簡約変数の導入による虚二次体における格子基底簡約

On Lattice Basis Reduction over Imaginary Quadratic Fields by Introducing Reduction Parameters

倉敷市立郷内中学校　　有元 康一[*1]
Koichi Arimoto
Kurashiki City Gonai Junior High School

Abstract

The author has generalized the LLL reduction algorithm so that it can be applied to obtain a LLL reduced basis over imaginary quadratic field by introducing a reduction parameter. The termination of the generalized algorithm is guaranteed by showing that a quantity which strictly decreases during the execution of the algorithm has a positive lower bound.

1　はじめに

LLL 格子基底簡約 (LLL Lattice basis reduction, 以後「基底簡約」と記す) は, 1982 年に, A.K.Lenstra, H.W.Lenstra, Jr., and L.Lovász が構築した理論である ([8]). 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.

Lenstra, et al. による基底簡約の研究は, 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 は, 基底簡約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 ([9]).

有元・平野は, Lenstra, et al. による基底簡約を, ある条件下において虚二次体における整数環上に一般化した ([4]). その後有元は, 虚二次体の一例であるガウスの数体における整数環上で, 常に簡約基底が存在するように定義を改良してアルゴリズムが終了することを示した ([2],[3]). すなわち基底簡約を, 有元・平野による当初の条件を改良したうえで, ガウスの数体における整数環上に一般化したことになる. この意味において, 虚二次体において一般化可能な環の範囲を拡大することが課題であった. ここで考えている環は, 単項イデアル整域とする.

そこで有元は, Lenstra, et al. による簡約変数 (reduction parameter) を導入することにより, 基底簡約を虚二次体における整数環上に一般化した. 本稿では, 研究成果の概略を述べる.

[*1] 〒 710-0142 倉敷市林 620 番地　E-mail: te27212@kurashiki-oky.ed.jp

2 準備

2.1 代数体とその整数環

代数体とその整数環について, 代数的整数論から基礎理論を述べる ([1]).

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.

この章では次節以降で, 有元が A.K.Lenstra, et al. による基底簡約をガウスの数体における整数環上に一般化した具体的内容を提示する ([2], [3]). 以降 F を有限次代数体, $\mathcal{O}_F$ を F の整数環とする.

2.2 $\mathcal{O}_F$-格子の定義

ここでは, 有元・平野 ([4]) が定義した $\mathcal{O}_F$-格子や, それに関する基本的な事柄を述べる.

定義 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,

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

を満たすものが存在することをいう.

定義 2
Λ の基底 $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ に対して,

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

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.

ここで, $\mathbb{R} \subsetneq F$ であ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.

2.3 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.

$$\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\} \tag{3}$$

$m > 0$ 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) $m \not\equiv 1 \pmod 4$ のとき,

$$\mathcal{O}_F = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\} \tag{4}$$

(ii) $m \equiv 1 \pmod 4$ のとき,

$$\mathcal{O}_F = \left\{ a + b \cdot \frac{1+\sqrt{m}}{2} \;\middle|\; a, b \in \mathbb{Z} \right\} \tag{5}$$

である.

2.4 $\mathcal{O}_F$-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 ([4, Theorem 4.4]). そのため, 以後 F を虚二次体とする.

定義 3
F^n における 2 つのベクトル $\boldsymbol{a} = (a_1, \cdots, a_n), \boldsymbol{b} = (b_1, \cdots, b_n)$ の内積を

$$(\boldsymbol{a}, \boldsymbol{b}) = a_1\overline{b}_1 + \cdots + a_n\overline{b}_n \tag{6}$$

(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,

$$\|\boldsymbol{x}\| := \sqrt{(\boldsymbol{x}, \boldsymbol{x})} = \sqrt{|x_1|^2 + |x_2|^2 + \cdots + |x_n|^2} \tag{7}$$

