修士論文

二次ディオファントス方程式の求解アルゴリズムについて

2130013
中村 悠人

主指導教員　　小川 瑞史

北陸先端科学技術大学院大学
先端科学技術研究科
(情報科学)

令和 6 年 12 月

abstract

多項式制約解消は、実数解と整数解の場合に分かれ、SMT ソルバーの背景理論として、それぞれ Nonlinear Real number Arithmetic (NRA)、Nonlinear Integer Arithmetic(NIA) に相当し、その手法と決定可能性は 異なる。多項式制約の実数上の充足可能解は、1930 年前後に Tarski が Quantifier elimination が適用可能であり、決定可能性を示した。しかし、そのアルゴ リ ズムは暗黙的であり、実際にアルゴリズムとして整 理 さ れ る のは Tarski 自身によって 1951 年になってからであった。多項式制約の整数解に限る場合を Diophantine 制約とよぶ。Diophantine 方程式の決定可能性は Hilbert の 第十問題として知られ、その否定的解決は Matijasevic により示された。一方。Grunwald は 1981 年単一の二次 Diophantine 方程式は決定可能であることをで示した。その論 文は数ページの短いものであるが、実際の内容は、Hasse 原理を含む古典的二次形式の理論、Hensel 補題を含む可換環論・代数群・Lie 環の基礎理論に基づき、背景知識は多岐にわたると同時にアルゴリズムの記述は暗黙的である。本論文では、Grunwald が提案した単一の二次 Diophantine 方程式の充足可能性の決定アルゴリズムを self-contained に紹介する。その際、数学的命題の証明は基本的に各参考文献にゆずるが、アルゴリズムの記述に必要となる命題、ならびに手続きは余さず記述する。

目次

1 Introduction

1.1 背景

有限個の n 変数整数係数多項式 $f_1, \cdots, f_r, g_1, \cdots, g_s$ を用いて

$$\bigwedge_{1 \leq i \leq r} f_i(x_1, \cdots, x_n) = 0 \wedge \bigwedge_{1 \leq j \leq s} g_j(x_1, \cdots, x_n) \geq 0$$

となる制約式を多項式制約といい、制約を満たす $(x_1, \cdots, x_n)$ のことをその解という。等式のみからなる多項式制約のことを多項式方程式といい、不等式のみからなる多項式制約の事を多項式不等式と呼ぶ。特に、複数の等式からなる等式方程式は連立多項式方程式と呼ぶ。

多項式制約解消は、実数解と整数解の場合に分かれ、SMT ソルバーの背景理論として、それぞれ Nonlinear Real number Arithmetic (NRA)、Nonlinear Integer Arithmetic(NIA) に相当し、その手法と決定可能性は異なる。

多項式制約の実数上の充足可能解は、1930 年前後に Tarski が Quantifier elimination が適用可能であり、決定可能性を示した。しかし、そのアルゴリズムは暗黙的であり、実際にアルゴリズムとして整理されるのは Tarski 自身によって 1951 年になってからであった [TAR 1951]。その計算量は non-elementary で、現在ではより効率の良い（double exponential）アルゴリズムとして、Collins により 1975 年に提案された CAD (Cylindrical Algebraic Decomposition) が知られている [COLL 1975]。現在、CAD の実装として、Mathematica、Maple、Reduce、QEPCAD などが知られている。

多項式制約の整数解に限る場合を Diophantine 制約とよぶ。Diophantine 方程式の決定可能性は Hilbert の第十問題として知られ、その否定的解決は [MATI 1970]、[MATI 1971] により示された。任意の Diophantine 方程式 $\bigwedge_{1 \leq i \leq r} f_i(x_1, \cdots, x_n) = 0$ は、新たな変数と二次式（例えば、新たな変数 z と二次式 xy = z）を導入することで、方程式内の見かけの次数を減らすことができ、一般性を失わずに各 f_i は二次式と仮定できる。したがって、等式の数に制限のない連立 Diophantine 方程式は二次式の範囲で既に決定不能である。方程式の個数を制限した場合、例えば単一方程式に限っても $\Sigma_{i=1}^{r} f_i(x_1, \cdots, x_n)^2 = 0$ と表すことで、単一の四次 Diophantine 方程式は決定不能であることがわかる。

Grunwald は単一の二次 Diophantine 方程式は決定可能であることを [GRUN 1981] で示した。その論文は数ページの短いものであるが、実際の内容は、Hasse 原理を含む古典的二次形式の理論 [CASS 1978]、Hensel 補題を含む可換環論・代数群・Lie 環の基礎理論に基づき、[GRUN 1980] の系となる内容であり、背景知識は多岐にわたると同時にアルゴリズムの記述は暗黙的である。

本論文では、Grunwald が提案した単一の二次 Diophantine 方程式の充足可能性の決定アルゴリズムを self-contained に紹介する。その際、数学的命題の証明は基本的に各参考文献にゆずるが、アルゴリズムの記述に必要となる命題、ならびに手続きは余さず記述する。

応用として、整数上の線形算術を基礎とする Hoare 論理におけるループ不変式生成は一般に計算不能問題であるが、有力な戦略として Farkas 補題を用いた手法がある。その際、二次の Diophantine 制約の整数の充足解をみつけることに帰着する。現状では、単一の二次 Diophantine 方程式のみであるが、拡張の可能性として、(a) 線形制約の追加、(b) 二次 Diophantine 不等式制約解消、(c) 決定可能性を保つ方程式の数と変数の数の制約条件、についても簡単に論じる。なお、著者の知る限り、単一の三次 Diophantine 方程式の決定可能性はいまだ未解決である。二次の場合には二次形式の古典的理論の利用が可能であったが、三次の場合は全く

異なるアプローチが必要となることが予想される。

本論文の構成は以下の通りである。1 章は本節に続き、全体のアルゴリズムの流れを概説する。2 章は、群、可換環などにおける基本的な代数的知識を紹介する。3 章は、線形代数ならびに二次形式の基本的な知識の解説、なお、ここでは二次の多項式方程式を対称行列 A とベクトル $\boldsymbol{b}$ を用いて、$x^\top Ax + \boldsymbol{b}^\top x + c = 0$ と表わす。4 章は、Siegel domain, Minkowski-reduced の概念を説明し、整数行列による二次形式の変換可能性を判定するアルゴリズムについて解説する。5 章は、二次形式の isotropic 性、すなわち原点でない零点を持つかどうかを判定するアルゴリズムについて解説する。二次形式の有理数体 $\mathbb{Q}$ 上での isotropic 性を調べるには実数体 $\mathbb{R}$ および p 進数体 $\mathbb{Q}_p$ での isotropic 性を調べれば良いことが知られている。(Hasseの原理)p 進数および (Hasse の原理) についてもこの章で解説する。6 章は、Lie 環の基本事項の解説、および冪零性に関連する central-flag を導入する。7 章は、$\mathbb{Q}$-群 群の基礎知識、特に $\mathbb{Q}$-群 が半直積分解できるということを説明する。さらに $\mathbb{Q}$-群 とその Lie 環の関係について説明する。8 章は、$\mathbb{Q}$-群 の 半直積分解の要素である冪単群と reductive 群を計算する。9 章は、8 章で計算した冪単群と reductive 群を用いて、$\mathbb{Q}$-群 の arithmetic subgroup の生成元を計算す方法について説明する。10 章は、上記の各アルゴリズムを組み合わせて、単一の二次 Diophantine 方程式の充足可能性の決定アルゴリズムを構成する。Singular な場合（$det\ A = 0$）はより変数が少ない場合に帰着する。Definite な場合（A の固有値がすべて同符号）は、十分大きな範囲で二次 Diophantine 多項式は単調となるので解の探索に上界を設けることができる。Indefinite な場合は、さらに $c^* = 0$ かどうかで場合分けがなされる。なお、ここで c^* は、二次の Diophantine 方程式 $x^\top Ax + \mathbf{b}^\top x + c = 0$ から一次の項を消去して、modulo 演算に帰着する際に導入される定数である（命題 10.1 参照）。$c^* = 0$ の場合は、2 変数の場合と 3 変数以上でさらに場合分けされ、3 変数以上の場合は isotropic かどうかでさらに場合分けが必要となるが、それぞれの場合は比較的簡単である。ここで isotropic 性の判定に Hasse 原理が用いられる。（ちなみに 5 変数以上の場合は、つねに isotropic であることが知られている。）$c^* \neq 0$ の場合は、4 変数以上かどうかで場合分けがなされ、4 変数以上の場合は簡単な modulo 演算に帰着する。2 変数および 3 変数の場合がもっとも複雑な場合であり、最終的に整数上の直交行列のなす群が有限生成であること [**?**]、さらにその生成元の計算アルゴリズム [GRUN 1980]（9 章）、その群による二次形式の軌道計算と等価性判定アルゴリズム（4 章）が必要となる。

Annals of Mathematics 75(3), 485-535 (1962)

11 章では、まとめに代えて、二次 Diophantine 制約の決定可能性にむけて、単一の二次 Diophantine 方程式からの拡張の可能性について簡単に論じる。

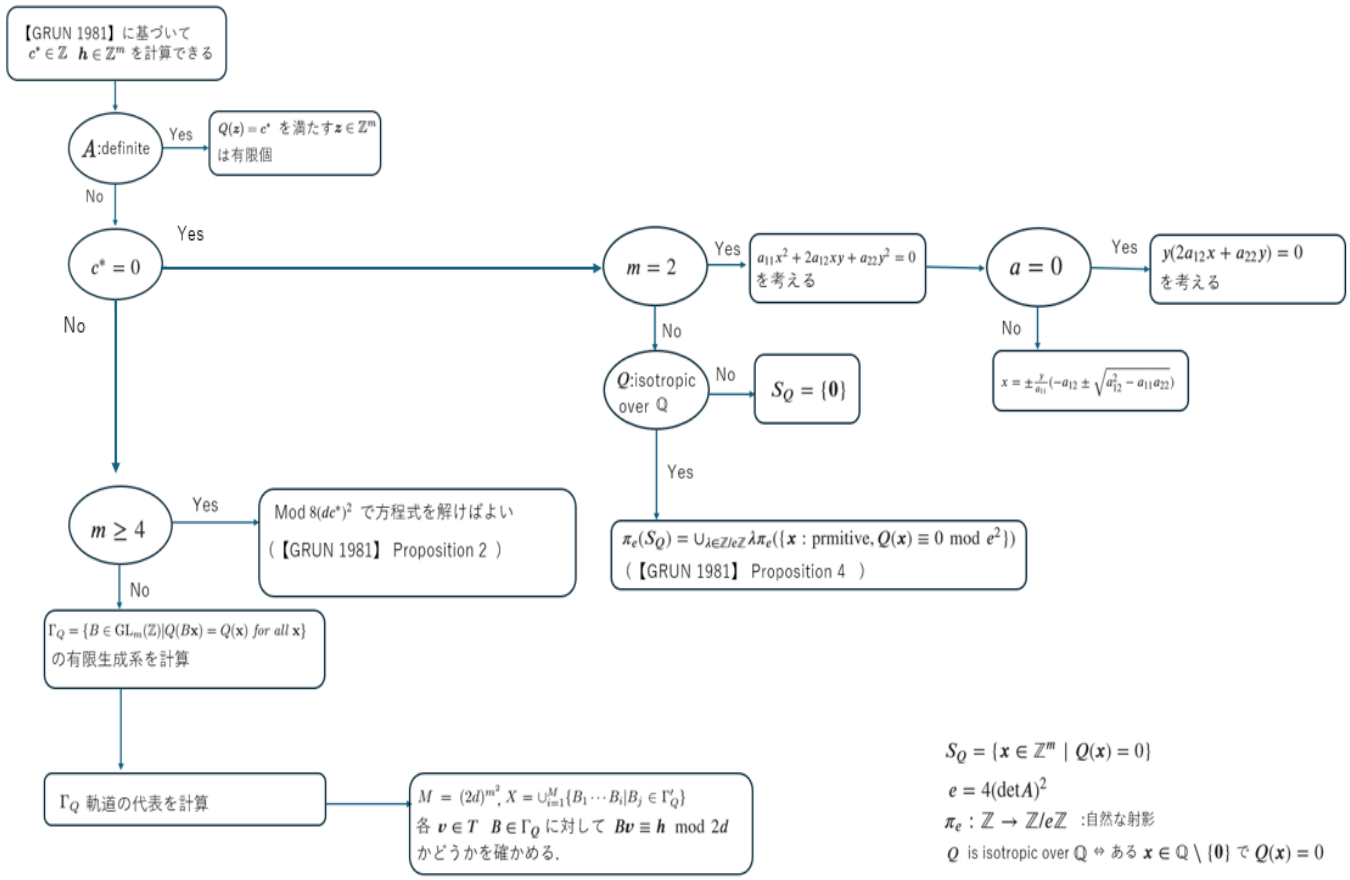
1.2 決定アルゴリズムの概要

$Q(\boldsymbol{x}) = \boldsymbol{x}^\top A\boldsymbol{x}$
$L(\boldsymbol{x}) = \boldsymbol{b}^\top \boldsymbol{x}$

