス三角形の1鋭角とπとの比が無理数となることを証明する. これは既に知られている事実である. この事実より, 円周上に有理点が3個あれば, その円周上には無限個の有理点が存在することが分かる. 与えられた個数の有理点をもつ円の中心や半径を求める活動は, 中学生から大学生, 一般まで親しめる題材となると考えられる. 章の最後には, 教材化について論じる. なお, 本章の数学の部分については[10]を参考にした.

7.1　円周上の有理点の個数

定義 7.1　3辺の長さがすべて整数であるような直角三角形を**ピタゴラス三角形** (Pythagorean triangle) という.

定理6.5を用いると次の補題が得られる.

補題 7.2　αをピタゴラス三角形の1つの鋭角とすると, α/πは無理数である.

証明　αはピタゴラス三角形の鋭角だから, ある正の整数k, m, n $(k^2+m^2=n^2)$で

$$\cos\alpha = \frac{k}{n}, \quad \sin\alpha = \frac{m}{n} \tag{7.1}$$

と表すことができる. ここで, $\alpha/\pi \in \mathbb{Q}$と仮定すると

$$\frac{\alpha}{2\pi} = \frac{M}{N} \quad (\text{既約分数で}, M, N > 0) \tag{7.2}$$

と書ける. 点$p(n^N, 0)$を原点を中心とする角αの回転Tで次々と移して, p, Tp, T^2p, $\cdots$とすると, ちょうどN回目の移動で元の点pに戻る. すなわち, $T^np = p$であり, N個の点p, Tp, T^2p, $\cdots$, $T^{n-1}p$は正N角形の頂点となる.

また, 角 α の回転行列 T は,

$$\begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} = \begin{bmatrix} k/n & -m/n \\ m/n & k/n \end{bmatrix} \tag{7.3}$$

であり, $p(n^N, 0)$ だから, $Tp, T^2p, \cdots, T^{n-1}p$ はすべて格子点となる. 従って, これらの N 個の点は, 格子正 N 角形となる. 定理 6.5 より, $N = 4$ でなければならない. ところが α は鋭角だから, 不可能である. ■

任意の正整数 n に対して, n 個以上の格子点をのせた円周が存在する. これを次の定理として与える.

定理 7.3　任意の $n \in \mathbb{Z}, n > 0$ に対して, n 個以上の格子点をのせた円周が存在する.

証明　この定理を証明するためには, 補題 7.5 を示せばよい. 補題 7.5 を認めると, 無限個ある有理点のなかから, 有限個 (n 個) の点を選び, これらの点の座標となるすべての有理数について, その分母の最小公倍数 ℓ をかけて分母をはらうことにより, n 個の格子点を得る. これらの n 個の有理点は, 原点を中心に ℓ 倍に拡大された格子点へそれぞれ移ることになる. このことにより, この定理が証明される. ■

ここで, 次のことを指摘しておく.

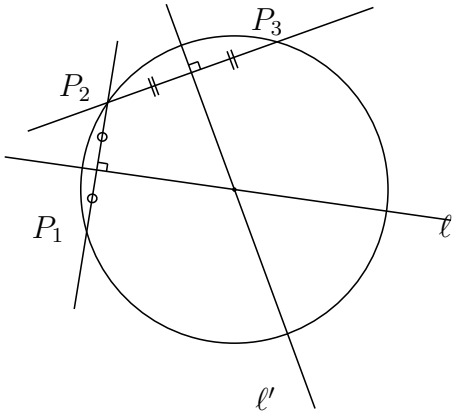
注 7.4　原点を中心とする円において, 円周上の有理点が与えられたとき, 適当に拡大することで, 格子点となる.

補題 7.5　円周上にある有理点の個数は, $0, 1, 2, \infty$ のいずれかである.

この補題の証明を, 補題 7.6〜補題 7.10 として述べる.

補題 7.6　3 個の有理点を通る円の中心は有理点である.

証明　円 C 上に 3 個の有理点 P_1, P_2, P_3 があるとする. このとき, 円 C の中心は, 線分 P_1P_2, 線分 P_2P_3 の垂直二等分線 ℓ, ℓ' の交点である.



直線 P_1P_2 および直線 P_2P_3 の傾きは有理数だから, それらにそれぞれ垂直な直線 ℓ, ℓ' の傾きも有理数である. また, 直線 ℓ は線分 P_1P_2 の中点 (これは有理点) を, 直線 ℓ' は線分 P_2P_3 の中点（これも有理点）を通るから, これらの直線の方程式は, すべて有理数係数となる. 従って, これら 2 本の直線の交点は有理数である. ■

補題 7.7　有理点が 1 個もない円が存在する.

証明　原点を中心として, 半径 r の 2 乗が有理数とならないような円の周上には有理点は一個もない (例えば $r^2 = \sqrt{2}$). ■

補題 7.8　有理点がちょうど 1 個の円が存在する.

証明　点 $(\sqrt{2}, 0)$ を中心とし, 原点を通る円周上には, 有理点は原点のみしか存在しないことを示す. 他に有理点がもう 1 個あると仮定する. このとき, x 軸に関して対称な 2 個の有理点が存在することになり, 合計 3 個（以上）有理点が存在することになる. このとき, 補題 7.6 より, この円の中心が有理点となり矛盾する. ■

補題 7.9　有理点がちょうど 2 個の円が存在する.

証明　点 $(\sqrt{2}, 0)$ を中心とし, $(0, 1)$, $(0, -1)$ を通る円周上には, ちょうど 2 個の有理点しかない. 他に有理点がもう 1 個あると仮定すると, 有理点が 3 個存在することになり, 補題 7.6 より, この円の中心が有理点となり矛盾する. ■

補題 7.10　円周上に有理点が 3 個存在すれば, その円周上には無限個の有理点が存在する.

証明　円周 C が, 少なくとも 3 個の有理点を通るとする. このとき, この円周上には無限個の有理点が存在することを示す. 補題 7.6 より, この円 C の中心は有理点である. C を平行移動して, 中心を原点とした円を C_0 とする. C 上の有理点はすべて C_0 上の有理点に移るから, 以下 C_0 で議論する.

