数理解析研究所講究録 第2108巻 2019年 115-123

虚二次体における LLL 格子基底簡約アルゴリズム

LLL Lattice Basis Reduction Algorithm over Imaginary Quadratic Fields

有元 康一[1]
Koichi Arimoto
兵庫教育大学大学院 連合学校教育学研究科（鳴門教育大学）
Joint Graduate School (Ph.D. Program) in Science of School Education,
Hyogo University of Teacher Education (Naruto University of Education)

平野 康之[2]
Yasuyuki Hirano
広島工業大学 情報学部
Faculty of Applied Information Science, Hiroshima Institute of Technology

1 はじめに

LLL 格子基底簡約アルゴリズム (LLL Lattice basis reduction algorithm) は，1982 年に, A.K.Lenstra, H.W.Lenstra, Jr., and L.Lovász ([6]) が開発したアルゴリズムである．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形の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.

A.K.Lenstra, et al. による LLL 格子基底簡約の研究は, 計算機代数の分野等で応用されており, 有理数係数多項式の因子分解を, その多項式の次数の多項式時間の計算量で行うために 1980 年代に導入されたものである. この研究をはじめとする一連の研究では, 格子を実数体 $\mathbb{R}$ 上のベクトル空間 $\mathbb{R}^n$ 内において, 整数環 $\mathbb{Z}$ 上の基底をもつ加群 ($\mathbb{Z}$-格子) で考えている. H.Napias ([7]) は, LLL reduction algorithm をユークリッド環やユークリッド整環上に一般化している.

本論では, 我々が取り組んできた成果 ([3], [4]) を紹介することが主な目的である. 我々は A.K.Lenstra, et al. による LLL 格子基底簡約を, 有限次代数体 F 上における整数環 $\mathcal{O}_F$ 上の加群 ($\mathcal{O}_F$-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が明らかになった. その他の代数体の場合, $\mathcal{O}_F$ 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 が集積点となるため, いくらでも 0 に近い元が存在する. 内容の一部は概要を [1] でも解説している. 本論の最後では, 有元・平野 ([3]) で定義した虚二次体上での簡約基底について, その存在性につ

[1]e-mail: 16201065@naruto-u.ac.jp
[2]e-mail: y.hirano.sv@it-hiroshima.ac.jp

いて調べた有元の成果について触れる.

2　$\mathbb{Z}$-格子での基底簡約

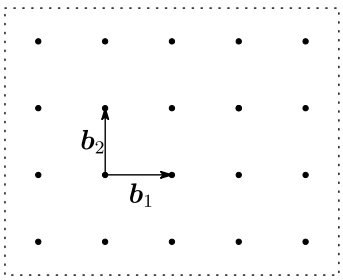
2.1　$\mathbb{Z}$-格子の定義

定義 2.1　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,

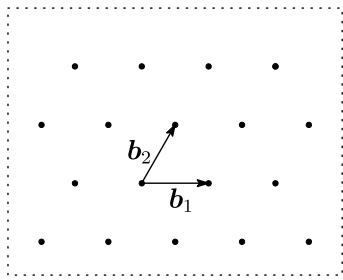
$$\Lambda = \mathbb{Z}\boldsymbol{b}_1 + \cdots + \mathbb{Z}\boldsymbol{b}_n = \left\{ \sum_{i=1}^{n} r_i \boldsymbol{b}_i \;\middle|\; r_i \in \mathbb{Z}\ (1 \leq i \leq n) \right\} \tag{1}$$

を満たすものが存在することをいう.

例 2.1　$n = 2$ のときの例を挙げる.　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になる :



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



【図 2】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く, 幾通りも存在することを注意しておく.

定義 2.2　Λ の基底 $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ に対して,

$$d(\Lambda) := \sqrt{|\det(\boldsymbol{b}_i, \boldsymbol{b}_j)_{1 \leq i,j \leq n}|} \tag{2}$$

を Λ の **判別式**(discriminant) という. ここで $(\ ,\ )$ は 2 つのベクトルの内積を表す. (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.

命題 2.1　Λ の基底 $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ に対して,

$$d(\Lambda) = |\det(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)| \tag{3}$$

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 2.2　$\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n \in \Lambda$ に対して,

$$|\det(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)| \leq \prod_{i=1}^{n} \|\boldsymbol{b}_i\| \tag{4}$$

が成立する (アダマールの不等式). ただし等号は 行列 $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ が正則のとき, $(\boldsymbol{b}_i, \boldsymbol{b}_j) = 0$ (for $i \neq j$) のときに成立する. 一般には, $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ は格子の元でなくても, ベクトル空間 $\mathbb{R}^n$ の元であればこの不等式は成立する.