とする。本節では、単一の 2 次ディオファントス方程式

$$Q(\boldsymbol{x}) + L(\boldsymbol{x}) = c \tag{1}$$

を解くアルゴリズムの概要を記す。まず以下にアルゴリズムの大まかなフローチャートを示す。1 変数の場合、及び二次形式が singular な場合は簡単なのでフローチャートには二次形式が regular で $m \geq 2$ な場合のみを書く。



二次の項に対応する係数行列 A が singular な場合は簡単である。$A = O$ の場合は単に一次方程式であるし、$A \neq O$ で singular な場合については、固有値 0 に対応する固有ベクトル $\boldsymbol{v}$ を一列目にもつ行列 $V \in \mathrm{GL}_m\mathbb{Z}$ が計算でき、これによる基底変換で二次形式の変数を減らすことができる。

A が regular な場合が主要な部分である。命題 10.1 により、$d = \det A, \boldsymbol{h} = \tilde{A}\boldsymbol{b}, c^* = 4d^2c + Q(\boldsymbol{h})$ とおくと、方程式 (1) が整数解 $\boldsymbol{x} \in \mathbb{Z}^m$ をもつ ⇔ $\exists \boldsymbol{z} \in \mathbb{Z}^m\,(Q(\boldsymbol{z}) = c^* \wedge \boldsymbol{z} = \boldsymbol{h} \pmod{2d})$ であるため、$Q(\boldsymbol{x})$ が definite である場合は、$Q(\boldsymbol{z}) = c^*$ の整数解の候補を有限個に絞ることができるため、以下 $Q(\boldsymbol{x})$ は indefinite であるとする。c^* が 0 がどうかで大きな場合分けが生じる。

$c^* = 0$ の場合

方程式 $Q(\boldsymbol{x}) = 0$ を解くことになる。$m = 2$ の場合は二次方程式の解の公式と初等整数論の計算により、方程式の解の媒介変数表示を得ることができ、これを mod $2d$ に射影することで命題 10.1 を適用することができる。$m \geq 3$ の場合は $e = 4d^2$ とおき、$Q(\boldsymbol{x})$ の零点集合を mod e に射影した像 $\pi_e(S_Q)$ を計算する。Q が $\mathbb{Q}$ 上 anisotropic であれば $\pi_e(S_Q)$ は原点のみであるから二次形式が $\mathbb{Q}$ 上 isotropic かを判定する (定義 3.35)。Hassse の原理より判定のためには実数体 $\mathbb{R}$ 上および各素数における p 進数体 $\mathbb{Q}_p$ 上 isotropic かを判定すればよい。$\mathbb{R}$ 上の判定については QE を用いることができる。5 変数以上の regular な二次形式は $\mathbb{Q}_p$ 上 isotropic(命題 5.13) である。$3, 4$ 変数の場合は基底変換による二次形

式の対角化及び Hilbert 記号の計算によって判定できる。$Q(\boldsymbol{x})$ が $\mathbb{Q}$ 上 isotropic である場合は、
$\pi_e(S_Q) = \cup_{\lambda\in\mathbb{Z}/e\mathbb{Z}}\pi_e(\{\boldsymbol{x}\in\mathbb{Z}^m|\boldsymbol{x}:\text{primitive}, Q(\boldsymbol{x})\equiv 0 \bmod e^2\})$
と計算できる。(命題 10.10)

$c^*\neq 0$ の場合

二次形式 Q の直交群 $\Gamma_Q = \{B\in \mathrm{GL}_m(\mathbb{Z})|Q(B\mathbf{x}) = Q(\mathbf{x}) \text{ for all } \mathbf{x}\}$ の有限生成系 Γ'_Q および Γ_Q-軌道の完全代表系 T_Q の部分集合 $T'_Q = \{\mathbf{v}\in T_Q|Q(\mathbf{v}) = c^*\}$ を計算し、$X = \cup_{i=0}^{(2d)^{m^2}+1}\{g_1\cdots g_i \mid g_1,\ldots,g_i\in\Gamma'_Q\}$、$\pi_{2d}:\mathrm{M}_m(\mathbb{Z})\to\mathrm{M}_m(\mathbb{Z}/2d\mathbb{Z})$ を自然な射影とすると、鳩ノ巣原理により $\pi_{2d}(X) = \pi_{2d}(\Gamma_Q)$ なので、X の各要素 g と T'_Q の各要素 $\boldsymbol{v}$ に対して $g\boldsymbol{v}$ が mod $2d$ で $\boldsymbol{h}$ と合同なものがあるかを調べことで方程式 (1) の可解性を判定できる。直交群 Γ_Q は有理数係数多項式で特徴づけられた $\mathbb{Q}$-群の arithmetic-subgroup なので、[BHC 1962]、[GRUN 1980] の議論にしたがって有限生成系を計算することができる。Γ_Q の生成系計算の仮定においては、$\mathbb{Q}$-群 $G_Q = \{B\in\mathrm{GL}_m(\mathbb{C})|Q(B\mathbf{x}) = Q(\mathbf{x}) \text{ for all } \mathbf{x}\}$ を unipotent な部分と reductive な部分の半直積に分解することが重要である。この分解は行列群を $\{\begin{pmatrix}1 & * & * & *\\ 0 & 1 & \ddots & *\\ \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & \cdots & 1\end{pmatrix}\}$ の形をした部分群 (対角成分がすべて 1 の上三角行列のみからなる群) と $\{\begin{pmatrix}\mathrm{GL}_{r_1}(\mathbb{C}) & O & O & O\\ O & \mathrm{GL}_{r_2}(\mathbb{C}) & \ddots & O\\ \vdots & \vdots & \vdots & \vdots\\ O & O & \cdots & \mathrm{GL}_{r_k}(\mathbb{C})\end{pmatrix}\}$ の部分群の積に分けることに相当する。G_Q を unipotent な N と reductive な H に分解できたとすると、$N\cap\mathrm{GL}_m(\mathbb{Z})$ と $H\cap\mathrm{GL}_m(\mathbb{Z})$ のそれぞれは有限の生成系を計算することができる。これを用いて、Γ_Q の生成系を計算することができる。T'_Q は [GRUN 1981]5 章の議論にしたがって計算することができる。(アルゴリズム 10.18) この際、二つの二次形式が $\mathrm{GL}_m(\mathbb{Z})$ の行列による基底変換で移りあうかどうかを判定するアルゴリズムを本質的に用いる。(アルゴリズム 4.25)

2 群、環、体の基本事項

2.1 群

この節では本論文で用いる群、環、体の一般論について述べる。群論については [雪江 群 2010] を参照している。

定義 2.1.

空でない集合 G とその上の 2 項演算 $\cdot: G\times G\to G$ の組 $(G,\cdot)$ が群であるとは、以下の 3 つの条件を満たすことを言う.

1.*(結合法則)* 任意の $g,h,k\in G$ について,$(g\cdot h)\cdot k = g\cdot(h\cdot k)$ が成り立つ。

2.*(単位元の存在)* どんな $g\in G$ についても $g\cdot e_G = e_G\cdot g = g$ になるような *(g には依存しない)*$e_G\in G$ が存在する. このような e_G は存在すれば一意であり G の単位元と呼ばれる.

3. *(逆元の存在)* 任意の $g \in G$ に対して $g \cdot g^{-1} = g^{-1} \cdot g = e_G$ を満たす $g^{-1} \in G$ が存在する.
また, 上記 1〜3 に加えて
4. *(交換法則)* 任意の $g, h \in G$ について $g \cdot h = h \cdot h$ が成り立つ.
を満たす群は可換群, あるいはアーベル群と呼ばれる.

文脈上演算が明らかな場合は単に G のみをさして群と言うことも多い。また、群の演算 $\cdot$ を乗法としてみる文脈では $g \cdot h$ を gh と書くように演算の記号を省略することも多い。

例 2.2.
整数全体 $\mathbb{Z}$、有理数全体 $\mathbb{Q}$, 実数全体 $\mathbb{R}$、複素数全体 $\mathbb{C}$ に通常の加法で演算を定めたもの $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ は 0 を単位元とするアーベル群になる。また、$\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$ に通常の乗法で演算を定めたものも 1 を単位元とするアーベル群になる。

例 2.3.
全単射 $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ 全て集めた集合を S_n で表す. これは写像の合成で群になる。この群を対称群という。

定義 2.4.
要素の個数が有限個である群を有限群という。有限群 G の要素の個数を G の位数とよび、$|G|$ で表す.

定義 2.5.
群 G の部分集合 H が G の演算によって閉じている、すなわち
1. $e_G \in H$
2. $a, b \in H$ ならば $ab \in H$
3. $a \in H$ ならば $a^{-1} \in H$
をみたすとき、H を G の部分群という。

定義 2.6.
G を群,H を G の部分群とする.
1. G 上の二項関係を $x^{-1}y \in H$ で定めるとき、これは同値関係となる.$x \in G$ の同値類を xH のように書き、x の H による左剰余類とよぶ. この同値関係による商集合、すなわち左剰余類の集合を G/H とかく。
2. G 上の二項関係を $yx^{-1} \in H$ で定めるとき、これも同値関係となる. $x \in G$ の同値類を Hx のように書き,x の H による右剰余類とよぶ. この同値関係による小集合、すなわち右剰余類の集合を $G\backslash H$ とかく.

左剰余類の個数と右剰余類の個数は等しいことが知られている。(両方とも無限個の場合も含む) また、各剰余類について、その要素の個数は部分群 H の要素の個数に等しい. 言い換えると以下が成り立つ。

命題 2.7.
H を G の部分群とするとき、以下 1, 2 がなりたつ。
1. $|G/H| = |G\backslash|$
2. 任意の $g \in G$ について $|gH| = |Hg| = |H|$
上記は両方が ∞ の場合も含む。

$|G/H|$ あるいは $|G\backslash H|$ のことを H の G における指数 (index) といい、$|G:H|$ とかく.

定義 2.8.
H を G の部分群とする. 任意の $g \in G$、$h \in H$ について $ghg^{-1} \in H$ となるとき、H を G の正規部分群という。

正規部分群について、以下の命題が成り立つ。

命題 2.9.
G が群、N が G の正規部分群,$g \in G$ とするとき、$gN = Ng$ が成り立つ。つまり、N が G の正規部分群であれば、$G/N = G\backslash N$ が成り立つ。

このことから群 G の正規部分群 N の剰余類の集合 G/H は G から融合される自然な演算によって新たな群をなす。

命題 2.10.
G を群、N を G の正規部分群とする。$gN, hN \in G/N$ に対して積を
$(gN)(hN) = (gh)N$
で定めると、これは代表元の取り方によらず well-defined であり、G/N が個の演算によって群になる。単位元は $e_G N$ であり gN の逆元は $g^{-1}N$ である。

上記のように定められた群を G の N による剰余群と呼ぶ。

定義 2.11.
G_1, G_2 を群とする。写像 $\phi : G_1 \to G_2$ が準同型であるとは、$\phi(xy) = \phi(x)\phi(y)$ が任意の $x, y \in G_1$ についてなりたつことをいう。準同型 $\phi : G_1 \to G_2$ が全単射であるとき、ϕ は同型であるという。群 G_1, G_2 の間に同型 $phi : G_1 \to G_2$ が存在するとき、G_1, G_2 は同型であるといい。$G_1 \simeq G_2$ とかく。

注 2.12.
$\phi : G_1 \to G_2$ が準同型であるとき、G_1 の単位元は ϕ によって G_2 の単位元にうつる。また、$\phi : G_1 \to G_2$ が同型である場合、$\phi^{-1} : G_2 \to G_1$ もまた準同型である。*(*したがって同型である。*)*

定義 2.13.
$\phi : G_1 \to G_2$ を群の準同型とする. 準同型 ϕ の核と像をそれぞれ
$\mathrm{Ker}(\phi) = \{g \in G_1 \mid \phi(g) = e_{G_2}\}$
$\mathrm{Im}(\phi) = \{\phi(g) \mid g \in R_1\}$
で定める。$\mathrm{Ker}(\phi)$ は G_1 の正規部分群、$\mathrm{Im}(\phi)$ は G_2 の部分群である。

Ker と Im について、準同型定理と呼ばれる以下の性質が成り立つ。

命題 2.14. *(*準同型定理*)*
$\phi : G_1 \to G_2$ を群の準同型とするとき、$G_1/\mathrm{Ker}(\phi) \simeq \mathrm{Im}(\phi)$ がなりたつ。

定義 2.15.
G を群、$S \subseteq G$ を部分集合とし,S^{-1} で $\{x^{-1} \mid x \in S\}$ を表すとする。$x_1 \cdots x_n$ $(x_i \in S \cup S^{-1} \cup \{e_G\})$ の形をした G の元を S の元による語 *(*word*)* という. ただし、$n = 0$ の場合は単位元 e を指すとする。