α を 3 辺が 3, 4, 5 であるピタゴラス三角形の最小の内角とする. C_0 上の有理点を 1 つとり, この有理点を回転角 α で次々回転させる. 角 α の回転行列は

$$\begin{bmatrix} 4/5 & -3/5 \\ 3/5 & 4/5 \end{bmatrix} \tag{7.4}$$

であるから, C_0 上に次々に有理点が得られる. また α はピタゴラス三角形の 1 つの鋭角だから, 補題 7.2 より α と π の比は無理数である. だから, 決して同じ点が 2 回以上現れることはない. 従って, C_0 上には有理点が無限個存在することがわかり, これらの有理点に対応して, C 上にも有理点が無限個存在することがわかる. ■

7.2　円周上の格子点の教材化

補題 7.6 の証明は, 教材化につながる話題がある. まず, 中学校では, 有理数係数の 2 元 1 次連立方程式の解 (x, y) が有理数になることを証明する活動があげられる. 生徒それぞれが考えた証明を筋道をたてて発表する活動は, 論理的な考え方をする能力の育成につながると考えられる. 2 つの式で, それぞれ分母の最小公倍数を両辺にかけて, 整数係数の方程式にできる. さらに, 両辺を何倍かして, 1 つの文字の係数の絶対値を等しくできる. 加減法により, 着目した 1 つの文字が消去され, もう一方の文字に関する方程式が得られる. その方程式を解けば, 有理数の解が得られる. この活動により, 連立方程式を解く手順を振り返ることになり, この解法の理解につながる. また, 1 つの文字を消去し, もう一方の文字についての一次方程式において, その文字の係数が有理数となることに着目することにより, 有理数の理解につながる.

また, 高等学校では, 思考力の育成を目的として, 補題 7.6 の別証明を扱う活動も考えられる. 円の方程式で, 通る 3 点がすべて有理数ならば, その中心も有理数となることの別の理由を考えればよい.

中学校や高等学校の数学の授業において, 補題 7.7〜補題 7.9 を満たす円, すなわち有理点が 0 個, 1 個, 2 個である円を見つけさせる活動は生徒の興味をひくものとなるだろう. その活動の後, 有理点がちょうど 3 個である円を見つける課題を出し, 試行錯誤の後, 実際は有理点が 3 個のっている円が存在すれば, その円上には無限個の有理点があることを教師が説明する. このとき, 補題 7.10 の証明を参照すればよいが, ここでは, 回転行列 (7.4) を使用している.

現在, 行列については高等学校では学習しない内容であるため, 行列を使わない方法で考える. 有理点 (x, y) に対して, その回転移動後の座標を

$$\begin{pmatrix} x \\ y \end{pmatrix} \longrightarrow \begin{pmatrix} \frac{4x-3y}{5} \\ \frac{3x+4y}{5} \end{pmatrix} \tag{7.5}$$

として与えればよい. 移動後の点も有理点となり, $\{(4x-3y)/5\}^2+\{(3x+4y)/5\}^2 = x^2+y^2$ であるから, 移動後の点も同じ円周上に存在することが分かる. 一般に, ピタゴラス三角形の 3 辺の長さが a, b, c $(a^2 + b^2 = c^2)$ のとき, 有理点 (x, y) に対して, その回転移動後の座標を

$$\begin{pmatrix} x \\ y \end{pmatrix} \longrightarrow \begin{pmatrix} \frac{bx-ay}{c} \\ \frac{bx+ay}{c} \end{pmatrix} \tag{7.6}$$

として与えてもよい. $\{(bx - ay)/c\}^2 + \{(bx + ay)/c\}^2 = x^2 + y^2$ となる a, b, c の値を求める活動も考えられる.

第8章　内接多角形の性質

本章では, 初等幾何学で有名なトレミーの定理と, その応用として, オイラーの結果である円周上の無限個の点（特に有理点とは限らない）で, 相互の距離がすべて有理数となるような円が存在することについて述べる. これらはすでに知られた事実である. なお, 本章は [10] を参考にした.

まず, 説明の準備として, ユークリッド幾何学において有名なトレミーの定理を述べる.

補題 8.1 [Ptolemy]　円に内接する四角形 $ABCD$ において

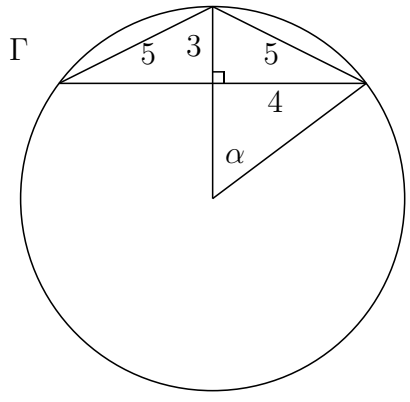
$$AB \cdot CD + BC \cdot AD = AC \cdot BD \tag{8.1}$$

が成り立つ.

補題 8.1 から, 次の定理 8.2 を得る.

定理 8.2 [Euler]　相互の距離がすべて有理数となるような無限個の点を含む円が存在する.

証明　3 辺の長さが例えば 5, 5, 8 の二等辺三角形の外接円 Γ の周上に, 直線距離で 5 離れた点を次々刻んでいく. 長さ 5 の弦を見込む中心角を α とする. このとき, $\frac{\alpha}{2}$ は 3 辺が 3, 4, 5 のピタゴラス三角形の 1 つの鋭角である.



補題 7.2 より $\frac{\alpha}{2}/\pi$ は無理数であるから, α と π の比は無理数である. 従って, 円周 Γ 上に距離が 5 離れた点を次々に刻んでいけば, 無限個の点が得られる. これらの点の間の距離はどれも有理数であることが, トレミーの定理 (補題 8.1) を用いて証明できる. ■

さらに次の系が得られる.

系 8.3 すべての正整数 n に対して, 相互の距離がすべて整数である n 個の点をもつ円が存在する.

トレミーの定理の証明は多くのものがあることが知られている. この定理の教材化は今後の課題となる. この定理 8.2 を改良した定理を第 10 章で示す.

第9章　菊池長良の公式とその教材化に向けて

本章では, 第1節で準備を行い, 第2節および第3節において, ヘロン三角形に関する話題として, 和算家である菊池長良の公式について考察する. 菊池の公式は, ヘロン三角形を表す式として江戸時代に紹介されていた. 著者らは, 田中 ([27],[28],[29]) の研究を踏まえて, 菊池の公式で表せない三角形が存在することを明らかにした. 第4節では, 和算を数学教育へ応用することについて論じた.

9.1　ヘロン三角形

定義 9.1　3辺の長さと面積が整数である三角形を, **ヘロン三角形** (Heronian triangle) という.

定義 9.2　3辺の長さの最大公約数が1であるようなヘロン三角形を, **原始ヘロン三角形** (primitive Heronian triangle) という.

定義 9.3　3辺の長さと面積が有理数である三角形を, **有理三角形** (rational triangle) という.

定義 9.4　3点が格子点となるヘロン三角形を, **格子ヘロン三角形** (lattice Heronian triangle) という.