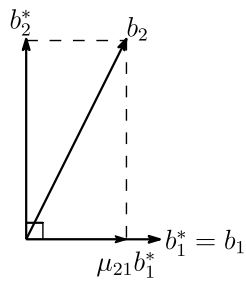
2.2 $\mathbb{Z}$-格子における簡約基底

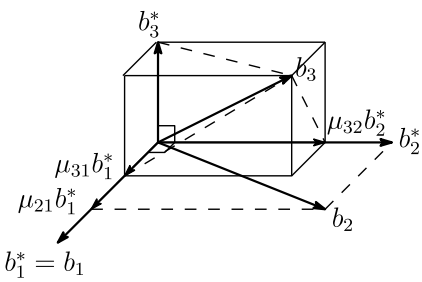
定義 2.3　$\Lambda = \mathbb{Z}\boldsymbol{b}_1 + \cdots + \mathbb{Z}\boldsymbol{b}_n$ とする. Λ の基底 $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ に対して,

$$\boldsymbol{b}_i^* := \boldsymbol{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \boldsymbol{b}_j^*, \quad \mu_{ij} := \frac{(\boldsymbol{b}_i, \boldsymbol{b}_j^*)}{(\boldsymbol{b}_j^*, \boldsymbol{b}_j^*)} \quad (1 \leq j < i \leq n) \tag{5}$$

とすると (Gram-Schmidt の直交化法), $\mu_{ij} \in \mathbb{R}$ である.

例 2.2　$n = 2, 3$ のとき次の図のように $\boldsymbol{b}_2^*, \boldsymbol{b}_3^*$ が順次決定される.





定義 2.4　$\Lambda = \mathbb{Z}\boldsymbol{b}_1 + \cdots + \mathbb{Z}\boldsymbol{b}_n$ 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 2.3 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 :

$$|\mu_{ij}| \leq \frac{1}{2} \quad (1 \leq j < i \leq n), \tag{6}$$

$$\|\boldsymbol{b}_i^* + \mu_{i,i-1} \boldsymbol{b}_{i-1}^*\|^2 \geq \frac{3}{4} \|\boldsymbol{b}_{i-1}^*\|^2. \tag{7}$$

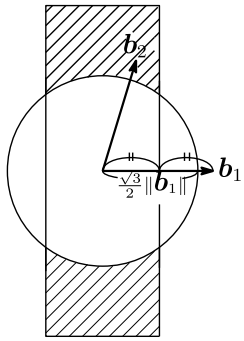
例 2.3　$n = 2$ のとき定義 2.4 は次の不等式で表せる :
(6) 式については

$$|\mu_{21}| \leq \frac{1}{2}, \tag{8}$$

(7) 式については, 定義 2.3 (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. したがって

$$\|\boldsymbol{b}_2\|^2 \geq \frac{3}{4}\|\boldsymbol{b}_1\|^2, \quad \text{すなわち} \quad \|\boldsymbol{b}_2\| \geq \frac{\sqrt{3}}{2}\|\boldsymbol{b}_1\| \tag{9}$$

となる. (8), (9) 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.



【図 5】 $n = 2$ のときの $\boldsymbol{b}_2$ の存在できる範囲

図 5 において, 帯状領域は上下方向に無限に伸びている.

2.3 $\mathbb{Z}$-格子における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 [6] に記述されている. ここでは, このアルゴリズムの概要を [10] 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 (5) 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主に次の 3 つである:

(Step A) $\mu_{m,m-1}$ 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, $r \leftarrow \{\mu_{m,m-1}\}, \boldsymbol{b}_m \leftarrow \boldsymbol{b}_m - r\boldsymbol{b}_{m-1}$ 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 $x + \frac{1}{2}, x - \frac{1}{2}$ のどちらかとする. このとき $\mu_{m,m-1} \leftarrow \mu_{m,m-1} - r$ 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) $i = m$ に対して, (7) が成立するならば (Step C) 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, m を $m-1$ で置き換える. その後 (Step A) に行く.

(Step C) ((Step A) 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, m を 1 増加させる. $m > n$ ならばアルゴリ

ズムは終了し, そうでなければ (Step A) に行く.