S の元による語全体は G の部分群になる。

命題 2.16.
G を群、$\langle S\rangle$ によって $S \subseteq G$ の元による語全体の集合とする. このとき、以下 $1, 2$ がなりたつ。
1 $\langle S\rangle$ は G の部分群になる。
2 H が G の部分群であって $S \subseteq H$ であるとき、$\langle S\rangle \subseteq H$ となる。つまり、$\langle S\rangle$ は S を含む G の部分群のうち最小のものである。

$\langle S\rangle$ のことを S によって生成された部分群、S のことを生成系、S の元のことを生成元という。S が有限集合で $\langle S\rangle = G$ であるとき G は有限生成であるという。有限集合によって生成された部分群 $\langle\{g_1, \ldots, g_m\}\rangle$ を $\langle g_1, \ldots, g_m\rangle$ のように省略して書くことがある。

定義 2.17.
二つの群 N, H に対して N の H による半直積とは
1. N は G の正規部分群、H は G の部分群であり、$G = NH = \{nh \mid n \in N, h \in H\}$
2. $N \cap H = \{e_G\}$
を満たす群 G のことであり、これを $N \rtimes H$ と書く。

群の一般論により、与えられた正規部分群 N に対してそれを要素に持つ半直積分解が存在することが知られている。

命題 2.18.
N を群 G の正規部分群とする。このとき、ある部分群 $H \subseteq G$ が存在して $N \rtimes H$ となる。

定義 2.19.
群 G の要素 g, g' について、$g^{g'} = g'^{-1}gg'$ と定める。また、G の部分群 H について、$H^g = \{g^{-1}hg \mid h \in H\}$ と定める。

定義 2.20.
G を群、X を集合とする。G の X への *(左)* 作用とは写像 $G \times X \ni (g, x) \mapsto gx$ であって以下 $1, 2$ をみたすものである。
1. $e_G x = x$
2. $g(hx) = (gh)x$
G から X への作用があるとき G は X に *(左から)* 作用するという。

定義 2.21.
群 G が集合 X に作用しているとする。$x \in X$ に対して x の安定化部分群 (stabilizer subgroup) $\mathrm{Stab}_G(x) \subseteq G$ を
$\mathrm{Stab}_G(x) = \{g \in G \mid gx = x\}$
で定める。これは G の部分群になっている。

定義 2.22.
群 G が集合 X に作用しているとする。$x \in X$ に対して x の G による軌道を

$Gx = \{gx \mid g \in G\}$
で定める。

命題 2.23.
群 G が集合 X に作用しているとする。X 上の二項関係を $Gx = Gy$ で定めるとこれは同値関係になる。したがってこの同値関係による商集合は X の G による軌道全体の集合である。

$y \in Gx$ であることを y が軌道 Gx の代表元であるとよぶ。また、各軌道の代表元をちょうど一つずつ含む集合を X の G による軌道の完全代表系と呼ぶ。

2.2 環と体

環と体の一般論については [雪江 環 2010] 及び [ATY 1994] を参照している. またグレブナー基底については [日比 2011] を参照している。

定義 2.24. 空でない集合 R とそれぞれ加法、乗法と呼ばれる 2 つの 2 項演算 $+ : R \times R \to R, \cdot : R \times R \to R$ の組 $(R, +, \cdot)$ が環であるとは、以下の条件を満たすことをいう。
1. 加法 $+$ について $(R, +)$ がアーベル群になる、すなわち
1-1 (加法結合法則) 任意の $a, b, c \in R$ について、$(a + b) + c = a + (b \cdot c)$ が成り立つ。
1-2 (加法単位元の存在) どんな $a \in R$ についても $a + 0 = 0 + a = a$ になるような *(*a には依存しない*)*$0 \in R$ が存在する。このような 0 は存在すれば一意であり R の零元と呼ばれる。
1-3 (加法逆元の存在) 任意の $a \in R$ に対して $a + (-a) = (-a) + a = 0$ を満たす $-a \in R$ が存在する。
1-4 (加法の交換法則) 任意の $a, b \in R$ について $a + b = b + a$ が成り立つ。
2. (乗法結合法則) 任意の $a, b, c \in R$ について,$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ が成り立つ。
3. (乗法単位元の存在) どんな $a \in R$ についても $a \cdot 1_R = 1 \cdot 1_R = a$ になるような *(*a には依存しない*)*$1_R \in R$ が存在する。このような 1_R は存在すれば一意であり R の *(*乗法*)* 単位元と呼ばれる。
4. (分配法則) 任意の $a, b, c \in R$ について、$a \cdot (b + c) = a \cdot b + a \cdot c$ および $(b + c) \cdot a = b \cdot a + c \cdot a$ が成り立つ。
また、上記 1 4 に加えて
5. (乗法の交換法則) 任意の $a, b \in R$ について $a \cdot b = b \cdot a$ が成り立つ。
を満たす場合環は可換環と呼ばれる。
さらに、R が可換環であって
6. (乗法逆元の存在) 任意の $a \in R \setminus \{0\}$ に対して $a \cdot a^{-1} = a^{-1} \cdot a = 1_R$ を満たす $a^{-1} \in R$ が存在する。
6. $0 \neq 1$
を満たす場合、R は体であるという。一元集合 $\{0\}$ は $0 + 0 = 0 \cdot 0 = 0$ 定めることで自明に環となる。この環を零環と呼ぶ。

群の場合と同様、文脈上演算が明らかな場合は単に R のみをさして環と言うことも多く、乗法の記号 $\cdot$ を省略して $a \cdot b$ を ab と書くことも多い. また以後可換環を扱うことが多いので特に断りのない限り単に環といった場合可換環を指すものとする。

定義 2.25.
R を環とする。$x \in R$ が R の単元であるとは $xy = 1$ となる $y \in R$ が存在することをいう。R の単元全体の

集合を $R^\times$ と書く。

例 2.26.
$\mathbb{Z}^\times = \{-1, 1\}$ である。また、体 F について $F^\times = F \setminus \{0\}$ である。

定義 2.27. R を環とする。$x \in R$ が零因子であるとは、$xy = 0$ になるような $y \in R$ が存在することをいう。0 以外の零因子を持たずかつ零環でもない環を整域という。

定義 2.28. R を整域とする。$R \times (R \setminus \{0\})$ に二項関係 $\sim$ を $(a, b) \sim (a', b') \overset{def}{\Leftrightarrow} ab' = a'b$ で定めるとこれは同値関係になる。(a, b) の同値類を $\frac{a}{b}$ のように書く。$R/\sim$ に加法、乗法を $\frac{a}{b} + \frac{a'}{b'} = \frac{ab'+a'b}{bb'}, \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$ によって定めると $\frac{0}{1}$ を零元、$\frac{1}{1}$ を単位元とする体になる。この体を R の商体とよび、$\mathrm{Frac}(R)$ と書く。

例 2.29. 整数の環 $\mathbb{Z}$ の商体は有理数体 $\mathbb{Q}$ である。

定義 2.30. R を環とする.R 係数 1 変数多項式全体の集合 $R[X] = \{f(X) = \sum_{i=0}^n a_i X^i \ (a_i \in R)\}$ に対して加法、乗法を
$\sum_{i=0}^n a_i X^i + \sum_{i=0}^n b_i X^i = \sum_{i=0}^n (a_i + b_i) X^i$
$(\sum_{i=0}^n a_i X^i) \cdot (\sum_{i=0}^m b_i X^i) = \sum_{k=0}^{m+n} (\sum_{i+j=k} a_i b_j) X^k$
で定めるとこれは環になる。この環を R 係数 1 変数多項式環と呼ぶ。$m \geq 2$ について R 係数 m 変数多項式環 $R[X_1, \ldots, X_m]$ を再帰的に
$R[X_1, \ldots, X_m] = R[X_1, \ldots, X_{m-1}][X_m]$
によって定める。

定義 2.31. 可換環 R の部分集合 $\mathfrak{a} \subseteq R$ がイデアルであるとは以下の条件 $1, 2$ を満たすことをいう。
1. $\mathfrak{a}$ は R の加法でアーベル群になる。2. 任意の $a \in R, x \in \mathfrak{a}$ について $ax \in \mathfrak{a}$ となる。

定義 2.32. R を可換環、$\mathfrak{a} \subseteq R$ をイデアルとする。R 上の二項関係を $a - b \in \mathfrak{a}$ で定めるとこれは同値関係になっている。R この同値関係で割った商集合には R の加法と乗法から自然に演算が定める。これによって定義される可換環 $(R/\mathfrak{a}, +, \cdot)$ を R を $\mathfrak{a}$ で割った剰余環、あるいは単に剰余環と呼ぶ。
$a \in R$ に対して、a の同値類を対応させる写像 $\pi_\mathfrak{a} : R \to R/\mathfrak{a}$ を自然な射影と呼ぶ。

定義 2.33.
R を環、$S \subseteq R$ を部分集合とする。$\sum_{i=1}^m a_i x_i \ (a_i \in R, x_i \in S)$ の形の R の要素全体の集合はイデアルになる。これを $\langle S \rangle$ と書き、S で生成されるイデアルという。有限集合 $\{x_1, \ldots, x_m\}$ で生成されるイデアルを $\langle x_1, \ldots, x_m \rangle$ と書く。R のイデアル $\mathfrak{a}$ がある有限集合で生成されるとき、$\mathfrak{a}$ は有限生成であるという。

定義 2.34.
$\boldsymbol{x} = (x_1, \ldots, x_m) \in R^m$ が primitive であるとは $\langle x_1, \ldots, x_m \rangle = \langle 1 \rangle = R$ となることを言う。

例 2.35.
$\boldsymbol{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^m$ が primitive である $\Leftrightarrow \gcd(x_1, \ldots, x_m) = 1$ である

定義 2.36.
環 R のイデアル $\mathfrak{p}$ が素イデアルであるとは、$xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ または $y \in \mathfrak{p}$ が成り立つことをいう。

定義 2.37.
R_1, R_2 を環とする。写像 $\phi : R_1 \to R_2$ が
1. $\phi(x+y) = \phi(x) + \phi(y)$
2. $\phi(xy) = \phi(x)\phi(y)$
3. $\phi(1_{R_1}) = 1_{R_2}$
を満たすとき ϕ を準同型であるという。準同型 $\phi : R_1 \to R_2$ が全単射であるとき、ϕ は同型であるという。環 R_1, R_2 の間に同型 $\phi : R_1 \to R_2$ が存在するとき、R_1, R_2 は同型であるといい、$R_1 \simeq R_2$ とかく。

定義 2.38.
$\phi : R_1 \to R_2$ を環の準同型とする。準同型 ϕ の核と像をそれぞれ
$\mathrm{Ker}(\phi) = \{a \in R_1 \mid \phi(a) = 0\}$
$\mathrm{Im}(\phi) = \{\phi(a) \mid a \in R_1\}$
で定める。$\mathrm{Ker}(\phi)$ は明らかに R_1 のイデアルであり、$\mathrm{Im}(\phi)$ は R_2 の部分環である。

Ker と Im について、群場合と同様、準同型定理が成り立つ。

命題 2.39. *(準同型定理)*
$\phi : R_1 \to R_2$ を環の準同型とするとき、$R_1/\mathrm{Ker}(\phi) \simeq \mathrm{Im}(\phi)$ がなりたつ。

命題 2.40. R を環とする. 以下の二条件は同値である。
1. 任意の R のイデアルの増大列 $I_1 \subseteq I_2 \subseteq \cdots$ にたいして $N \in \mathbb{N}$ が存在して $I_N = I_{N+1} = \cdots$ となる。
2. R の任意のイデアルは有限生成である。

命題 2.40 の条件 $1, 2$ のいずれか (したがって両方) を満たす環をネーター環と呼ぶ。

命題 2.41. R がネーター環であるとき、1 変数多項式環 $R[X]$ もまたネーター環である。

系 2.42. R がネーター環であるとき、多項式環 $R[X_1, \ldots, X_m]$ もまたネーター環である。特に、体 F 上の多項式環 $F[X_1, \ldots, X_m]$ はネーター環であるためそのイデアルはすべて有限生成である。

定義 2.43.
環 A の素イデアルの包含関係の列 $\mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_r$ の長さ r の上限を環 A のクルル次元といい,$\dim A$ で表す。環 A のイデアル $\mathfrak{a}$ について、剰余環 $A/\mathfrak{a}$ のクルル次元をイデアル $\mathfrak{a}$ の次元とよび、$\dim\mathfrak{a}$ と書く。

命題 2.44.
F を体とするとき、$\dim F[X_1, \ldots, X_m] = m$ である。したがって $\dim F[X_1, \ldots, X_m]$ の任意のイデアルの次元は m 以下である。

定義 2.45.
$\mathfrak{a}$ を環 R のイデアルとする。$\mathfrak{a}$ の根基 $\sqrt{\mathfrak{a}}$ を
$\sqrt{\mathfrak{a}} = \{x \in R \mid \exists n > 0\ x^n \in \mathfrak{a}\}$
と定義する。

定義 2.46.