9.2　菊池の公式

菊池長良について，田中 ([27], [28]) の研究によって次のことが明らかにされている. 菊池長良は仙台で活躍した和算家であり, 彼の主著は『算法整数起源抄』であるとされてい

る．この文献は, 整数図形の問題（整数術または生数術, いわゆる図形の整数論）で構成されている．このなかでヘロン三角形の 3 辺の長さを求める公式を与えている．扉に菊池宇太之丞長良閲，門人・金子左右平編輯となっている。菊池が門人に編集させたものであることがわかる．「起源」は理論を意味し,「抄」は要点を簡潔に述べたという意味である．さらに, 田中は同じ文献で, 菊池の研究結果 ([12]) として, ピタゴラス三角形の 3 辺の長さを与える公式を探求する第 1 問題と，ヘロン三角形の 3 辺の長さと面積を与える公式を探求する第 2 問題を挙げている．ここで，菊池における第 2 問題の解答を，菊池の公式として以下に示す.

公式 9.5 [*12*]　3 辺の長さを a, b, c, 面積を S とすると, ヘロン三角形は次の公式でつくられる.

(1) $a = r(v^2 + w^2), b = v(r^2 + w^2), c = (r + v)(w^2 - rv), S = rvw(r + v)(w^2 - rv)$,

(2) $a = r(v^2 + w^2), b = v(r^2 + w^2), c = (r - v)(w^2 + rv), S = rvw(r - v)(w^2 + rv)$.

ここで, r, v, w は正の整数である．ただし, 原始ヘロン三角形をつくるには 3 辺の最大公約数で約す.

9.3　菊池の公式の考察

田中は, この公式ですべてのヘロン三角形を表すことができるのか研究した．その後の研究成果として, 田中 ([29]) は, 菊池の公式ではすべての原始ヘロン三角形が, 直接に出てくるとは限らないことを指摘している．例えば公式 9.5(1) において, 3 辺の長さが $3, 4, 5$ である原始ヘロン三角形は, どの r, v, w の整数の組み合わせに対しても得られず, 実際に, $r = 1, v = 2, w = 2$ として, 3 辺の長さを 2 で割ることにより得られることを明らかにした.

ヘロン三角形の 3 辺の長さが与えられたとき, それらの値から菊池の公式における 3 変数を導く公式を補題として与える．これらの補題は著者らによる結果である.

補題 9.6 [*2*, 定理 1, p3]　菊池の公式 (公式 9.5)(1) において, 次の等式が成り立つ.

$$r^3 = \frac{(a - b + c)^2(a + b - c)}{4c(b - a + c)}, \tag{9.1}$$

$$v^3 = \frac{(b - a + c)^2(a + b - c)}{4c(a - b + c)}, \tag{9.2}$$

$$w^6 = \frac{(a+b+c)^3(a-b+c)(b-a+c)}{2^4c^2(a+b-c)}. \tag{9.3}$$

証明　$a+b+c, a+b-c$ を求めると,

$$a+b+c = 2w^2(r+v), \tag{9.4}$$

$$a+b-c = 2rv(r+v), \tag{9.5}$$

より, $(a+b+c)/(a+b-c) = w^2/rv$ となり,

$$w^2 = \frac{a+b+c}{a+b-c}rv \tag{9.6}$$

である. 従って,

$$a = r\left(v^2 + \frac{a+b+c}{a+b-c}rv\right), \tag{9.7}$$

$$b = v\left(r^2 + \frac{a+b+c}{a+b-c}rv\right), \tag{9.8}$$

となり, これらの比をとると,

$$\frac{a}{b} = \frac{(a+b+c)r + (a+b-c)v}{(a+b+c)v + (a+b-c)r} \tag{9.9}$$

となる. よって,

$$(a+b)(a-b+c)v = (a+b)(b-a+c)r \tag{9.10}$$

となる. ここで $a+b \neq 0$ だから,

$$(a-b+c)v = (b-a+c)r \tag{9.11}$$

である. この式と (9.5) より,

$$\begin{aligned}
(a-b+c)^2(a+b-c) &= (a-b+c)^2 \cdot 2rv(r+v) && (9.12)\\
&= 2\{(b-a+c)r\}^2 r + 2\{(b-a+c)r\}(a-b+c)r^2 && (9.13)\\
&= 2\{(b-a+c)r^2\}\{(b-a+c)r + (a-b+c)r\} && (9.14)\\
&= 2(b-a+c)r^2 \cdot 2cr && (9.15)\\
&= 4(b-a+c)cr^3. && (9.16)
\end{aligned}$$

ゆえに, (9.1) が得られる. 同様にして (9.5), (9.11) より, (9.2) が得られる. また, (9.6) の両辺を 3 乗すれば, (9.3) が得られる. ■

補題 9.7 [2, 定理 2, p3]　菊池の公式 (公式 9.5)(2) において, 次の等式が成り立つ.

$$r^3 = \frac{(a+b+c)^2(b-a+c)}{4c(a+b-c)}, \tag{9.17}$$

$$v^3 = \frac{(b+a-c)^2(b-a+c)}{4c(a+b+c)}, \tag{9.18}$$

$$w^6 = \frac{(a-b+c)^3(a+b+c)(a+b-c)}{2^4c^2(b-a+c)}. \tag{9.19}$$

補題 9.6, 補題 9.7 を適用すると, 例えば, 3 辺の長さが 5, 12, 13 であるヘロン三角形は, 菊池の公式 (公式 9.5) では直接的に記述できない. すなわち，菊池の公式を満たす r, v, w は整数の範囲では存在しないことがわかる.

日本では, 菊池の公式が得られていたが, それ以降に Carmichael が菊池とは独立に, この問題を解決している. この結果を補題として次に挙げる.

補題 9.8 [8]　すべてのヘロン三角形の 3 辺の長さは,

$$n(m^2+h^2), \quad m(n^2+h^2), \quad (m+n)(mn-h^2) \tag{9.20}$$

の形の数に比例する. ここで, m, n, h は正の整数で, $mn > h^2$ である.

9.4　和算の教育への応用

本章の前節までに述べた内容は, 文献 [2] として, すでに公刊されている. この文献は, 現在著者が勤務している倉敷市立郷内中学校の図書館に配架されており, 生徒が自由に閲覧できる. 生徒にとっては, 著者が自分の所属している学校の教師であるため, 質問もしやすい環境である. この章の内容に限らず, 自己の研究により明らかになった結果を, 小学生から大学生や一般までに解説し, その魅力を伝えていくことが今後の課題となる.

また, 和算の魅力について, かつて高等学校で数学教師を務め, この分野に関する文献を多数出している深川 ([11]) は, 和算書の解読に従事した経験をもとに,「江戸時代の日本の数学である和算の内容が高校生にとってすばらしい数学教材であることを確認した.」と述べている. 和算の内容は, このように教育への応用が豊富にある教材となる. 江戸時代に, 神社や仏閣にある算額などに代表される和算は, 研究者だけでなく庶民にも親しまれ

ていた. 当時と同様に, 和算の話題はこれからを生きる児童・生徒が馴染み, 主体的に学ぶことができるための格好の教材となるだろう.