アルゴリズムのなかで, $\boldsymbol{b}_i^*$ は成分を使って明示的に使用されないが, 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示す.

$$D_i := \det(\boldsymbol{b}_\mu, \boldsymbol{b}_\nu)_{1\leq\mu,\nu\leq i} \quad (1 \leq i \leq n) \tag{10}$$

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

$$D := \prod_{j=1}^{n-1} D_j \tag{11}$$

とする. (2), (5) によって,

$$D_i = \prod_{j=1}^{i} \|\boldsymbol{b}_j^*\|^2 \quad (1 \leq i \leq n) \tag{12}$$

を得る. (Step B) 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 $\frac{3}{4}$ に減少する. したがって, D の値も $\frac{3}{4}$ となる. しかし, D_i に対し, 正の下界 S_i で次を満たすものが存在する :

$$D_i \geq S_i > 0 \ \ (1 \leq i \leq n) \tag{13}$$

したがって, アルゴリズムは有限回のステップで終了する.

2.4 $\mathbb{Z}$-格子における簡約基底の性質

$\mathbb{Z}$-格子における簡約基底の性質として, 次の命題を与える. 証明については [6, Prop.(1.6),(1.11),(1.12)] で述べられている.

命題 2.3 $[6, \text{Prop.}(1.6), (1.11), (1.12)]$ $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ を Λ の簡約基底とする. また, $\boldsymbol{b}_i^*$ $(i = 1, 2, \cdots, n)$, μ_{ij} は定義 2.3 で定義した通りとする. このとき次が成立する :

(L1) $\|\boldsymbol{b}_j\|^2 \leq 2^{i-1}\|\boldsymbol{b}_i^*\|^2$ $(1 \leq j \leq i \leq n)$,

(L2) $d(\Lambda) \leq \prod_{i=1}^{n} \|\boldsymbol{b}_i\| \leq 2^{\frac{n(n-1)}{4}} d(\Lambda)$,

(L3) $\|\boldsymbol{b}_1\| \leq 2^{\frac{n-1}{4}} d(\Lambda)^{\frac{1}{n}}$,

(L4) $\|\boldsymbol{b}_1\|^2 \leq 2^{n-1}\|\boldsymbol{x}\|^2$ for $^\forall \boldsymbol{x} \in \Lambda,\ \boldsymbol{x} \neq \boldsymbol{0}$,

(L5) $\|\boldsymbol{b}_j\|^2 \leq 2^{n-1}\max\{\|\boldsymbol{x}_1\|^2, \cdots, \|\boldsymbol{x}_t\|^2\}$ $(1 \leq j \leq t \leq n$ で, $\boldsymbol{x}_1, \cdots, \boldsymbol{x}_t$ は線型独立).

3 $\mathcal{O}_F$-格子での基底簡約

複素数 α が有理数を係数とする, ある多項式の根であるとき, α は**代数的数**であるという. 代数的数全体のつくる体 Ω の部分体を**代数体**という. 代数体 F は明らかに有理数体 $\mathbb{Q}$ をふくみ, したがって $\mathbb{Q}$ 上のベクトル空間とみなせるが, 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) という.

また, 複素数 ω 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**であるという. 代数的整数全体の集合を Γ とする. 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. $\mathcal{O}_F$ は F の部分環であり, $\mathcal{O}_F \cap \mathbb{Q} = \mathbb{Z}$ である. $\mathcal{O}_F$ の元を F の**整数**という.

この章の 3.1〜3.3 では有元・平野による研究の成果を紹介する. この内容は, 文献 [1],[3],[4] でも述べている. 3.4 では, その後の有元による研究成果を結果のみ示す. 詳細については他の機会に譲る. 以降 F を有限次代数体, $\mathcal{O}_F$ を F の整数環とする.

3.1 $\mathcal{O}_F$-格子の定義

定義 3.1 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,

$$\Lambda = \mathcal{O}_F\boldsymbol{b}_1 + \cdots + \mathcal{O}_F\boldsymbol{b}_n = \left\{ \sum_{i=1}^{n} r_i\boldsymbol{b}_i \;\middle|\; r_i \in \mathcal{O}_F \ (1 \le i \le n) \right\} \tag{14}$$

を満たすものが存在することをいう.

格子の判別式などについても同様に定義する. F の元は実数の範囲を超えていることを確認しておく. 例えば今から考える虚二次体 $F = \mathbb{Q}(\sqrt{m}),\ m < 0$ には, 虚数の元が存在する.