環 R のイデアル $\mathfrak{q}$ が $xy \in \mathfrak{q} \Rightarrow x \in \mathfrak{q}$ または $\exists n > 0\ y^n \in \mathfrak{q}$ という性質をみたすとき、$\mathfrak{q}$ は準素イデアルであるという。

命題 2.47.
$\mathfrak{q}$ が準素イデアルであるとき、$\sqrt{\mathfrak{q}}$ は $\mathfrak{q}$ を含む素イデアルのうち包含関係で最小のものである。

定義 2.48.
$\mathfrak{q}$ が準素イデアルで $\mathfrak{p} = \sqrt{\mathfrak{q}}$ であるとき, $\mathfrak{q}$ を $\mathfrak{p}$-準素イデアルであるという。

定義 2.49.
環 R のイデアル $\mathfrak{a}$ が準素イデアル有限個の共通部分で書けるとき $\mathfrak{a}$ は準素分解を持つという。イデアル $\mathfrak{a}$ の準素分解 $\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{q}_i$*(*各 $\mathfrak{q}_i$ は準素イデアル*)* が
1. $i \neq j$ ならば $r(\mathfrak{q}_i) \neq r(\mathfrak{q}_j)$
2. $\mathfrak{q}_i \not\supseteq \cap_{j \neq i} \mathfrak{q}_j$
を満たすとき、この準素分解を $\mathfrak{a}$ の最短準素分解という。

最短準素分解には以下の意味の一意性がある。

命題 2.50.
$\mathfrak{a}$ は準素分解を持つイデアルであり、$\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{q}_i$ を最短準素分解とする。$\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ とおく. このとき、集合 $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ は $\mathfrak{a}$ の最短準素分解のやり方によらない。

命題 2.50 の $\mathfrak{p}_i$ を $\mathfrak{a}$ の素イデア、あるいは $\mathfrak{a}$ に属している素イデアルと呼ぶ。また、$\sqrt{\mathfrak{a}} = \cap_{i=1}^{n} \mathfrak{p}_i$ であるが $\sqrt{\mathfrak{a}}$ をこの形で書くことを $\mathfrak{a}$ の根基の (最短) 素イデアル分解という。
準素イデアル $\mathfrak{q}$ が $\sqrt{\mathfrak{q}} = \mathfrak{q}$ であるとき、定義から明らかに $\mathfrak{q}$ は素イデアルである。したがって以下が成り立つ。

命題 2.51.
$\mathfrak{p}$ が素イデアル $\Leftrightarrow$ $\mathfrak{p}$ が準素イデアルでかつ $\sqrt{\mathfrak{q}} = \mathfrak{q}$

素イデアルは明らかに準素イデアルであるから、$\mathfrak{p}$ が素イデアルなら $\mathfrak{p} = \mathfrak{p}$ 自体が最短準素分解であり、$\mathfrak{p}$ に属している素イデアルは $\mathfrak{p}$ のみである。したがって、最短準素分解及び最短素イデアル分解ができれば命題 2.51 により与えられたイデアルが素イデアルかどうかを判定することができる。$\mathbb{Q}[X_1, \ldots, X_m]$ のイデアルについては準素分解パッケージ noro_pd.rr の noro_pd.syci_dec 関数を使えば最短準素分解が、noro_pd.prime_dec 関数を使えば根基の最短素イデアル分解が行えるので素イデアルかどうかの判定も行うことができる。

ネーター環のイデアルは準素分解を持つことが知られている。

命題 2.52.
R がネーター環であるとき、R のすべてのイデアルは準素分解をもつ。特に体 F を係数ににもつ多項式環 $F[X_1, \ldots, X_m]$ のイデアルは準素分解を持つ。

定義 2.53.
F を体とする。係数が *1* の単項式たちの集まり $\{X_1^{e_1} \cdots X_m^{e_m} \mid (e_1, \ldots, e_m) \in \mathbb{N}^m\} \subseteq F[X_1, \ldots, X_m]$ に対して $\mathbb{N}^m$ における辞書式順序によって順序を定める。この順序を辞書式単項式順序と呼ぶ。

定義 2.54.
F を体とし、$f \in F[X_1, \ldots, X_m]$ を 0 でない多項式とする。f は $a_1, \ldots, a_s \in F$, 相異なる単項式 $u_1, \ldots, u_t$ を用いて $f = a_1u_t + \cdots + a_tu_t$ と一意に表すことができる。単項式の集合 $\{u_1, \ldots, u_t\}$ のことを f の台と呼ぶ。f の台に属する単項式のうち辞書式単項式順序において最大であるものを f のイニシャル単項式と呼び $\mathrm{ini}_<(f)$ とかく。

定義 2.55.
F を体とし $\mathfrak{a} \subseteq F[X_1, \ldots, X_m]$ を $\{0\}$ でないイデアルとする。$\mathfrak{a}$ のイニシャルイデアル $\mathrm{ini}(\mathfrak{a})$ とは集合 $\{\mathrm{ini}_<(f) \mid f \in \mathfrak{a}\}$ で生成されるイデアルのことである。

定義 2.56.
F を体とし $\mathfrak{a} \subseteq F[X_1, \ldots, X_m]$ を $\{0\}$ でないイデアルとする. このとき、$\mathfrak{a}$ のグレブナー基底とは $\mathfrak{a}$ に属する有限個の多項式の集合 $\{g_1, \ldots, g_r\}$ であって、$\{\mathrm{ini}_<(g_1), \ldots, \mathrm{ini}_<(g_r)\}$ がイニシャルイデアル $\mathrm{ini}(\mathfrak{a})$ の生成系になっているものをいう。

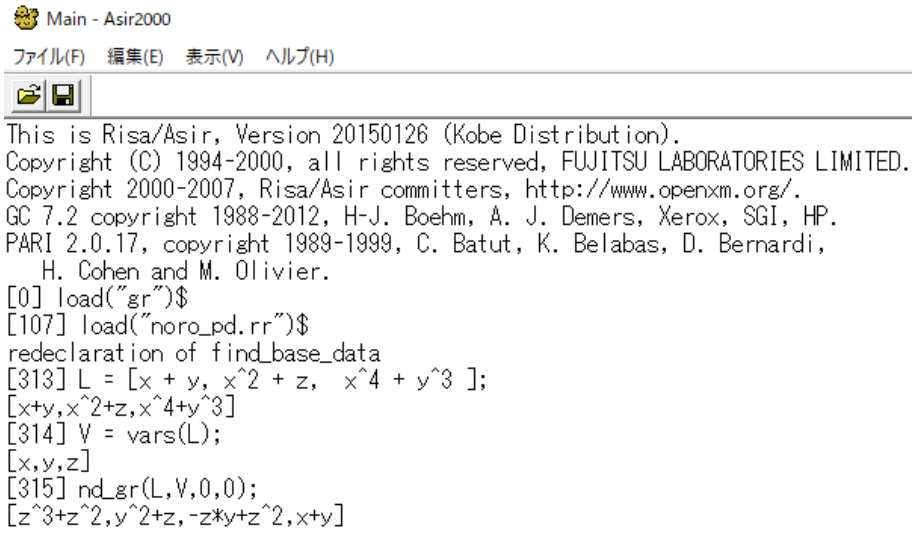
定義 2.57.
F を体とし $\mathfrak{a} \subseteq F[X_1, \ldots, X_m]$ を $\{0\}$ でないイデアルとする。$\mathfrak{a}$ のグレブナー基底 $\{g_1, \ldots, g_r\}$ が被約グレブナー基底であるとは、以下の条件を満たすことをいう。
1. 各多項式 g_i における $\mathrm{ini}_<(g_i)$ の係数は 1 である
2. $i \neq j$ のとき g_j の台に属する単項式は $\mathrm{ini}_<(g_i)$ で割り切れない。

命題 2.58. (*[日比 2011]* 補題 1.1.7)
F を体とし $\mathfrak{a} \subseteq F[X_1, \ldots, X_m]$ を $\{0\}$ でないイデアルとする。このとき、$\mathfrak{a}$ の被約グレブナー基底は必ず存在する。また、被約グレブナー基底は一意である。

2.3 イデアル計算のアルゴリズムと数式処理システムを用いた実装例

$\mathbb{Q}[X_1, \ldots, X_m]$ のイデアルの被約グレブナー基底は数式処理システム Risa/Asir とその上で動くパッケージ noro_pd.rr を用いて計算することができる.

例 2.59. 以下は Risa/Asir でのグレブナー基底計算の実行例である。$\langle x + y, x^2 + z, x^4 + y^3 \rangle$ の被約グレブナー基底は $\{z^3 + z^2, y^2 + z, -yz + z^2, x + y\}$ という結果を得ている。



以下、疑似コード中では $\mathbb{Q}[X_1,\ldots,X_m]$ のイデアル $\mathfrak{a}$ に対して,nd_gr($\mathfrak{a}$) によって、$\mathfrak{a}$ のグレブナー基底の要素を並べたリストを表すとする。グレブナー基底はイデアル $\mathfrak{a}$ に対して一意ではないが被約グレブナー基底はイデアルに対して一意である。被約グレブナー基底を計算し、それらが一致するかどうかを調べることで二つのイデアルが等しいかどうかを判定することができる。

アルゴリズム【whether $\mathfrak{a}=\mathfrak{b}$**】**

Input:$\mathbb{Q}[X_1,\ldots,X_m]$ のイデアル $\mathfrak{a},\mathfrak{b}$ の生成元のリスト $[f_1,\ldots,f_r]$ および $[g_1,\ldots,g_s]$

Output:$\mathfrak{a}=\mathfrak{b}$ かどうか

```
1 :     B_1 ← nd_gr(a)
2 :     B_2 ← nd_gr(b)
3 :     if length(B_1) ≠ length(B_2)
4 :         output FALSE
5 :     count ← 0
3 :     for f_i in B_1
4 :         for g_j in B_2
5 :             if f_i = g_j
6 :                 count ←count + 1
7 :     if count = length(B_1)
8 :         output TRUE
9 :     else
10 :        output FALSE
```

$\mathfrak{a}\subseteq\mathfrak{b}$ かどうかも以下のアルゴリズムで判定できる。

アルゴリズム【whether $\mathfrak{a}\subseteq\mathfrak{b}$**】**

Input:$\mathbb{Q}[X_1, \ldots, X_m]$ のイデアル $\mathfrak{a}, \mathfrak{b}$ の生成元のリスト $[f_1, \ldots, f_r]$ および $[g_1, \ldots, g_s]$
Output:$\mathfrak{a} \subseteq \mathfrak{b}$ かどうか

```
1 :     c ← a ∩ b
2 :     if a = c
3 :         flag ← TRUE
4 :     else
5 :         flag ← FALSE
6 :     output flag
```

$\mathbb{Q}[X_1, \ldots, X_m]$ のイデアル $\mathfrak{a}$ のクルル次元 $\dim\mathfrak{a}$ を数式処理システム Macaulay2 を用いて計算することができる。

例 2.60.
以下は Macaulay2 の実行画面の例である。$I = \langle x^3 - yz, xy \rangle \in \mathbb{Q}[x, y, z]$ のクルル次元を計算しており,$\dim I = 1$ という結果を得ている.

```
Macaulay2, version 1.24.05
with packages: ConwayPolynomials, Elimination, IntegralClosure, InverseSystems, Isomorphism, LLLBases, MinimalPrimes,
               OnlineLookup, PrimaryDecomposition, ReesAlgebra, Saturation, TangentCone, Truncations, Varieties

i1 : R = QQ[x,y,z];

i2 : I = ideal(x^3-y*z, x*y);

o2 : Ideal of R

i3 : dim I

o3 = 1
```

2.4 実数上の量化子除去 (QE) について

多項式を用いて書かれた実数上の条件は量化子除去 (QE) アルゴリズムによって真偽を決定できるうえ、条件を満たす実数が存在する場合はその実数を任意精度で近似できる有理数列を得ることができる。

命題 2.61. $S(x_1, \ldots, x_r)$ を $+, \cdot, =, <$ 及び論理記号 $\vee, \wedge, \neg, \forall, \exists$ を用いて一階述語論理で書かれた実数についてのステートメントとする.QE(Quantifier Elimination) アルゴリズム *([COLL 1975]*、*[TAR 1951])* に

よって
1. $\exists x_1, \ldots, x_r S(x_1, \ldots, x_r)$ の真偽を決定できる.
2. $\exists x_1, \ldots, x_r S(x_1, \ldots, x_r)$ が真である場合に $S(x_1, \ldots, x_r)$ を満たす実数 $x_1, \ldots, x_r$ に対して
$f_1(x_1) = \cdots = f_r(x_r) = 0$ となる 1 変数整数係数既約多項式 $f_1, \ldots, f_r$ 及び $i = 1, \ldots, r$ にたいして I_i に入る f_i の実根が x_i のみになるような十分小さい区間 I_i を得ることができる。(代数的実数の区間表示) QE アルゴリズムによってこのように多項式と区間によって実数の表現を得ることを以後実数を近似的に求めるという。実数を近似的に求められているとニュートン法などによって $|x_i^{(m)} - x_i| < 2^{-m}$ $(i = 1, \ldots, r)$ を満たす有理数列 $\{x_i^{(m)}\}$ を得ることができるので、今後論じるアルゴリズムで実数や実行列などを近似的に求めると述べている場合はその実数をいくらでも近づく有理数列が得られているとしてよい。QE アルゴリズムとしては CAD と呼ばれるものがよく用いられており、QEPCAD などのパッケージが知られている。(*[穴井 2003]*)