本研究で取り上げた, 菊池の公式 (公式 9.5) については, パソコンに 3 変数を入力して, ヘロン三角形の 3 辺の長さを計算する活動が考えられる. この活動は ICT 教育の一環としても取り組めるだろう. また, ヘロン三角形を書かせて高さを測る活動や, 3 辺の長さ, 面積, 3 垂線の長さがすべて整数である三角形を見つける活動も考えられる. 他には, 中学校の課題学習において, ヘロン三角形の具体的な例を見出す活動が考えられるが, 何も条件を与えなければ生徒にとって難しいと思われる. 従って具体的な支援として, 定義 7.1 で定義したピタゴラス三角形を 2 つ組み合わせることによってヘロン三角形を構成するように教師が働きかけることにより, 生徒の実態に応じた授業設計が可能である. このヘロン三角形の構成法については [29] で述べられている. この授業実践は今後の課題とする.

前節までで述べた菊池の公式を含めたヘロン三角形は, 課題学習において教材化の可能性を多分に含んでいる. ヘロン三角形の高さを求める活動では, 三平方の定理を適用する能力の育成が期待できる. 菊池の公式を含めた和算については, 自分に必要な文献をインターネット等の情報手段を活用して検索する能力の育成, また, 菊池の公式を適用してヘロン三角形の 3 辺の長さをパソコンで求める活動では, 情報機器を活用して必要とする数量を求める能力の育成が図られる. さらに, そこで求めた 3 辺を長さにもつヘロン三角形について, その高さを求めることにより, この三角形についての理解を深めることができる.

第10章　格子ヘロン三角形とその教材化に向けて

本章の第2節では, 第6章から第8章における既知の事実を適用して, 著者ら ([4]) によって明らかにされた結果を述べ, 格子ヘロン三角形の頂点になる例を2つ与える.

第3節では, 著者らによって得られた結果の教材化に向けた例を示す. まず, 中学校において課題学習で扱うことを想定した, 有理三角形の頂点となる有理点の作図について, 次に, 高等学校において扱うことを想定した, 有理三角形の頂点を通る円の存在の別証明について述べる.

10.1　ピタゴラス数とその性質

定義 10.1　等式 $a^2+b^2=c^2$ を満たす正整数 a,b,c の組を**ピタゴラス数** (Pythagorean triple) という. 特に, a,b,c の最大公約数が1のとき, **原始ピタゴラス数** (primitive Pythagorean triple) という.

定義 7.1 より, 3辺の長さがピタゴラス数となる三角形は, ピタゴラス三角形であり, 直角三角形になる. 逆に, ピタゴラス三角形の3辺の長さは, ピタゴラス数になっている. 次の補題は初等整数論において有名である.

補題 10.2 [13]　a,b,c は方程式 $a^2+b^2=c^2$ の互いに素な整数解とする. このとき a か b は偶数となるので, a を偶数とすると, a,b,c は

$$a=2uv, b=u^2-v^2, c=u^2+v^2, \tag{10.1}$$

の形で表される. ここで, u と v は $u+v$ が奇数であり, $u>v$ を満たす互いに素な正の整数である. すべての u,v の組はそれぞれ, 原始ピタゴラス数 a,b,c に対応している.

10.2　格子ヘロン三角形

格子点に関する結果で, 著者らによって得られた定理を述べる. この定理は, 命題 10.4 を適用して証明されるため, 証明は後で述べる.

定理 10.3 [4, Theorem 3.1]　相互の距離がすべて整数となるような, n 個の格子点を含む円が存在する.

補題 7.5 と定理 8.2 を用いて, 次の命題 10.4 を得る. この命題も, 著者らが導いた結果である.

命題 10.4 [4, Proposition 3.1]　相互の距離がすべて有理数となるような, 無限個の有理点を含む円が存在する.

証明　a, b, c をピタゴラス数とする. 3 辺の長さが $P_0P_1 = P_0P_s = c$, $P_1P_s = 2a$ である二等辺三角形 $\triangle P_0P_1P_s$ の外接円を Γ とする. このとき外接円 Γ の方程式は $x^2+y^2 = (c^2/2b)^2$ である. 長さ c がである弦 P_0P_1 を見込む角を α とし, また, 辺 OP_0 と辺 P_1P_s との交点を H とする. $\angle OP_0P_1 = 90^\circ - \alpha/2$ だから, $\angle P_0P_1H = \alpha/2$ である. $\angle P_0P_1H$ は, ピタゴラス三角形 $\triangle P_0P_1H$ の 1 つの鋭角だから, 補題 7.2 より, $\alpha/2\pi$ は無理数である.

いま, 点 P_0 を外接円 Γ と y 軸との交点となるようにすると, $P_0(0, c^2/2b)$ となり, 点 $P_i(i = 1, 2, \cdots)$ を, 中心角 α で時計回りに次々刻んでいく. $\alpha/2\pi$ は無理数だから, 点 $P_i(i = 1, 2, \cdots)$ はすべて異なる. すなわち, 外接円 Γ は無限個の点 $P_i(i = 1, 2, \cdots)$ を含む.

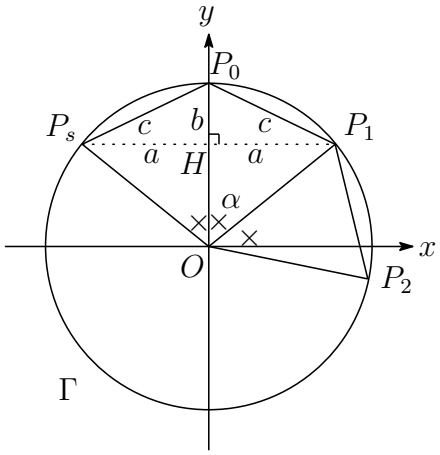
ここで, 点 $P_i(x_i, y_i), P_{i+1}(x_{i+1}, y_{i+1})$ に対して, 原点を中心に時計周りの方向への回転移動を考えると,

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} (2a^2 - c^2)/c^2 & 2ab/c^2 \\ -2ab/c^2 & (2a^2 - c^2)/c^2 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix}, \tag{10.2}$$

を得る. a, b, c は正整数だから, $(2a^2 - c^2)/c^2, 2ab/c^2$ は有理数である. だから, P_i が有理点ならば, P_{i+1} も有理点となる. このようにして, 点 $P_i(i = 0, 1, \cdots)$ はすべて有理点となる.