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 4
$\Lambda = \mathcal{O}_F\boldsymbol{b}_1 + \cdots + \mathcal{O}_F\boldsymbol{b}_n$ とする. Λ の基底 $(\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ に対して,

$$\boldsymbol{b}_i^* := \boldsymbol{b}_i - \sum_{j=1}^{i-1} \mu_{ij}\boldsymbol{b}_j^*, \quad \mu_{ij} := \frac{(\boldsymbol{b}_i, \boldsymbol{b}_j^*)}{(\boldsymbol{b}_j^*, \boldsymbol{b}_j^*)} \;\; (1 \le j < i \le n) \tag{8}$$

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 ([2], [3]). A.K.Lenstra, et al. による $\mathbb{Z}$-格子における簡約基底の定義に倣いながら, また, 常に簡約基底が存在するようにそれを改良する. F はガウスの数体, すなわち $F = \mathbb{Q}(\sqrt{-1})$ の場合, 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 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**簡約基底**であるとは, 定義 4 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 :

$$|\mu_{ij}| \le \frac{\sqrt{2}}{2} \;\; (1 \le j < i \le n), \tag{9}$$

$$\|\boldsymbol{b}_i^* + \mu_{i,i-1}\boldsymbol{b}_{i-1}^*\|^2 \ge \frac{3}{4}\|\boldsymbol{b}_{i-1}^*\|^2. \tag{10}$$

この簡約基底の性質として, 次の命題が得られる ([3], [5]):

命題 6
$F=\mathbb{Q}(\sqrt{-1})$ とする. $(\boldsymbol{b}_1,\cdots,\boldsymbol{b}_n)$ を Λ の簡約基底とし, また, $\boldsymbol{b}_i^*$ $(i=1,2,\cdots,n)$, μ_{ij} は定義 4 で定義した通りとする. このとき次が成立する :

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

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

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

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

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

3 主結果

この章では, 虚二次体における整数環 $\mathcal{O}_F$ に対し, $\mathcal{O}_F$-格子において汎用性を高めるために Lenstra, et al. による簡約変数を導入し, また, 簡約基底が常に存在するようにそれを定義する. これにより, 基底簡約を虚二次体における整数環で, 単項イデアル整域である環上に一般化できることを示すことになる. ここで, 単項イデアル整域とは, 環 $\mathcal{O}_F$ の任意のイデアルが 1 個の元により生成される単項イデアルであることをいう.

3.1 簡約変数の導入

定義 7
基底簡約において, **簡約変数** (reduction parameter) とは, 実数 α で,

$$\frac{1}{4}<\alpha<1 \tag{11}$$

を満たすものをいう. 変数の**標準値** (standard value) は,

$$\alpha=\frac{3}{4} \tag{12}$$

とする.

任意の $x\in\mathbb{Q}(\sqrt{m})$ $(m<0, m$ は平方因子をもたない整数) に対して, x に最も近い $\mathcal{O}_F$ の元との距離は, $m\not\equiv 1(\mathrm{mod}\ 4)$ のとき $\frac{\sqrt{1-m}}{2}$ 以下であり, $m\equiv 1(\mathrm{mod}\ 4)$ のとき $\frac{\sqrt{9-m}}{4}$ 以下である. この事実を踏まえて, 簡約基底を次のように定義する:

定義 8
$F=\mathbb{Q}(\sqrt{m})$, $m<0$ で m は平方因子をもたない整数とし, $\Lambda=\mathcal{O}_F\boldsymbol{b}_1+\cdots+\mathcal{O}_F\boldsymbol{b}_n$ とする.
Λ の基底 $(\boldsymbol{b}_1,\cdots,\boldsymbol{b}_n)$ が**簡約基底**であるとは, 定義 4 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. ただし α は $\frac{1}{4}<\alpha<1$ を満たす簡約変数である :
(i) $m\not\equiv 1\ (\mathrm{mod}\ 4)$ のとき

$$|\mu_{ij}|\le\frac{\sqrt{1-m}}{2}\quad(1\le j<i\le n), \tag{13}$$

$$\|\boldsymbol{b}_i^* + \mu_{i,i-1}\boldsymbol{b}_{i-1}^*\|^2 \geq \alpha\|\boldsymbol{b}_{i-1}^*\|^2. \tag{14}$$

(ii) $m \equiv 1 \pmod 4$ のとき

$$|\mu_{ij}| \leq \frac{\sqrt{9-m}}{4} \quad (1 \leq j < i \leq n), \tag{15}$$

および (14).