例 2.62. $A = \begin{pmatrix} a & c \\ c & b \end{pmatrix} \in \mathrm{M}_2(\mathbb{Q})$ を与えられた行列とする。一階論理の論理式 $\exists\lambda.\,[\exists x_1 \exists x_2.\,(ax_1 + cx_2 = \lambda x_1 \wedge cx_1 + bx_2 = \lambda x_2) \wedge \forall\lambda'.\,\{\exists y_1 \exists y_2.\,(ay_1 + cy_2 = \lambda' y_1 \wedge cy_1 + by_2 = \lambda' y_2) \rightarrow \lambda \leq \lambda'\}]$ の真偽を QE で判定すると真になり、λ として A の最小の固有値が近似的に算出される。λ より小さな有理数をとることで A の固有値の下界となる有理数を得ることができる。より一般に与えられた有理数成分対称行列に対してその固有値の下界となる有理数を得ることができる。

3 線形代数と二次形式

この章では方程式 1 の二次の項に対応する二次形式を扱うのに必要な線形代数及び二次形式の一般的事項について述べる。線形代数については [斉藤 1966] を、二次形式については、[CASS 1978] を参照している。

3.1 線形代数

定義 3.1.
体 F 上のベクトル空間とはアーベル群 V とスカラー倍と呼ばれる作用 $\cdot : F \times V \rightarrow V$ の組であって条件
1. $a \in F, \boldsymbol{u}, \boldsymbol{v} \in V$ について $a(\boldsymbol{u} + \boldsymbol{v}) = a\boldsymbol{u} + a\boldsymbol{v}$ がなりたつ
2. $a, b \in F, \boldsymbol{u} \in V$ について $(a + b)\boldsymbol{u} = a\boldsymbol{u} + b\boldsymbol{u}$ が成り立つ
3. $a, b \in F, \boldsymbol{u} \in V$ について $(ab)\boldsymbol{u} = a(b\boldsymbol{u})$ が成り立つ
4. $1\boldsymbol{u} = \boldsymbol{u}$ がなりたつを満たすものをいう。ベクトル空間の元をベクトルといい、V の加法単位元を零ベクトルといい $\mathbf{0}$ とかく。

定義 3.2.
V をベクトル空間とする。有限部分集合 $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\} \subseteq V$ が一次独立であるとは $\sum_{i=1}^n c_i \boldsymbol{v}_i = \mathbf{0}$ ならば $c_1 = \cdots = c_n = 0$ が成り立つことをいう.

定義 3.3.
V をベクトル空間とする. 有限部分集合 $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\} \subseteq V$ で生成されたベクトル空間を $\{\sum_{i=1}^n c_i \boldsymbol{v}_i \mid c_1, \ldots, c_n \in F\}$ で定め, $\langle \boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \rangle$ とかく.

定義 3.4.

V をベクトル空間とする. 有限部分集合 $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\} \subseteq V$ が V の基底であるとは $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ が一次独立でありかつ $V = \langle \boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \rangle$ が成り立つことをいう. 基底の元の個数を V の次元といい $\dim V$ とかく.

例 3.5.
F を体とする。F^m に通常の和とスカラー倍を定めたものは m 次元ベクトル空間になる。

定義 3.6.
V, W を体 F 上のベクトル空間とする。写像 $f : V \to W$ が
1. $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$ に対して $f(\boldsymbol{v}_1 + \boldsymbol{v}_2) = f(\boldsymbol{v}_1) + f(\boldsymbol{v}_2)$
2. $bmv \in V, a \in F$ に対して $f(a\boldsymbol{v}) = af(\boldsymbol{v})$
を満たすとき、f は線形写像であるという。V から W への線形写像全体の集合を $\mathrm{Hom}_F(V, W)$ と書く。

定義 3.7.
環 R の要素を長方形状にならべたもの $\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ldots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$ を R を成分に持つ行列と呼ぶ。縦に m 個、横に n 個の成分が並んでいる行列を $m \times n$ 行列という. 行列 A の縦 i 行目横 j 列目にある成分を行列 A の ij 成分といい,A_{ij} あるいは文脈上混乱が生じない場合は小文字を用いて a_{ij} と書く。
R を成分に持つ $m \times n$ 行列全体の集合を $R^{m \times n}$ と書く。$m \times m$ 行列を m 次正方行列といい、R を成分に持つ m 次正方行列全体の集合を $\mathrm{M}_m(R)$ と書く。
$A \in \mathrm{M}_m(R)$ について、a_{ii} を A の対角成分といい、a_{ij} $(i \neq j)$ を非対角成分という。また、ij 成分が a_{ij} である行列を (a_ij) のように書くことがある。
行列 $X \in R^{m \times n}$ について、この $m \times n$ を指して行列 X の形ということがある。
行列 $A \in R^{m \times n}$ に対してその転置 $A^\top$ を $(A^\top)_{ij} = A_{ji}$ によって定める。

定義 3.8.
m 行 n 列の零行列を $O_{m,n}$ と書く。文脈上行列の形が明らかな零行列は O と省略して書くことがある。
対角成分が 1 で非対角成分が 0 である行列を単位行列といい、$m \times m$ の単位行列を m 次の単位行列と呼び I_m とかく。

定義 3.9.
対角成分が $a_1, \ldots, a_m$ であるような対角行列を $\mathrm{diag}(a_1, \ldots, a_m)$ とかく。また $A_1 \in \mathrm{M}_{m_1}(R), A_2 \in \mathrm{M}_{m_2}(R), \ldots, A_k \in \mathrm{M}_{m_k}(R)$ を対角線上に並べて得られる $m_1 + m_2 + \cdots + m_k$ 次正方行列を $\mathrm{diag}(A_1, \ldots, A_k)$ とかく。(一般的なブロック行列の表記に従う)

定義 3.10.
行列の和、スカラー倍、積を以下のように定義する。
和:$A, B \in R^{m \times n}$ について $(A + B)_{ij} = A_{ij} + B_{ij}$
スカラー倍:$A \in R^{m \times n}, a \in R$ について $(aA)_{ij} = aa_{ij}$
積: $A \in R^{m \times l}.B \in R^{l \times n}$ について $(AB)_{ij} = \sum_{k=1}^{l} a_{ik} b_{lj}$

定義 3.11.
$R^{m \times n}$ は定義 *3.10* の和とスカラー倍で R 加群になる。また、$\mathrm{M}_m(R)$ は定義 *3.10* の和と積によって可換と

は限らない環となる. この環の零元は零行列 O で乗法単位元は単位行列 I_m である。M_mR の単元 (可逆行列とよばれる) 全体の集合を $\mathrm{GL}_m(R)$ と書き、R 上 m 次一般線形群とよぶ。$g \in \mathrm{GL}_m(R)$ の乗法逆元 g^{-1} を g の逆行列という。

定義 3.12.
・m 次正方行列 N がある自然数 k において $N^k = O$ となるとき N を冪零 (nilpotent) であるという。
・m 次正方行列 U において、$U - I_m$ が冪零であるとき、U を冪単 (unipotent) であるという。

注 3.13.
行列からなる集合 X に対し、$\{A^\top \mid A \in X\}$ のことを $X^\top$ と書いたり、可逆行列からなる集合 Y に対して $\{B^{-1} \mid B \in Y\}$ のことを Y^{-1} と書いたりなど、行列の集合に行列演算の記号を当てはめた記法をすることがある。ほかに例えば $XY = \{AB \mid A \in X, B \in Y\}, \mathrm{diag}(X_1, \ldots, X_k) = \{\mathrm{diag}(A_1, \ldots, A_k) \mid A_1 \in X_1, \ldots, A_k \in X_k\}$ といった書き方などをすることがある。

行列式について述べる。

定義 3.14.
対称群 S_m の元 σ について集合 $\{(x, y) \in \{1, \ldots, m\} \mid x < y \wedge \sigma(x) > \sigma(y)\}$ の要素の個数を σ 転倒数と呼ぶ.σ の転倒数が奇数である場合 σ は奇置換であるといい、偶数である場合は偶置換であるという。

定義 3.15.
対称群 S_m の元 σ に対して σ の符号 $\mathrm{sgn} : S_m \to \{1, -1\}$ を
$\mathrm{sgn}(\sigma) = \begin{cases} 1 \ (\sigma\text{が偶置換}) \\ -1 \ (\sigma\text{が奇置換}) \end{cases}$ によって定める。

定義 3.16.
m 次正方行列 $A \in \mathrm{M}_m(R)$ について,A の行列式 $\det A$ を
$\det A = \sum_{\sigma \in S_m} (\prod_{i=1}^m a_{i\sigma(i)})$
によって定める。

定義 3.17.
$\mathrm{GL}_m(R)$ の元のうち、行列式が 1 であるものの集合を $\mathrm{SL}_m(R)$ と書き、R 上の m 次特殊線形群と呼ぶ。実際、$\mathrm{SL}_m(R)$ は $\mathrm{GL}_m(R)$ の正規部分群である。

例 3.18.
F を体とすると $\mathrm{GL}_m(F) = \{g \mid \det g \neq 0\}$ である.$g \in \mathrm{GL}_m(F)$ である行列を正則行列と呼ぶ。

例 3.19.
$\mathrm{GL}_m(\mathbb{Z}) = \{g \mid \det g = \pm 1\}$ である。

G が $\mathrm{GL}_m(\mathbb{C})$ の部分群で、R を $\mathbb{C}$ の部分環とするとき、$G \cap \mathrm{GL}_m(R)$ のことを G_R とかく。

定義 3.20.
$A \in M_m(R)$ $(m \geq 2)$ とする。A の i 行目と j 列目をのぞいてできる $(m-1) \times (m-1)$ 行列を $A^{(i,j)}$ と書く。$(-1)^{i+j} \det A^{(i,j)}$ を A の (i, j) 余因子といい, $\tilde{A}_{(i,j)}$ あるいは小文字を用いて $\tilde{a}_{(i,j)}$ で表す.ij 成分が $\tilde{a}_{ji}$

であるような $m \times m$ 行列 *(i と j が逆になっていることに注意)* を A の余因子行列といい $\tilde{A}$ と書く。

余因子を用いると行列式を表す。定義 3.16 とは別の式を得ることができる。

命題 3.21.
$A \in M_m(R)$ として、任意の $i, j \in \{1, \ldots, m\}$ を固定する。このとき $\det A = \sum_{k=1}^{m} a_{ik}\tilde{a}_{(i,k)} = \sum_{k=1}^{m} a_{kj}\tilde{a}_{(k,j)}$ がなりたつ。

命題 3.21 により余因子行列が逆行列の計算に用いることができることがわかる。

命題 3.22.
$A \in M_m(R)$ とする。このとき、$A\tilde{A} = \tilde{A}A = \det A I_m$ が成り立つ。特に $\det A \in R^{\times}$ であるとき、$A^{-1} = (\det A)^{-1}\tilde{A}$ である。

定義 3.23.
F を体とする。$A \in \mathrm{M}_m(F), \lambda \in F, \boldsymbol{x} \in F^m \setminus \{\boldsymbol{0}\}$ が等式 $A\boldsymbol{x} = \lambda\boldsymbol{x}$ をみたすとき、λ を行列 A の固有値といい、$\boldsymbol{x}$ を固有値 λ に対応する固有ベクトルという。

命題 3.24.
F を体とする。$A \in \mathrm{M}_m(F)$ の固有値は λ は方程式 $\det(A - \lambda I_m) = 0$ の解である。この方程式を固有方程式という。

$\mathrm{M}_m(\mathbb{C})$ の冪零行列と冪単行列の固有値について、以下が知られている。

命題 3.25.
・$N \in \mathrm{M}_m(\mathbb{C})$ が冪零 $\Leftrightarrow$ N の固有値がすべて 0
・$U \in \mathrm{M}_m(\mathbb{C})$ が冪単 $\Leftrightarrow$ U の固有値がすべて 1

定義 3.26.
$\mathbb{U} = \{U \in \mathrm{GL}_m(\mathbb{C}) \mid U \text{ は上三角行列で対角成分がすべて } 1\}$
と定める。明らかに $\mathbb{U}$ の要素はすべて冪単である。

行列の指数関数と対数関数について述べる。

定義 3.27.
実行列 $A \in \mathrm{M}_m(\mathbb{R})$ の行列ノルム $||A||_{\mathrm{mat}}$ を
$||A||_{\mathrm{mat}} = \sqrt{\sum_{1 \le i,j, \le m} a_{ij}}$
で定める.*(行列を $m \times m$ 次元ベクトルとみた場合のユークリッドノルムと同義である)*

定義 3.28.
$A \in \mathrm{M}_m(\mathbb{R})$ とする. 行列の指数関数 $\exp(A)$ を
$\exp(A) = \sum_{n=0}^{\infty} \frac{1}{n!} A^n$
で定める. この級数は任意の $A \in \mathrm{M}_m(\mathbb{R})$ で収束する. 特に A が冪零の場合は有限和になる.