次に, 点 $P_i(i = 0, 1, \cdots)$ に対して, 辺 $P_jP_k(0 \le j < k \le n)$ の長さが有理数となることを示す. いま, 与えられた点 $P_i(i = 0, 1, \cdots, n)$ に対して, 円に内接する四角形 $P_0P_jP_kP_n(0 < j < k \le n)$ を考える. いま, $P_iP_j(0 \le i < j \le n-1)$ が有理数とすれば, トレミーの定理 (補題 8.1) を帰納的に適用すると, 辺 P_0P_n の長さは有理数である. 2 辺の長

さ $P_0P_1 = c$ と $P_0P_2 = 2a$ はすべて有理数だから, この議論を帰納的に適用することにより, 結論を得る. ■



例 10.5 [4, Example 3.1] 円 $C : x^2 + y^2 = (25/6)^2$ は, 相互の距離がすべて有理数となる無限個の点を含む.

$a = 4, b = 3, c = 5$ をピタゴラス数とする. 点 $P_i(x_i, y_i), P_{i+1}(x_{i+1}, y_{i+1})$ に対して, 定理 10.4 の証明における回転行列 (10.2) は,

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 7/25 & 24/25 \\ -24/25 & 7/25 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix}, \tag{10.3}$$

となる. この行列により得られる $P_i (i = 0, 1, \cdots)$ はすべて有理点である. いま $P_0(0, 25/6)$, $P_1(4, 7/6)$, $P_2(56/25, -527/150)$ であり, $P_0P_1 = P_1P_2 = 5$, $P_0P_2 = 8$ である.

この回転行列から, ヘロン三角形となる格子点の例を挙げる. この円を原点を中心として 150 倍に拡大した円 $C' : x^2 + y^2 = 625^2$ を考える. このとき, $P_0'(0, 625)$, $P_1'(600, 175)$, $P_2'(336, -527)$ に対して, $P_0'P_1' = 750, P_1'P_2' = 750, P_0'P_2' = 1200$, $\triangle P_0'P_1'P_2' = 270000$ であり, これらの点を頂点にもつ三角形はヘロン三角形である. 回転行列 (10.3) から得られる, 有理点 $P_i, P_j, P_k (0 \le i \le j \le k)$ に対して, それらの x, y 座標の分母の最小公倍数 ℓ をかけて得られる点 (これらの点は, 原点を中心として ℓ 倍に拡大された円上に存在する) P_i', P_j', P_k' はヘロン三角形を構成する. この議論を一般化したのが, この節の冒頭で述べた, 定理 10.3 である.

ここで, 著者らによって得られた, 定理 10.3 の証明をする.

証明　命題 10.4 の回転行列 (10.2) により, 有理点 $P_i(x_i, y_i)(i = 0, 1, \cdots, n-1)$ と有理距離 $P_jP_k(0 \leq j \leq k \leq n-1)$ を得る. すべての $x_i, y_i(i = 0, 1, \cdots, n-1)$ の分母, および $P_jP_k(0 \leq j \leq k \leq n-1)$ に対して, これらの最小公倍数を ℓ とする. 命題 10.4 で考えた円 $\Gamma : x^2 + y^2 = (c^2/2b)^2$ を原点を中心にして ℓ 倍に拡大した円 $\Gamma' : x^2 + y^2 = (\ell \cdot c^2/2b)^2$ を考える. 点 $P_i'(\ell x_i, \ell y_i)$ とすると, 各点 $P_i'(i = 0, 1, \cdots, n-1)$ はすべて円 Γ' の周上に存在し, $P_j'P_k' = \ell \cdot P_jP_k$ である. ここで, $\ell x_i, \ell y_i(i = 0, 1, \cdots, n-1)$ および $\ell \cdot P_jP_k(0 \leq j \leq k \leq n-1)$ はすべて整数となる. ■

ピタゴラス三角形は直角三角形である. 補題 10.2 より, ピタゴラス三角形において, 斜辺以外の 2 辺のうち一方は偶数であるから, その面積は整数となる. 3 辺の長さがすべて整数である格子三角形は, 外接する格子四角形から, ピタゴラス三角形と格子長方形を取り除いたものになる. これより, 次の補題を得る.

補題 10.6 [4, Lemma 3.1]　相互の距離がすべて整数となる格子点が 3 点与えられたとき, その 3 点を頂点にもつ三角形の面積は整数となる, すなわち, 3 点は格子ヘロン三角形の頂点となる.

定理 10.3 と補題 10.6 により, 次の定理を得る.

定理 10.7 [4, Theorem 3.2]　ヘロン三角形の頂点となるような, 3 個の格子点を含む円が存在する.

この定理の条件を満たす円は, 命題 10.4 における円周上の有理点から 3 個を選び, 適当な整数倍に拡大したものである. この整数を ℓ とすると, ℓ^2 倍された面積が整数となる. 従って, 命題 10.4 における円周上から 3 点を選んでできる三角形の面積は有理数となる. ゆえに, 次の補題を得る.

補題 10.8　命題 10.4 における無限個の有理点から, 任意に 3 点を選んでできる三角形の面積は有理数である. すなわち有理三角形となる.

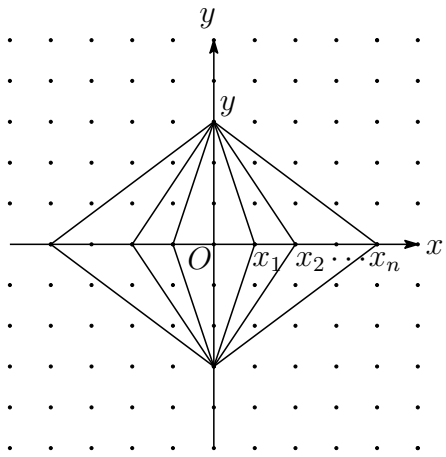
次に, ピタゴラス数に関する古典的な結果 (補題 10.2) を適用することにより, 次の定理を得る. この定理も著者らによる結果である.

定理 10.9 [4, Theorem 3.3]　$2n+3$ 個の格子点からなる集合

$$\{(0,\pm y),(0,0),(\pm x_1,0),\cdots,(\pm x_n,0)\} \tag{10.4}$$

の異なる 3 点が同一直線上になければ, それらの 3 点を結んだ三角形はヘロン三角形である. ここで, $p_i(i=1,\cdots,n)$ を奇素数として, $p_i > p_j(i<j)$ に対して $p_1 > 2p_2\cdots p_n$ となるように十分大きく p_1 を選んだとき, $x_k=(p_1\cdots p_k)^2-4(p_{k+1}\cdots p_n)^2$ $(k=1,\cdots,n)$, $y=4p_1\cdots p_n$ である.

証明　$u:=p_1\cdots p_k$, $v:=2(p_{k+1}\cdots p_n)$ とおく. u は奇数, v は偶数だから, $u+v$ は奇数である. また, $x_1<\cdots<x_k<\cdots<x_n$ である. ここで, 補題 10.2 を適用すると, 結論が得られる. ■



10.3　格子ヘロン三角形の教材化

n を具体的に与えて, 定理 10.3 を満たす円を見つけさせる活動が, 教材化の例として考えられる. 以下では格子ヘロン三角形を求める活動の例を示す.