3.2 虚二次体の具体的表示

以降, F を 2 次の代数体 (**二次体**) とする. このとき, $\dim_{\mathbb{Q}} F = 2$ である. 二次体は, 次のように表される. ただし m は平方因子をもたない整数である.

$$\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\} \tag{15}$$

$m > 0$ のとき, **実二次体**, $m < 0$ のとき, **虚二次体** という. 二次体の整数は

(i) $m \equiv 2, 3 \pmod 4$ のとき,

$$\mathcal{O}_F = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\} \tag{16}$$

(ii) $m \equiv 1 \pmod 4$ のとき,

$$\mathcal{O}_F = \left\{ a + b \cdot \frac{1+\sqrt{m}}{2} \;\middle|\; a, b \in \mathbb{Z} \right\} \tag{17}$$

である.

3.3 $\mathcal{O}_F$-格子における簡約基底とその性質

代数体 (とくに二次体) への一般化を考えるとき, $F \not\subset \mathbb{R}$ であるから, 複素ベクトル空間で考えなければならない. ここで, ベクトル空間 F^n における 2 つのベクトルの内積およびノルムを定義する.

$\mathcal{O}_F$ が最小元をもつための必要十分条件は, F が有理数体または虚二次体であることである ([3, Theorem4.4], [4, Theorem3.6]). そのため, 以後 F を虚二次体とする.

定義 3.2 F^n における 2 つのベクトル $\boldsymbol{a} = (a_1, \cdots, a_n)^t, \boldsymbol{b} = (b_1, \cdots, b_n)^t$ の内積を

$$(\boldsymbol{a}, \boldsymbol{b}) = a_1\overline{b}_1 + \cdots + a_n\overline{b}_n \tag{18}$$

(エルミート内積) で定義する. ここで, $\overline{b}$ は b の共役な複素数である. また F^n におけるノルムを, $\boldsymbol{x} \in F^n$ にたいして,

$$\|\boldsymbol{x}\| := \sqrt{(\boldsymbol{x}, \boldsymbol{x})} = \sqrt{|x_1|^2 + |x_2|^2 + \cdots + |x_n|^2} \tag{19}$$

で定義する. ここで x_i はベクトル $\boldsymbol{x}$ の第 i 成分である.

定義 3.3 $\Lambda = \mathcal{O}_F\boldsymbol{b}_1 + \cdots + \mathcal{O}_F\boldsymbol{b}_n$ とする. Λ の基底 $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ に対して,

$$\boldsymbol{b}_i^* := \boldsymbol{b}_i - \sum_{j=1}^{i-1} \mu_{ij}\boldsymbol{b}_j^*, \quad \mu_{ij} := \frac{(\boldsymbol{b}_i, \boldsymbol{b}_j^*)}{(\boldsymbol{b}_j^*, \boldsymbol{b}_j^*)} \;\; (1 \le j < i \le n) \tag{20}$$

とすると, $\mu_{ij} \in \mathbb{C}$ である.

次に $\mathcal{O}_F$-格子における簡約基底を定義する. A.K.Lenstra, et al. による $\mathbb{Z}$-格子における簡約基底の定義 (定義 2.4) と同様にして次のように定義する:

定義 3.4 $\Lambda = \mathcal{O}_F\boldsymbol{b}_1 + \cdots + \mathcal{O}_F\boldsymbol{b}_n$ とする. Λ の基底 $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ が **LLL-簡約基底**であるとは, 定義 3.3 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 :

$$|\mu_{ij}| \le \frac{1}{2} \;\; (1 \le j < i \le n), \tag{21}$$

$$\|\boldsymbol{b}_i^* + \mu_{i,i-1}\boldsymbol{b}_{i-1}^*\|^2 \ge \frac{3}{4}\|\boldsymbol{b}_{i-1}^*\|^2. \tag{22}$$

$\mathcal{O}_F$ 格子における簡約基底においても, A.K.Lenstra, et al. による $\mathbb{Z}$-格子における簡約基底の性質 (命題 2.3) と同様の結果が得られる. それを証明なしで述べる.

命題 3.1 [3, Theorem3.3] F を虚二次体, $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ を Λ の簡約基底とする. また, $\boldsymbol{b}_i^*$ $(i = 1, 2, \cdots, n)$, μ_{ij} は定義 3.3 で定義した通りとする. このとき次が成立する :

(L1) $\|\boldsymbol{b}_j\|^2 \leq 2^{i-1}\|\boldsymbol{b}_i^*\|^2$ $(1 \leq j \leq i \leq n)$,

(L2) $d(\Lambda) \leq \prod_{i=1}^{n} \|\boldsymbol{b}_i\| \leq 2^{\frac{n(n-1)}{4}} d(\Lambda)$,

(L3) $\|\boldsymbol{b}_1\| \leq 2^{\frac{n-1}{4}} d(\Lambda)^{\frac{1}{n}}$,

(L4) $\|\boldsymbol{b}_1\|^2 \leq 2^{n-1}\|\boldsymbol{x}\|^2$ for $^\forall \boldsymbol{x} \in \Lambda,\ \boldsymbol{x} \neq \boldsymbol{0}$,

(L5) $\|\boldsymbol{b}_j\|^2 \leq 2^{n-1}\max\{\|\boldsymbol{x}_1\|^2, \cdots, \|\boldsymbol{x}_t\|^2\}$ $(1 \leq j \leq t \leq n$ で, $\boldsymbol{x}_1, \cdots, \boldsymbol{x}_t$ は線型独立).