定義 3.29.
級数 $\log(A) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} (A - I_m)^n$

が収束する $A \in \mathrm{M}_m(\mathbb{R})$ に対して, これを行列の対数関数とよび $\log(A)$ と書く.
特に A が冪単の場合は有限和になる.

最後に行列のスペクトルノルムについて述べる。

定義 3.30.
$A \in \mathrm{M}_m(\mathbb{R})$ に対して A のスペクトルノルムを $||A|| = \sup_{||\boldsymbol{x}||\leq 1}||A\boldsymbol{x}||$ によって定める。

スペクトルノルムの計算は固有値の計算を行うことでできることが以下の命題よりわかる。

命題 3.31.
$A \in \mathrm{M}_m(\mathbb{R})$,$A^\top A$ の固有値のうち最大のものを $\lambda_{\max}$ とする。このとき、$||A|| = \sqrt{\lambda_{\max}}$ が成り立つ。

3.2 二次形式

定義 3.32.
R を環とする。対称行列 $A \in \mathrm{M}_m(R)$ を用いて $Q(\boldsymbol{x}) = \boldsymbol{x}^\top A\boldsymbol{x}$ と表せる関数 $Q : R^m \to R$ を R 上の二次形式と呼ぶ。A のことを係数行列という。$\det A$ のことを $d(Q)$ とかく。$d(Q) \neq 0$ であるとき Q は regular であるといい、$d(Q) = 0$ であるとき Q は singular であるという。

定義 3.33.
R を環,$S \subseteq R$ を部分環とする.R 上の二次形式 $Q_1.Q_2$ がある $T \in \mathrm{GL}_m(S)$ によって $Q_2(\boldsymbol{x}) = Q_1(T\boldsymbol{x})$ と表せるとき、Q_1, Q_2 は S-equivalent であるという。

命題 3.34.
$\mathbb{C}$ 上の二次形式 Q_1, Q_2 が $\mathbb{Z}$-equivalent ならば $d(Q_1) = d(Q_2)$ である

【証明】
Q_1, Q_2 が $\mathbb{Z}$-equivalent ならば $T \in \mathrm{GL}_m(Z)$ によって $Q_2(\boldsymbol{x}) = Q_1(T\boldsymbol{x})$ と書ける。$Q_1(\boldsymbol{x}) = \boldsymbol{x}^\top A\boldsymbol{x}$ とすると $Q_2(\boldsymbol{x}) = \boldsymbol{x}^\top T^\top AT\boldsymbol{x}$ であるが、$\det T = \pm 1$ なので、$\det A = \det T^\top AT$ である。

定義 3.35.
Q を環 R 上の二次形式とする。$Q(\boldsymbol{x}) = 0$ となる $\boldsymbol{x} \neq \boldsymbol{0}$ が存在する場合、Q は isotropic であるという。isotropic でない場合、Q は anisotropic であるという。

$\mathbb{R}$ 上の二次形式 $Q(\boldsymbol{x}) = \boldsymbol{x}^\top A\boldsymbol{x}$ には定値性の概念がある。

定義 3.36.
・$\mathbb{R}$ 上の二次形式 $Q(\boldsymbol{x}) = \boldsymbol{x}^\top A\boldsymbol{x}$ が半正定値であるとは、任意の $\boldsymbol{x} \neq \boldsymbol{0}$ について $Q(\boldsymbol{x}) \geq 0$ がなりたつことをいう。これは A の固有値がすべて非負であることと同値である。
・$\mathbb{R}$ 上の二次形式 $Q(\boldsymbol{x}) = \boldsymbol{x}^\top A\boldsymbol{x}$ が正定値であるとは、任意の $\boldsymbol{x} \neq \boldsymbol{0}$ について $Q(\boldsymbol{x}) > 0$ がなりたつことをいう。これは A の固有値がすべて正であることと同値である。
・$\mathbb{R}$ 上の二次形式 $Q(\boldsymbol{x}) = \boldsymbol{x}^\top A\boldsymbol{x}$ が半負定値であるとは、任意の $\boldsymbol{x} \neq \boldsymbol{0}$ について $Q(\boldsymbol{x}) \leq 0$ がなりたつことをいう。これは A の固有値がすべて 0 以下であることと同値である。

・$\mathbb{R}$ 上の二次形式 $Q(\boldsymbol{x}) = \boldsymbol{x}^\top A\boldsymbol{x}$ が負定値であるとは、任意の $\boldsymbol{x} \neq \boldsymbol{0}$ について $Q(\boldsymbol{x}) < 0$ がなりたつことをいう、これは A の固有値がすべて負であることと同値である。
正定値、あるいは負定値な二次形式は明らかに regular である。半正定値であるか半負定値である二次形式を definite であるといい。definite でないことを indefinite であるという。

二次形式の isotropic 性を判定する上で重要な Hilbert 記号についても述べる.

定義 3.37.
F を体とし,$a, b \in F^\times$ とする。Hilbert 記号 $(a, b)_F$ を
$$(a,b)_F = \begin{cases} 1\ (ax^2 + by^2 - z^2 \text{が} F \text{上isotropic}) \\ -1\ (\text{otherwise}) \end{cases}$$
で定める。

以下は Hilbert 記号を計算するうえでの基本的な公式である。

命題 3.38. (*[雪江 2013]* 命題 9.2.2)

(1) $(a, b)_F = (b, a)_F$
(2) $(a_1a_2, b)_F = (a_1, b)_F(a_2, b)_F$

定義 3.39.
$Q(\boldsymbol{x}) = \boldsymbol{x}^\top A\boldsymbol{x}$ を $\mathbb{Q}$ 上の二次形式とする。ベクトル空間 $\mathbb{Q}^m$ の基底 $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ が
$\boldsymbol{b}_i^\top A\boldsymbol{b}_j = 0\ (i \neq j)$
を満たすときこの基底は Q 上 normal であるという。

任意の二次形式 Q について,Q 上 normal な基底は必ず存在する。このことを示すために直交補空間の概念を導入する。

定義 3.40.
$Q(\boldsymbol{x}) = \boldsymbol{x}^\top A\boldsymbol{x}$ を $\mathbb{Q}$ 上の二次形式,$V \subseteq \mathbb{Q}^m$ を線形部分空間とする.V の直交補空間 $V^\perp$ を
$V^\perp = \{\boldsymbol{u} \in \mathbb{Q}^m \mid \forall \boldsymbol{v} \in V.\, \boldsymbol{v}^\top A\boldsymbol{u} = 0\}$
によって定める。$V^\perp$ もまた $\mathbb{Q}^m$ の線形部分空間である。

定義 3.41.
$Q(\boldsymbol{x}) = \boldsymbol{x}^\top A\boldsymbol{x}$ を $\mathbb{Q}$ 上の二次形式、$V \subseteq \mathbb{Q}^m$ を線形部分空間とする。部分空間 V が二次形式 Q について regular であるとは V の基底 $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r$ について、二次形式 $\sum_{1 \leq i,j \leq r} (\boldsymbol{v}_i^\top A\boldsymbol{v}_j)x_ix_j$ が $\mathbb{Q}$ 上 regular であることをいう。

命題 3.42. (*[CASS 1978]* Chapter2 LEMMA 1.3)
$Q(\boldsymbol{x}) = \boldsymbol{x}^\top A\boldsymbol{x}$ を $\mathbb{Q}$ 上 m 変数二次形式,$V \subseteq \mathbb{Q}^m$ を Q について regular な線形部分空間とする。このとき、$\mathbb{Q}^m$ は V と $V^\perp$ の直和で表すことができる。

命題 3.43. (*[CASS 1978]* Chapter2 LEMMA 1.4)
$\mathbb{Q}$ 上の二次形式 $Q(\boldsymbol{x}) = \boldsymbol{x}^\top A\boldsymbol{x}$ には必ず Q 上 normal な $\mathbb{Q}^m$ の基底が存在する。

【証明】$Q(\boldsymbol{x})$ が恒等的に 0 であればどんな基底も normal である。そうでないなら $Q(\boldsymbol{b}_1) \neq 0$ となる $\boldsymbol{b}_1$ が存在し、$V = \langle \boldsymbol{b}_1 \rangle$ とすると、$U = V \oplus V^{\perp}$ と書ける。$V^{\perp}$ の基底 $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{m-1}$ を求め二次形式 $\sum_{1 \leq i,j \leq m-1} (\boldsymbol{v}_i^{\top} A \boldsymbol{v}_j) x_i x_j$ に対して帰納的に同じ操作を繰り返せば normal な基底 $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ を得ることができる。 □

さらに regular な二次形式については以下が成り立つ。

命題 3.44. (*[CASS 1978]* Chapter2 LEMMA 1.5)
$Q(\boldsymbol{x}) = \boldsymbol{x}^{\top} A \boldsymbol{x}$ を $\mathbb{Q}$ 上の二次形式、$\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ を Q 上 normal な基底とすると、Q が regular であることと各 j について $\boldsymbol{b}_j^{\top} A \boldsymbol{b}_j \neq 0$ であることが同値である。

以上の性質から与えられた $\mathbb{Q}$ 上の regular な二次形式 Q に対してそれと $\mathbb{Q}$-equivalent な $\mathbb{Q}$ 係数対角二次形式を得ることができることがわかる。

命題 3.45.
$Q(\boldsymbol{x}) = \boldsymbol{x}^{\top} A \boldsymbol{x}$ を regular な $\mathbb{Q}$ 上の二次形式として $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ を Q 上 normal な基底とする。このとき $Q'(\boldsymbol{x}) = Q(x_1 \boldsymbol{b}_1 + \cdots + x_m \boldsymbol{b}_m) = \sum_{i,j} \phi(\boldsymbol{b}_i, \boldsymbol{b}_j) x_i x_j$ は対角二次形式であってかつ Q と $\mathbb{Q}$-equivalent である。

命題 3.45 で得た二次形式 Q' を適切に整数倍して分母を払うことで以下の系を得る。

系 3.46.
$Q(\boldsymbol{x}) = \boldsymbol{x}^{\top} A \boldsymbol{x}$ を regular な $\mathbb{Q}$ 上の二次形式とする。このとき、$Q''(\boldsymbol{x}) = \sum_{i=1}^{m} a_i x_i^2 \ (a_i \in \mathbb{Z})$ であって「Q が $\mathbb{Q}$ 上 isotropic $\Leftrightarrow$ Q'' が $\mathbb{Q}$ 上 isotropic」を満たすような対角二次形式 Q'' が存在する。

例 3.47.
$Q(\boldsymbol{x}) = \boldsymbol{x}^{\top} A \boldsymbol{x}$,$A = \begin{pmatrix} 1 & 3 & -3 \\ 3 & 2 & 1 \\ -3 & 1 & -1 \end{pmatrix}$ を考える。$Q((1,0,0)^{\top}) \neq 0$ であり、$\{\boldsymbol{v} \in \mathbb{Q}^3 \mid \forall t \ \in^m athbbQ.\, t(1,0,0,)A\boldsymbol{v} = 0\} = \{\boldsymbol{v} \mid (1,0,0,)A\boldsymbol{v} = 0\}$ の基底は $\boldsymbol{b}_2 = (-3,1,0)^{\top}, \boldsymbol{b}_3 = (3,0,1)^{\top}$ である。2 変数の二次形式 $g(u_1, u_2)$ を $g(u_1, u_2) = Q(u_1 \boldsymbol{b}_2 + u_2 \boldsymbol{b}_3)$ で定めると $g(u_1, u_2) = (u_1, u_2) \begin{pmatrix} -7 & 5 \\ 5 & -10 \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}$ であり $g(1,0) \neq 0$ である。$\{\boldsymbol{w} \in \mathbb{Q}^2 \mid \forall t \in \mathbb{Q}.\, t(1,0) \begin{pmatrix} -7 & 5 \\ 5 & -10 \end{pmatrix} \boldsymbol{w} = 0\}$ の基底は $(1, \frac{7}{5})$ である.$1(-3,1,0) + \frac{7}{5}(3,0,1) = (\frac{6}{5}, 1, \frac{7}{5})$ だから $\mathbb{Q}^3$ の基底 $(1,0,0)^{\top}, (-3,1,0)^{\top}, (6,5,7)^{\top}$ をとると $(1,0,0)A(-3,1,0)^{\top} = (1,0,0)A(6,5,7)^{\top} = (-3,1,0)A(6,5,7) = 0$ であり、$Q'(u_1, u_2, u_3) = Q(u_1(1,0,0)^{\top} + u_2(-3,1,0)^{\top} + u_3(6,5,7)^{\top}) = u_1^2 + 29u_2^2 + 35u_3^2$ と対角二次形式なる。そして、Q が $\mathbb{Q}$ 上 isotropic $\Leftrightarrow$ Q'' が $\mathbb{Q}$ 上 isotropic