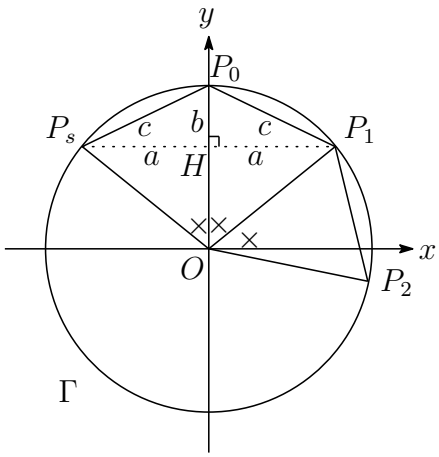
10.3.1　有理三角形の頂点となる有理点の作図

著者らにより得られた, 命題 10.4 および補題 10.8 によって, 有理三角形の頂点となる有理点を作図により与えることができる. この結果を認めれば, 中学校や高等学校の課題学習で扱うことが可能である. この作図の方法を次の補題として示す.

補題 10.10　有理三角形の頂点となる有理点は作図可能である.

方法　$a, b, c \in \mathbb{Z}$ をピタゴラス数とする. 3 辺の長さが $P_0P_1 = P_0P_s = c$, $P_1P_s = 2a$ である二等辺三角形 $\triangle P_0P_1P_s$ の外接円を Γ とすれば, 以下の手順によりこの外接円が作図できる. 長さ 1 の線分が与えられれば, 底辺を a, 高さが b である三角形 $\triangle P_0P_1H$ の 3 つの頂点を決定できる. ここで, $\angle P_0HP_1 = 90^\circ$ である. 線分 P_0P_1 が与えられたので, 線分 P_0H を共通にもつ $\triangle P_0P_sH$ を図のように同様に決定して, 線分 P_0P_s が得られる. これらの 2 本の線分の垂直二等分線の交点が外接円 Γ の中心となる.

次に, 線分 P_0P_1 を弦として, この長さで等間隔に円周上に点をとれば, 有理三角形の頂点となる有理点が得られる. これらの有理点のうち 3 個を任意に選べばよい. ■



実際にこの作図に取り組ませる課題を授業で取りあげることが可能である. この課題により, 垂線や垂直二等分線の作図や, 与えられた三角形の外接円を作図する技能を高めることができる.

10.3.2　有理三角形の頂点を通る円の存在の別証明

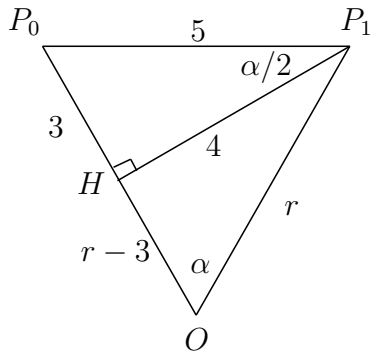
著者らによる結果である命題 10.4 の別証明を与える. ここでは, 具体的にピタゴラス数 $3, 4, 5$ で考えるが, 一般の a, b, c で考えることもできる. この過程は, 高等学校の数学 II の円の方程式の学習として扱うことが可能である. 命題 10.4 の系として次を与える. この系は, 命題 10.4 の具体的な数値を用いた別証明である.

系 10.11　3 辺の長さが $5, 5, 8$ である二等辺三角形の外接円で, 任意の有理点からの距離が 5 となる点を次々刻んだとき, それらの点はすべて有理点となり相異なる (無限個の点となる). また, それらの任意の 2 点の距離は有理数である.

証明　3 辺の長さが $5, 5, 8$ である二等辺三角形で, 2 つの等しい長さの辺の交点を P_0 として, y 軸上にとる. この外接円を Γ とする. この円の半径を r とすると, $\triangle OP_1H$ でピタゴラスの定理を適用して,

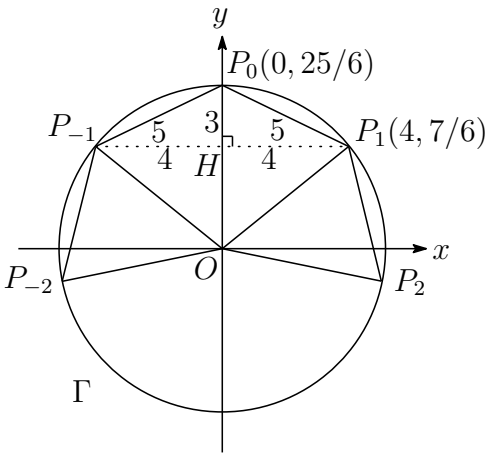
$$4^2 + (r-3)^2 = r^2 \tag{10.5}$$

より, $r = 25/6$ を得る.



長さ 5 の弦を見込む角を α とする. $\alpha/2$ はピタゴラス三角形の 1 つの鋭角だから補題 7.2 より, $\frac{\alpha}{2}/\pi$ は無理数である. 従って α/π は無理数である.

Γ の周上に距離が 5 である点を P_0 から次々と刻んでいく. それらの点を時計回りに $P_1, P_2, \cdots$ とし, 反時計回りに $P_{-1}, P_{-2}, \cdots$ とする. このとき, 無限個の点が得られる. トレミーの定理 (補題 8.1) を適用すれば, これらの任意の 2 点間の距離はどれも有理数であることがわかる.



次に点 $P_i(i=0,1,\cdots)$ が有理点となることを示す. まず, $P_0(0,25/6)$ でありこれは有理点である.

点 P_1 が有理点であることを示す. 円 Γ の方程式と, P_0 を中心とし, 半径が 5 である円の方程式を連立させて,

$$\begin{cases} x^2+y^2=(\frac{25}{6})^2 \\ x^2+(y-\frac{25}{6})^2=5^2 \end{cases} \tag{10.6}$$

より, 直線 $P_{-1}P_1$ の方程式 $6y=7$ を得る. 円 Γ と直線 $P_{-1}P_1$ の方程式より $P_1(4,7/6)$ となりこれは有理点である. $P_{-1}(-4,7/6)$ であることも分かる.