3.2 基底簡約アルゴリズム

有元によって一般化された, ガウスの数体における整数環上での基底簡約アルゴリズム ([2]) に基づき, 単項イデアル整域の状況下で, これを虚二次体における整数環上に一般化する. 以下にそのアルゴリズムを提示する.

アルゴリズム 1
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 (8) により計算する. このとき, 簡約基底が基底のベクトルの個数 n により帰納的に構成される. 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)
$\mu_{m,m-1}$ の値を $|\mu_{m,m-1}| \leq \frac{\sqrt{1-m}}{2}$ となるようにする.
もし $|\mu_{m,m-1}| > \frac{\sqrt{1-m}}{2}$ ならば, $\boldsymbol{b}_m \leftarrow \boldsymbol{b}_m - \{\mu_{m,m-1}\}\boldsymbol{b}_{m-1}$ 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.
一番近い元が 2 個以上ある場合は, $\{x\}$ はそれらのうちのいずれかとする.
このとき $\mu_{m,m-1} \leftarrow \mu_{m,m-1} - \{\mu_{m,m-1}\}$ となり, $|\mu_{m,m-1}| \leq \frac{\sqrt{1-m}}{2}$ 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) に進む.

(Step B)
$i = m$ に対して, (14) 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) に戻る.

(Step C)
(Step A) と同様に $j = m-2, m-3, \cdots, 1$ に対して,
μ_{mj} の値を $|\mu_{mj}| \leq \frac{\sqrt{1-m}}{2}$ 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) に進む.

定理 9
アルゴリズム 1 は終了する.

証明 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.

$$D_i := \det(\boldsymbol{b}_\mu, \boldsymbol{b}_\nu)_{1 \leq \mu,\nu \leq i} \quad (1 \leq i \leq n) \tag{16}$$

を, $d(\Lambda)^2(=D_n)$ の小行列式とすると, (2), (8) によって,

$$D_i = \prod_{j=1}^{i} \|\boldsymbol{b}_j^*\|^2 \quad (1 \leq i \leq n) \tag{17}$$

を得る. また,

$$D := \prod_{j=1}^{n-1} D_j \tag{18}$$

とする. (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 α ($\frac{1}{4} < \alpha < 1$) 倍になり減少する. したがって, D の値も同様に α 倍となり減少する. しかし, D に対し正の下界 S で次を満たすものが存在する ([4, Theorem 4.4]):

$$D \geq S > 0 \quad (1 \leq i \leq n) \tag{19}$$

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. ∎

謝　辞

本研究に関して有益なご助言を頂きました, 上越教育大学の中川仁教授に感謝の意を表します.

参 考 文 献

[1] 石田信,「代数的整数論」, 森北出版, 1974.

[2] K. Arimoto, *On the termination of quasi LLL Lattice basis reduction algorithm over gaussian number fields*, Far East J. Math. Sci., **109**(1), 175-184, 2018.

[3] K. Arimoto, *On the existence of LLL reduced bases over imaginary quadratic fields*, Sci. Math. Jpn., (submitted).

[4] K. Arimoto and Y. Hirano, *A Generalization of LLL Lattice Basis Reduction over Imaginary Quadratic Fields*, Sci. Math. Jpn., **82**(1), 1-6, 2019.

[5] 有元康一, 平野康之, 虚二次体における LLL 格子基底簡約アルゴリズム, 高度情報化社会に向けた数理最適化の新潮流, 数理解析研究所講究録 **2108**, 115-123, 2019.

[6] M. R. Bremner, *Lattice Basis Reduction*, CRC Press, 2011.

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

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

[9] 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.

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

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