4　整数行列による二次形式の変換可能性判定アルゴリズム

4.1　Minkowski-reduced form と Siegel-domain

命題 4.1. (*[CASS 1978]* chapter9 Corollary1)
Q を $d(Q)=d$ である regular な m 変数二次形式とする。このときある primitive な $\boldsymbol{a}\in\mathbb{Z}^m$ が存在して、$|Q(\boldsymbol{a})|\leq(\frac{4}{3})^{\frac{m-1}{2}}|d|^{\frac{1}{m}}$ がなりたつ。

Q を $d(Q)=d$ である regular な m 変数二次形式とすると、命題 4.1 より $|Q(\mathbf{a})|\leq(\frac{4}{3})^{\frac{m-1}{2}}|d|^{\frac{1}{m}}$ がなりたつ primitive な $\mathbf{a}\in\mathbb{Z}^m$ が存在する。このとき、$\boldsymbol{a}=\boldsymbol{a}_1,\boldsymbol{a}_2,\ldots,\mathbf{a}_m$ と $\mathbb{Z}^m$ の基底を得ることができ、$A=(\boldsymbol{a}_1,\boldsymbol{a}_2,\ldots,\mathbf{a}_m)\in\mathrm{GL}_m(\mathbb{Z})$ である。
$Q'(\boldsymbol{x})=Q(A\boldsymbol{x})=\sum_{i,j}f'_{ij}x_ix_j$ とおくと,$f'_{11}=Q(\boldsymbol{a})$ である。$Q(\boldsymbol{a})=f'_{11}=\alpha$ とおくと、平方完成により、
$\alpha Q'(\boldsymbol{x})=(\alpha x_1+f'_{12}\cdots+f'_{1m}x_m)^2+g(x_2,\ldots,x_m)$
(ただし g は $d(g)=\alpha^{m-2}d(Q)$ なる $m-1$ 変数二次形式)
とかける。加えて、代入変換
$$\begin{cases} y_1=x_1+u_2x_2+\cdots+u_mx_m\\ y_2=x_2\\ \vdots\\ y_m=x_m\end{cases}$$
を考えると、$|f'_1j|\leq\alpha$ $(j=2,\ldots,m)$ と仮定してよい。まとめると、$d(Q)=d$ であるような Q は、
$\frac{1}{M}((Mx_1+f'_{12}\cdots+f'_{1m}x_m)^2+g(x_2,\ldots,x_m))$ (ただし $|M|\leq(\frac{4}{3})^{\frac{m-1}{2}}|d|^{\frac{1}{m}}$, $d(g)=M^{m-2}d$, $|f'_{1j}|\leq|M|$ $(j=2,\ldots,m)$) の形の二次形式と $\mathbb{Z}$-equivalent である。

定義 4.2.
正定値な二次形式 $Q(\mathbf{x})$ が Minkowski-reduced であるとは、$j=1,\ldots,m$ に対して、$Q(\mathbf{e}_j)\leq Q(\mathbf{e}^*_j)$ が成り立つことをいう。但し、$\mathbf{e}^*_j$ は $\boldsymbol{e}_1,\ldots,\boldsymbol{e}_{j-1},\boldsymbol{e}^*_j$ からベクトルを追加して $\mathbb{Z}^m$ の基底が得られるようなベクトルの範囲を動くとする。

注 4.3.
正定値な二次形式 $Q(\boldsymbol{x})$ が Minkowski-reduced であることは、$\mathrm{g.c.d}(b_j,b_{j+1},\ldots,b_m)=1$ なる $\boldsymbol{b}=(b_1,\ldots,b_m)^{\mathrm{T}}$ に対して $Q(\boldsymbol{e}_j)\leq Q(\boldsymbol{b})$ がなりたつことと同値である。

命題 4.4. (*[CASS 1978]* chapter12 Theorem1.1) Q を正定値な二次形式とする。Q はすくなくとも 1 つの Minkowski-reduced な二次形式と $\mathbb{Z}$-equivalent である。しかも、Q と $\mathbb{Z}$-equivalent な Minkowski-reduced 二次形式は高々有限個。

(Proof sketch) 以下のようにして $\mathbb{Z}^m$ の基底 $\boldsymbol{b}_1,\ldots,\boldsymbol{b}_m$ を帰納的に得ることができる。

1 $\boldsymbol{b}_1\in\mathbb{Z}^m$ を $Q(\boldsymbol{b}^*)=\min_{b^*_1}\{Q(\boldsymbol{b}^*_1)\,|\,\boldsymbol{b}^*_1:\text{primitive}\}$ となるような $\boldsymbol{b}^*$ のなかから一つとる。
2 $j=2,\ldots,m$ について、$\boldsymbol{b}_j\in\mathbb{Z}^m$ を $Q(\boldsymbol{b}^*)=\min_{b^*_j}\{Q(\boldsymbol{b}^*_j)\,|\,\boldsymbol{b}_1,\ldots,\boldsymbol{b}_{j-1},\boldsymbol{b}^*_j$ からベクトルを追加して $\mathbb{Z}^m$ の基底を得ることができる $\}$ となるような $\boldsymbol{b}^*$ のなかから一つとる。

上記の構成から $Q'(y_1\ldots,y_m)=Q(y_1\boldsymbol{b}_1,\ldots,y_m\boldsymbol{b}_m)$ は Minkowski-reduced で Q と $\mathbb{Z}$-equivalent.Q が正

定値なとき任意の正の数 M について $\{m \in \mathbb{Z}^m \,|\, Q(m) \leq M\}$ は有限集合になることに注意すれば、基底 $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ の取り方は高々有限パターン。

次は一定の範囲の二次形式を集めた集合である Siegel-domain を導入し、二次形式の変数の数のみに依存する十分な広さの Siegel-domain をとればすべての Minkowski-reduced な二次形式を含むことができることを述べる。

定義 4.5.
$\delta, \eta > 0$ とする。Siegel-domain $\mathfrak{S}(\delta, \eta)$ を、以下のような二次形式の集合として定める。
$\mathfrak{S}(\delta, \eta) = \{Q(\boldsymbol{x}) \,|\, Q(\boldsymbol{x}) = h_1(x_1 + c_{12}x_2 + \cdots + c_{1n}x_)^2 + h_2(x_2 + c_{23}x_3 + \cdots + c_{2n}x_n)^2 + \cdots + h_n x_n^2,\ 0 < h_j \leq \delta h_{j+1}\,(1 \leq j < n)\ |c_{ij}| \leq \eta\,(1 \leq i < j \leq n)\}$
また、Siegel-domain $\mathfrak{S}(\delta, \eta)$ に属する二次形式に対応する行列の集合を $\mathfrak{Q}_{\delta,\eta}$ とかく。すなわち、
$\mathfrak{Q}_{\delta,\eta} = \{A \in \mathrm{M}_m(\mathbb{R}) \mid \boldsymbol{x}^\top A \boldsymbol{x} \in \mathfrak{S}(\delta, \eta)\}$
である。

定義 4.6. (i) j にのみ依存する定数 $C_4(j)$ $(j = 1, \ldots, m)$ を漸化式
$$\begin{cases} C_4(1) = 1 \\ C_4(j) = (1 + \dfrac{1}{2}\displaystyle\sum_{i<j} \sqrt{C_4(i)})^2 \end{cases}$$
によって定める。
(ii) m にのみ依存する定数 $C_5(m)$ を $\frac{(\frac{4}{3})^{\frac{m(m-1)}{2}}}{(\min_k(C_4(k)))^{m-1}}$ によって定める。
(iii) m にのみ依存する定数 $C_6(m)$ を $(\max_k(C_4(k)))C_5(m)$ によって定める。

定義 4.7. j にのみ依存する定数 H_j $(j = 1, \ldots, m)$ を漸化式
$$\begin{cases} H_1 = \dfrac{1}{2} \\ H_j = \dfrac{1}{2}C_6(m) + \displaystyle\sum_{i<j} C_6(m)^{j-i} H_i^2 \end{cases}$$
によって定める。

以下が成り立つ

命題 4.8. (*[CASS 1978]* chapter12 lemma1.3)
どのような Minkowski-reduced な二次形式も $\mathfrak{S}(\delta_m, \eta_m)$ に入るような、変数の数 m にのみ依存する正の数 δ_m, η_m が存在する。それは具体的に $\delta_m = C_6(m), \eta_m = \max_{1 \leq j \leq m} H_j$ で求められる。

4.2 正定値な二次形式の有界性

定義 4.9.
正定値な二次形式 Q の successsive-minima を以下の条件を満たす正の数の列 $M_{Q,1} \leq M_{Q,2} \leq \cdots \leq M_{Q,m}$ として定める。

(i) 集合 $\{\mathbf{m} \in \mathbb{Z}^m \mid Q(\mathbf{m}) \leq M_{Q,j}\}$ が生成する実ベクトル空間の次元が j 以上
(ii) 集合 $\{\mathbf{m} \in \mathbb{Z}^m \mid Q(\mathbf{m}) < M_{Q,j}\}$ が生成する実ベクトル空間の次元が j 未満
あきらかに $M_{Q,1} = \min_{\mathbf{m} \in \mathbb{Z}^m \setminus \{\mathbf{o}\}} Q(\mathbf{m})$ であり、$M_{Q,1} \leq M_{Q,2} \leq \cdots \leq M_{Q,m}$ は一意に定まる。

注 4.10. Q を正定値二次形式、$M_{Q,1} \leq M_{Q,2} \leq \cdots \leq M_{Q,m}$ をその successsive-minima とすると、$Q(\boldsymbol{m}_j) = M_{Q,j}$ を満たし,$\mathbb{R}$ 上一次独立なベクトル $\boldsymbol{m}_1, \ldots, \boldsymbol{m}_m \in \mathbb{Z}^m$ がとれる。*(*取り方は一意とは限らない*)*
Q が整数係数であれば、$M_{Q,j}$ は正の整数である。

定義 4.11. 定数 C_{10}, C_{11} を、
$C_{10} = 1 + \eta_m^2 \sum_{j=1}^{m} \delta_m^j$
$C_{11} = \sqrt{\max\{\frac{1}{4}(1 + \delta_m + \cdots + \delta_m^{m-1}), \delta_m^{m-1} C_{10}\}}$
で定める。

注 4.12. $C_4(j), C_5(m), C_6(m), H_j, C10, C11, C12$ のノーテーションは *[CASS 1978]* の記述にしたがってつけているものである。

命題 4.13. $Q(\boldsymbol{x}) = \sum_{i=1}^{m} h_i(x_i + c_{i,i+1}x_{i+1} + \cdots + c_{i,m}x_m)^2$ を Minkowski-reduced な正定値二次形式として、その successsive-minima を $M_{Q,1} \leq M_{Q,2} \leq \cdots \leq M_{Q,m}$ とする。$Q(\boldsymbol{m}_j) = M_{Q,j}$ を満たし、$\mathbb{R}$ 上一次独立なベクトル $\boldsymbol{m}_1, \ldots, \boldsymbol{m}_m \in \mathbb{Z}^m$ をとり、$\boldsymbol{m}_j$ の第 i 成分を $m_{j,i}$ のように書く。j を固定して
$\mu_i^{(j)} = m_{j,i} + c_{i,i+1}m_{j,i+1} + \cdots + c_{i.m}m_{j,m}$ とおくと、
$|\mu_i^{(j)}| \leq C_{11}$ が成り立つ。

命題 4.14. (*[CASS 1978]* chapter12 lemma 4.2)
数列 $\nu_1, \ldots, \nu_m$ を漸化式
$$\begin{cases} \nu_1 = C_{11} \\ \nu_j = C_{11} + \sum_{i<j} \eta\nu_i \end{cases}$$
によって定め, $C_{12} = \max_{1 \leq j \leq} \nu_i$ とおく. このとき、
$|m_{j,i}| \leq C_{12}$ が成り立つ。

(Proof sketch) 命題 4.14 の結果と $\mu^{(j)_i}$ の定義を用いる。

系 4.15.
命題 *4.14* の結果を用いて、2 つの Minkowski-reduced な正定値二次形式が $\mathbb{Z}$-equivalent かどうかを判定するための基底変換行列の候補を有限個に絞ることができる。

アルゴリズム 4.16. (*[CASS 1978]* chapter12 theorem 1.4)
以下の条件を満たす、m, δ, η にのみ依存する定数 $C(m, \delta, \eta)$ が存在する。そしてそれは以下の手順で計算することができる。
【条件】$Q(\boldsymbol{x}), Q(T\boldsymbol{x}) \in \mathfrak{S}(\delta, \eta),\ T \in \mathrm{GL}_m(\mathbb{Z})$ ならば T の成分の絶対値は $C(m, \delta, \eta)$ 以下