点 P_2 が有理点であることを示す. 円 Γ の方程式と, P_1 を中心とし, 半径が 5 である円の方程式を連立させて,

$$\begin{cases} x^2+y^2=(\frac{25}{6})^2 \\ (x-4)^2+(y-\frac{7}{6})^2=5^2 \end{cases} \tag{10.7}$$

より, 直線 P_0P_2 の方程式

$$144x+42y=175 \tag{10.8}$$

を得る. また, 円 Γ の方程式と, P_0 を中心とし, 半径が 8 である円の方程式を連立させて,

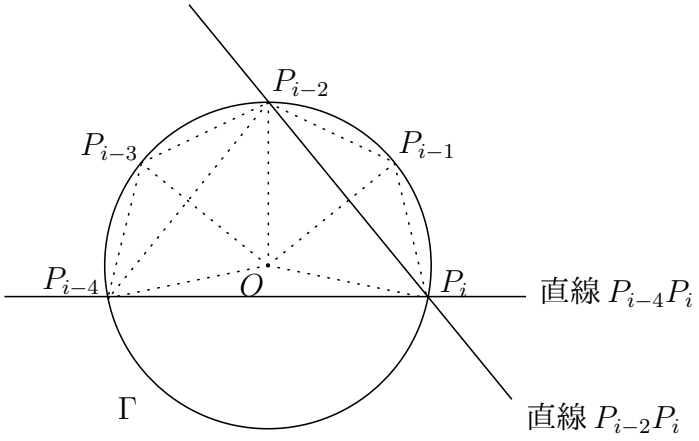
$$\begin{cases} x^2+y^2=(\frac{25}{6})^2 \\ x^2+(y-\frac{25}{6})^2=8^2 \end{cases} \tag{10.9}$$

より, 直線 $P_{-2}P_2$ の方程式

$$150y=-527 \tag{10.10}$$

を得る. 2 直線 P_0P_2, $P_{-2}P_2$ の交点が P_2 だから, (10.8) (10.10) より $P_2(56/25,-527/150)$ となりこれは有理点である.

同様にして, 点 P_i $(i=3,4,\cdots)$ が有理点であることを以下のように示すことができる.



円 Γ の方程式と, 点 P_{i-1} を中心, 半径が 5 である円の方程式より, 直線 $P_{i-2}P_i$ の方程式が得られる. 次に, 円 Γ の方程式と, 点 P_{i-2} を中心, 半径が 8 である円の方程式より, 直線 $P_{i-4}P_i$ の方程式が得られる. これらはすべて有理数係数となるから, 交点 P_i は有理点である. ■

この系 10.11 の証明を授業で取り扱うことにより, 次のことが期待できる.

- 中心の座標と半径が与えられたとき, その円の方程式を導く能力を高める.
- 交点を 2 個もつ 2 つの円の方程式を連立させることにより, 2 個の交点を通る直線の方程式が得られることを理解する.

まとめと今後の課題

まず, 本論文のまとめを行う. 第 I 部では, 格子の基底を中心に論じた. A.K.Lenstra, et al.([15]) による LLL 格子基底簡約の理論は, 筆者らの研究により, 内積としてエルミート積, ノルムとして通常のものを適用すれば虚二次体へ一般化できることが明らかになった. また, これ以外の有限次代数体では 0 が集積点となるため, 基底簡約理論が適用できないことが分かった. 虚二次体に一般化する際に, 常に簡約基底が存在するように, この基底の定義を修正することにより, 簡約基底の存在性が保証される. ここで論じた格子基底簡約問題は, 換言すれば, 格子簡約しきつめ問題ともいえる. 図形のしきつめについては, 小学校の算数でも取りあげられるテーマでもある. 教育への応用については, 格子基底簡約は, 格子簡約しきつめと同値であることも明らかとなった. これにより, 格子基底簡約理論は, 計算機代数の理論のみに留まることなく, 数学教育への応用も期待される.

第 II 部では, 格子多角形の性質を中心に論じた. 離散数学, 組合せ数学の内容は, 初等幾何の延長線上にあるため, 馴染みやすく数学教育へ応用できる. ピックの定理, 格子正多角形, 円周上の有理点の個数を挙げて, その教材化に向けて考察した. また, 和算家である菊池長良の公式で直接的に表現できないヘロン三角形について述べ, 教材として発展させることができる事例を提示した. 離散数学や組合せ数学の既知の事実を用いて, 定理 10.4 において, 円周上の無限個の有理点で, 相互の距離がすべて有理数となるような円が存在することを明らかにし, この証明のなかで具体的な構成法を述べた. また, ピタゴラス数に関する古典的な結果を適用することにより, 定理 10.9 において, 格子ヘロン三角形となる頂点の例を挙げた. 著者らによって得られた結果などを含む数学理論を教育へ応用することにより, 「主体的・対話的で深い学び」を実現するための教材化を試みることができた.

このように本論文では, 著者らの研究成果を含めた数学理論の成果を提示し, それを数学教育へ応用する観点で論を展開した. 最後に, 数学理論を教材化する際に, どのように教材として再構成するのか, また, どのような基準で行うのかについて述べる. まず, 教師が体系化されている数学理論を学び, そのうえで定義, 命題, 定理などからなる各要素間の

関連を明確にすることにより, 数学理論としての視点から体系化されている当該概念の全体像を把握する. また, 教材化を行う学校種に対応する児童生徒の発達段階や, 実際に授業実践を計画している集団や児童生徒一人一人の実態を把握して, 指導する概念についての素材を取捨選択し再構成する. このとき, 児童生徒の理解を支援することを目的として, 各学習要素間のギャップを補足し, 実生活との関連を明確にすることも必要である. これらの観点で検討を重ねたうえで授業設計を行い, 指導計画を立案することが大切であると考える.

次に, 今後の課題について述べる. 数学の面では, ガウスの数体 $\mathbb{Q}(\sqrt{-1})$ 上の格子において, その簡約基底の存在性や性質について明らかになったが, それ以外の虚二次体では, 満たすべき簡約基底の性質などをはじめとして, 格子基底簡約の一般論としては未だ完成されていない. $\mathbb{Q}(\sqrt{m}), m < 0$ で m の絶対値が大きい場合, 簡約基底の存在を保障するためには, 基底の満たす条件をさらに弱めざるを得ない. また, この整数環の性質をさらに詳しく調べる必要がある. これらのことにより, 虚二次体上の格子基底簡約理論を構築していきたい.

また, 格子ヘロン三角形における研究に関連して, 今回は有理点の性質を円で考察したが, 他にも有理点の性質がよく研究されている楕円曲線上で考えることもできるだろう. このことにより, あらたな知見が得られることが期待できる. 楕円曲線上の有理点の研究は整数論, 代数幾何学との関連が強く, 初等的な研究だけではなく, 抽象代数学の視点からの研究にもつなげていきたい.

数学教育の面では, 著者らによる数学の研究で得られた結果を含めて, 数学で知られている結果を, 算数・数学の授業で取りあげていくための教材化を進めることが今後の課題である. このことは, 今後数学教育においても展開が望まれる「主体的・対話的で深い学び」の充実に寄与できると考える.