3.4 $\mathcal{O}_F$-格子における簡約基底の存在性

有元・平野による定義 3.4 において, 簡約基底が常に存在するように定義を見直す. ここではその結果のみ述べ, 詳細については別の機会に譲ることにする.

ここで, F はガウスの数体, すなわち, $F = \mathbb{Q}(\sqrt{-1})$ とする. このとき, $\mathcal{O}_F = \mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$. である.

定義 3.5 $F = \mathbb{Q}(\sqrt{-1})$ 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 3.3 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 :

$$|\mu_{ij}| \leq \frac{\sqrt{2}}{2} \quad (1 \leq j < i \leq n), \tag{23}$$

$$\|\boldsymbol{b}_i^* + \mu_{i,i-1}\boldsymbol{b}_{i-1}^*\|^2 \geq \frac{3}{4}\|\boldsymbol{b}_{i-1}^*\|^2. \tag{24}$$

命題 3.2 $F = \mathbb{Q}(\sqrt{-1})$ とする. このとき定義 3.5 で定義された擬 LLL-簡約基底は常に存在する. そこで $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ 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 3.3 で定義した通りとする. このとき次が成立する :

(L1) $\|\boldsymbol{b}_j\|^2 \leq 4^{i-1}\|\boldsymbol{b}_i^*\|^2$ $(1 \leq j \leq i \leq n)$,

(L2) $d(\Lambda) \leq \prod_{i=1}^{n} \|\boldsymbol{b}_i\| \leq (2^n - 1)d(\Lambda)$,

(L3) $\|\boldsymbol{b}_1\| \leq \left(\frac{4^n - 1}{3}\right)^{\frac{1}{2n}} d(\Lambda)^{\frac{1}{n}}$,

(L4) $\|\boldsymbol{b}_1\|^2 \leq 4^{n-1}\|\boldsymbol{x}\|^2$ for $^\forall \boldsymbol{x} \in \Lambda,\ \boldsymbol{x} \neq \boldsymbol{0}$,

(L5) $\|\boldsymbol{b}_j\|^2 \leq 4^{n-1}\max\{\|\boldsymbol{x}_1\|^2, \cdots, \|\boldsymbol{x}_t\|^2\}$ $(1 \leq j \leq t \leq n$ で, $\boldsymbol{x}_1, \cdots, \boldsymbol{x}_t$ は線型独立).

謝辞

本研究に関して有益なご助言を頂きました, 松岡隆教授（鳴門教育大学）, 中川仁教授（上越教育大学）に感謝の意を表します.

参考文献

[1] 有元康一, 平野康之, *A generalization of LLL lattice basis reduction over imaginary quadratic fields*, 言語, 論理, 代数系と計算機科学の展開, 数理解析研究所講究録 **2051**, 9-13, 2017.

[2] 石田信：「代数的整数論」，森北出版，1974.

[3] K.Arimoto and Y.Hirano, *A Generalization of LLL Lattice Basis Reduction over Imaginary Quadratic Fields*, Sci. Math. Jpn.,(to appear).

[4] K.Arimoto and Y.Hirano, *On the non Existence of Least Positive Elements of Certain Lattices in the Field of Complex Numbers*, Sci. Math. Jpn.,(submitted).

[5] H.Cohen, *A Course in Computational Algebraic Number Theory*, GTM **138**, Springer Verlag, 1993.

[6] A.K.Lenstra, H.W.Lenstra,Jr., and L.Lovász, *Factoring Polynomials with Rational Coefficients*, Math. Ann., **261**, 515-534, 1982.

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

[8] K.Peter, *The LLL-Algorithm and some Applications*, 2009, available at `http://user.math.uzh.ch/dehaye/thesis_students/Karin`

[9] M.E.Pohst *Computational Algebraic Number Theory*, DMV Seminar **21**, Birkhäuser Verlag, 1993.

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

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

[12] W.M.Schmidt, *Diophantine Approximation*, LNM **785**, Springer Verlag, 1980.