また, 第 II 部で論じた, 離散数学, 組合せ数学の話題は, 多くの内容が教育で取り上げることのできる可能性があることが分かった. ピックの定理や, 格子正多角形, 円周上の有理点の個数, トレミーの定理, 格子ヘロン三角形など, 和算の話題も含めて, 魅力的な題材が豊富にある. これらの題材を具体的に教材化し, 算数・数学の授業で実践していきたい.

数学の教師自身が, 教科内容の研究に取り組むことは, 数学の正しい知識をもち, 数学の見方や考え方を体感, 理解することにつながる. このことにより, 教師自身が数学の本質

である公理に基づく手法を理解することになる. 従って, 教師自身が教科内容の研究に取り組むことは, 「主体的・対話的で深い学び」を進めていくうえで必要不可欠である. また, 教師が, 児童生徒の興味・関心や理解度に応じて関連する内容を授業において取り上げるためには, 学校種に依存せず数学の内容を俯瞰し, 系統的に再構築する力が求められる. この意味でも, 本論文の内容は教師教育として, 数学の教員研修等において取りあげることが考えられる. 教師に対しても, 興味を引く題材を提示し, 数学の研究をすることの魅力や, 数学の内容を正しく学ぶことの大切さを伝えていきたい.

純粋数学の研究内容がそこに留まることなく, 教科内容学の中核をなす要素の 1 つとして発展し, ひいては, 学校教育の充実へとつながることが期待できる. 今後, 数学研究と併行して, これらのことに従事していきたい.

謝辞

博士課程在学中, 御指導, 御助言をいただきました, 主指導教員である松岡隆教授 (鳴門教育大学), 2 年次まで主指導教員であった平野康之教授 (広島工業大学, 前 鳴門教育大学) をはじめ, 副指導教員である中川仁教授 (上越教育大学), 秋田美代教授 (鳴門教育大学), また, 公聴会にて御助言をいただきました, 論文審査委員である本田亮教授 (鳴門教育大学), 胸組虎胤教授 (鳴門教育大学), 村田守特任教授 (鳴門教育大学) に心よりお礼を申し上げます. また, ヘロン三角形について御助言をいただきました, 故・田中昭太郎教授 (元 鳴門教育大学), 博士課程入学前から, 研究全般について御助言や励ましをいただきました, 丸林英俊名誉教授 (鳴門教育大学) に心よりお礼を申し上げます.

最後になりますが, 著者の勤務校である倉敷市立郷内中学校の教職員の皆様, 支えてくれた妻子や亡き両親に心より感謝の意を表し, 謝辞と致します.

参考文献

[1] 秋田美代, 教科内容学を基にした教員教育の改善 -教科専門と教科教育の役割について-, 日本教科内容学会誌, 第 1 巻 第 1 号, 2015, 29-39.

[2] 有元康一・平野康之, ヘロン三角形の三辺の長さを与える公式について- 和算家・菊池長良の公式で直接的に表現できないヘロン三角形-, 数学史研究, 日本数学史学会, **230**, 2018, 1-8.

[3] K.Arimoto and Y.Hirano, *A generalization of LLL lattice basis reduction over imaginary quadratic fields*, Scientiae Mathematicae Japonicae, **82**(1), 2019, 1-6.

[4] K.Arimoto and Y.Hirano, *On lattice points which become vertices of Heronian triangles*, Far East Journal of Mathematical Sciences, **107**(2), 2018, 511-518.

[5] K.Arimoto, *On the existence of LLL reduced bases over imaginary quadratic fields*, Scientiae Mathematicae Japonicae, (submitted).

[6] K.Arimoto, *On the termination of quasi LLL Lattice basis reduction algorithm over gaussian number fields*, Far East Journal of Mathematical Sciences, **109**(1), 2018, 175-184.

[7] M.R.Bremner, *Lattice Basis Reduction:An Introduction to the LLL Algorithm and Its Applications*, CRC Press, 2011.

[8] R.D.Carmichael, *The Theory of Numbers and Diophantine Analysis*, Dover, 1959, 11-13.

[9] J.W.S.Cassels, *An Introduction to the Geometry of Numbers*, Springer Verlag, 1971.

[10] P.Frankl・前原濶, 幾何学の散歩道 -離散・組合せ幾何入門-, 共立出版, 1991.

[11] 深川英俊・トニー・ロスマン, 聖なる数学:算額, 森北出版, 2010.

[12] 菊池長良, 算法整数起源抄, 1845.

[13] H.Koch, *Number Theory: Algebraic Numbers and Functions*, Graduate Studies in Mathematics, 24, American Mathematical Society, 2000.

[14] 桑田孝泰・前原濶, 整数と平面格子の数学, 共立出版, 2015.

[15] A.K.Lenstra, H.W.Lenstra,Jr., and L.Lovász, *Factoring polynomials with rational coefficients*, Math. Ann., **261**, 1982, 515-534.

[16] 枡田幹也・福川由貴子, 格子からみえる数学, 日本評論社, 2013.

[17] 松崎和孝, トポロジーの学習内容とその教材群の研究 -小学校から大学までの学習内容の系統性を意識して-, 兵庫教育大学大学院 連合学校教育学研究科 博士論文, 2017.

[18] 文部科学省, 小学校学習指導要領 (平成 29 年告示), 2017.

[19] 文部科学省, 中学校学習指導要領 (平成 29 年告示), 2017.

[20] 文部科学省, 高等学校学習指導要領 (平成 30 年告示), 2018.

[21] 永嶋裕樹・白柳潔, 安定化手法に基づく計算履歴法と LLL アルゴリズムへの適用, 数式処理とその周辺分野の研究, 数理解析研究所講究録 **2054**, 2017, 1-13.

[22] H.Napias, *A generalization of the LLL-algorithm over euclidean rings or orders*, Journal de Theorie des Nombres de Bordeaux, tome 8, no 2, 1996, 387-396.

[23] M.Pohst and H.Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge University Press, 1989.

[24] W.Scherrer, *Die Einlangerung eines Regularen Vielecks in ein Gitter*, Elemente der Math., **1**, 1946, 97-98.

[25] W.H.Schikhof, *Ultrametric calculus*, Cambridge University Press, 1984.

[26] J.H.Silverman, はじめての数論 原書第 3 版 (鈴木治郎 訳), 丸善出版, 2014.

[27] 田中昭太郎, 整数三角形について, 学校数学研究, 学校数学研究会 鳴門教育大学, **4** (1), 1996, 27-39.

[28] 田中昭太郎, 整数三角形について・続, 学校数学研究, 学校数学研究会 鳴門教育大学, **4** (2), 1996, 31-37.

[29] 田中昭太郎, 整数三角形の新しい作り方, 学校数学研究, 学校数学研究会 鳴門教育大学, **9** (2), 2001, 121-127.