【手順】

二つの基底 $(\boldsymbol{b}_1,\ldots,\boldsymbol{b}_m),(\boldsymbol{b}'_1,\ldots,\boldsymbol{b}'_m)$ について、$Q(x_1\boldsymbol{b}_1+\cdots+x_m\boldsymbol{b}_m)=Q(x_1\boldsymbol{b}'_1+\cdots+x_m\boldsymbol{b}'_m)$ とする.Q の successsive-minima に対応する一次独立なベクトル $\boldsymbol{m}_1,\ldots,\boldsymbol{m}_m\in\mathbb{Z}^m$ をとると、
$\boldsymbol{m}_j=\sum_i m_{j,i}\boldsymbol{b}_i=\sum_i m'_{j,i}\boldsymbol{b}'_i$ $(m'_{j,i}\in\mathbb{Z})$ とかけて、行列の計算により、$\boldsymbol{b}_j=\sum_{i=1}^m t_{ij}\boldsymbol{b}'_i$ が得られる. ところが, $|m_{j,i}|,|m'_{j,i}|\le C_{12}$ であることからこの t_{ij} の絶対値は C_{12} を使って計算される m,δ,η のみに依存する定数によって上から抑えられる。実際、
$\begin{pmatrix} m_{1,1} & \cdots & m_{1,m}\\ \vdots & \vdots & \vdots\\ m_{m,1} & \cdots & m_{m,m}\end{pmatrix}\begin{pmatrix}\boldsymbol{b}_1\\ \vdots\\ \boldsymbol{b}_m\end{pmatrix}=\begin{pmatrix} m'_{1,1} & \cdots & m'_{1,m}\\ \vdots & \vdots & \vdots\\ m'_{m,1} & \cdots & m'_{m,m}\end{pmatrix}\begin{pmatrix}\boldsymbol{b}'_1\\ \vdots\\ \boldsymbol{b}'_m\end{pmatrix}$ であり、$\boldsymbol{b}_j=\sum_{i=1}^m t_{ij}\boldsymbol{b}'_j$ なので $|t_{ij}|$ も C_{12} を使って計算される値で上から抑えられる。

4.3 Hermite-reduced form

定義 4.17.
Q を regular な二次形式とする。正定値二次形式からなる集合 Φ_Q を
$\Phi_Q=\{Q'(\boldsymbol{x})=L_1(\boldsymbol{x})^2+\cdots+L_r(\boldsymbol{x})^2+L_{r+1}(\boldsymbol{x})^2+\cdots+L_{r+s}(\boldsymbol{x})^2\,|\,r+s=m\text{で各}L_i\text{は1次斉次式},Q(\boldsymbol{x})=L_1(\boldsymbol{x})^2+\cdots+L_r(\boldsymbol{x})^2-L_{r+1}(\boldsymbol{x})^2-\cdots-L_{r+s}(\boldsymbol{x})^2\}$ で定める。Φ_Q の要素 Q' を Q の Hermite-majorant と呼ぶ。

定義 4.18.
regular な二次形式 Q が Hermite-reduced であるとは、Φ_Q に少なくともひとつ Minkowski-reduced な二次形式を持つことをいう。

命題 4.19. (*[CASS 1978]* chapter13 lemma 2.1)
Q を regular な二次形式とすると Q はある Hermite-reduced な二次形式と $\mathbb{Z}$-equivalent。

(Proof sketch) $Q'\in\Phi_Q$ とするとある $T\in\mathrm{GL}_m(\mathbb{Z})$ があって $Q'(T\boldsymbol{x})$ が Minkowski-reduced になるが、$Q'(T\boldsymbol{x})$ は $Q(T\boldsymbol{x})$ の Hermite-majorant である。 □

補題 4.20. (*[CASS 1978]* chapter13 lemma 11.1)
$f(\boldsymbol{x})=\boldsymbol{x}^\top F\boldsymbol{x}$ を regular で indefinite な二次形式とし、$g(\boldsymbol{x})=\boldsymbol{x}^\top G\boldsymbol{x}$ を f の Hermite-majorant とする。このとき、$(FG^{-1})^2=I_m$ となる。

$m\times m$ 行列 $J=(j_{ik})$ を
$$j_{ik}=\begin{cases}1 & \text{if } i+k=m+1\\ 0 & \text{otherwise}\end{cases}$$
で定める。線形変換 $\boldsymbol{x}\mapsto J\boldsymbol{x}$ は変数 $x_1,\ldots,x_m$ の順番を逆にするものであり、したがって $J^{-1}=J$ である。

補題 4.21. (*[CASS 1978]* chapter13 lemma 11.2)
与えられた正の数 η に対して、m と η にのみ依存する正の数 η_1 であって以下の条件を満たすものを算出することができる。
【条件】regular で正定値な二次形式 $g(\boldsymbol{x})=\boldsymbol{x}^\top G\boldsymbol{x}$ が Siegel domain $\mathfrak{S}(\delta,\eta)$ に属しているならば二次形式 $\boldsymbol{x}^\top JG^{-1}J\boldsymbol{x}$ は $\mathfrak{S}(\delta,\eta_1)$ に属する。

(Proof sketch) $g \in \mathfrak{S}(\delta, \eta)$ の条件から

$$C = \begin{pmatrix} 1 & c_{12} & c_{13} & \cdots & c_{1m} \\ 0 & 1 & c_{23} & \cdots & c_{2m} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

$H = \mathrm{diag}(h_1, \ldots, h_m)$

$(0 < h_j \leq \delta h_{j+1},\ |c_{ij}| \leq \eta)$

なる行列 C, H を用いて $G = C^\top HC$ と表すことができる。ここで、$H_1 = JH^{-1}J,\ C_1 = J(C^\top)^{-1}J$ とおくと、$JG^{-1}J = C_1^\top H_1 C_1$ である.$H_1 = \mathrm{diag}(\frac{1}{h_m}, \ldots, \frac{1}{h_1})$ であり、$0 < \frac{1}{h_{j+1}} \leq \delta \frac{1}{h_{j+}}$ であることは明らか. また,C の成分の絶対値の bound である η を用いて C_1 の成分の絶対値の bound η_1 を算出することができる。

補題 4.22. (*[CASS 1978]* chapter13 lemma 11.3)
regular で正定値な二次形式 $g(\boldsymbol{x}) = \boldsymbol{x}^\top G\boldsymbol{x}$ が Siegel domain $\mathfrak{S}(\delta, \eta)$ に属しているとする。また、$T \in M_m(\mathbb{Z})$ を正則な行列とし、二次形式 $(T\boldsymbol{x})^\top G(T\boldsymbol{x})$ の successsive-minima を $M_1 \leq M_2 \leq \cdots \leq M_m$, 対応するベクトルを $\boldsymbol{m}_1, \boldsymbol{m}_2, \ldots \leq \boldsymbol{m}_m \in \mathbb{Z}^m$ とする. このとき、$T\boldsymbol{m}_j$ の成分の絶対値は $m, \delta, \eta, \mathrm{det}T$ にのみに依存する定数 $\beta(m, \delta, \eta, \mathrm{det}T)$ によって上から抑えられる。

(Proof sketch) $M_1 \leq M_2 \leq \cdots \leq M_m$ が $g(\boldsymbol{x})$ の successsive-minima でもあり,$T\boldsymbol{m}_1, T\boldsymbol{m}_2, \ldots \leq T\boldsymbol{m}_m \in \mathbb{Z}^m$ が対応するベクトルなので、4.14 を用いて $\beta(m, \delta, \eta, \mathrm{det}T)$ を計算することができる。

系 4.23. *([CASS 1978]* chater13 COROLLARY11.1 *)*

$d \neq 0$ を固定する。$d(Q) = d$ となる Hermite-reduced な二次形式は有限個。

(Proof sketch) $f(\boldsymbol{x}) = \boldsymbol{x}^\top F\boldsymbol{x}$ を $d(f) = d$ を満たす Hermite − reduced な二次形式とし,$g(\boldsymbol{x}) = \boldsymbol{x}^\top G\boldsymbol{x}$ を f の Hermite − majorant で Minkowski − reduced であるとする. 補題 4.20 より,$G = FG^{-1}F$ であり,$T = JF$ とおくと $G = T^\top(JG^{-1}J)T$ である. g は Minkowski − reduced であることから, 命題 4.8 の Siegel domain $\mathfrak{S}_{\delta_m, \eta_m}$ に属している. そのため, 補題 4.21 で算出される η_1 について二次形式 $\boldsymbol{x}^\top JG^{-1}J\boldsymbol{x}$ は $\mathfrak{S}(\delta_m, \eta_1)$ に属する.$T\boldsymbol{m}_j, \boldsymbol{m}_j$ の成分の絶対値がともに有界なので,$T = JF$ の成分の絶対値も有界. とくに F の成分の絶対値も有界である.

4.4 $\mathbb{Z}$-equivalent 性判定アルゴリズム

アルゴリズム 4.24. 与えられた $d \neq 0$ に対して、$d(Q) = d$ となる Hermite-reduced な二次形式をすべて含む有限集合 T_d を算出する。

【手順】
命題 4.20 に基づいて $f(\boldsymbol{x}) = \boldsymbol{x}^\top F\boldsymbol{x}$ を $d(f) = d$ を満たす Hermite-reduced な二次形式に対応する行列 F の成分の絶対値を上から評価して全列挙により計算する。 □

アルゴリズム 4.25. 与えられた 2 つの $\mathbb{Z}$ 係数二次形式 Q, Q' が $\mathbb{Z}$-equivalent かどうかを判定する

【手順】
STEP1:$d(Q), d(Q')$ を計算する。$d(Q) \neq d(Q')$ であれば $\mathbb{Z}$-equivalent ではない.$d(Q) = d(Q')$ であった場合は STEP2 に進む。
STEP2:Q, Q' の Hermite-majorant g, g' を算出する。
STEP3: さらに $g(S\boldsymbol{x}), g'(S'\boldsymbol{x})$ が Minkowski-reduced になるような $S, S' \in \mathrm{GL}_m(\mathbb{Z})$ を算出する。$Q(S\boldsymbol{x}), Q'(S'\boldsymbol{x})$ は Hermite-reduced である。
STEP4: 命題 4.8 の δ_m, η_m を算出する。
STEP5: 補題 4.22 にもとづいて $T \in \mathrm{GL}_m(\mathbb{Z})$ の成分の絶対値の bound を計算して、$Q(TS\boldsymbol{x}) = Q'(S'\boldsymbol{x})$ になる T が存在するかを確かめる。存在する場合は $\mathbb{Z}$-equivalent、存在しない場合は $\mathbb{Z}$-equivalent でない。
□

5 二次形式の isotropic 性の判定アルゴリズム

$\mathbb{Q}$ 上の二次形式が $\mathbb{Q}$ 上 isotropic かどうかを判定するにあたっては Hasse の原理により、$\mathbb{Q}$ の位相の完備化である $\mathbb{R}$ 上、及びすべての素数 p に対し $\mathbb{Q}_p$ 上 isotropic かどうかを調べればよい。$\mathbb{R}$ については QE で、$\mathbb{Q}_p$ については Hilbert 記号の計算に帰着させることで判定を行う。

5.1 p 進数

定義 5.1.
$\mathbb{R}_{\geq 0}$ で非負実数全体の集合を表すとする。写像 $||\cdot|| : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ が
1. $||a|| = 0 \Leftrightarrow a = 0$
2. $||ab|| = ||a|| \cdot ||b||$
3. $||a + b|| \leq ||a|| + ||b||$
を満たすときこの写像を $\mathbb{Q}$ 上の乗法的ノルムという. さらに 3 よりも強い条件
4. $|a + b|| \leq \max(||a||, ||b||)$
を満たす乗法的ノルムを Archimedes 的ノルムといい、Archimedes 的ノルムでないノルムを非 Archimedes 的ノルムという。

例 5.2.
通常の意味での絶対値 $|a|$ は $\mathbb{Q}$ 上の乗法的ノルムという。しかし、例えば $|1 + (-3)| = 2 > 1, -3 = 1$ なので非 Archimedes 的ノルムである。このノルムをユークリッドノルムと呼ぶ。

例 5.3.
素数 p を固定する. 任意の有理数 $q = \frac{a}{b}$ $(a \in \mathbb{Z}, b \in \mathbb{N}, q \neq 0)$ は $q = p^v \frac{a'}{b'}$ $(v \in \mathbb{Z}$ かつ $a' \in \mathbb{Z}, b' \in \mathbb{N}$ は p と互いに素$)$ という形で一意に表すことができる。この v を q の p 進付値とよび $v_p(q)$ と書く。便宜上 $v_p(0) = \infty$ と定め、v_p の定義域を $\mathbb{Q}$ 全体に拡張すると p 進付値は
1. $v_p(q_1 q_2) = v_p(q_1) + v_p(q_2)$
2. $v_p(q_1 + q_2) \geq \min(v_p(q_1), v_p(q_2))$
を満たすので写像 $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ を $|q|_p = \exp(-v_p(q))$ で定めるとこの写像は Archimedes 的ノルムにな

る. このノルムを p 進ノルムという。

$\mathbb{Q}$ 上の乗法的ノルムによる完備化によって p 進数体 $\mathbb{Q}_p$ を定義する。

定義 5.4.
有理数値をとる数列 $\{a_n\}$ が $\mathbb{Q}$ 上の乗法的ノルム $||\cdot||$ における Cauchy 列であるとは、$\forall\epsilon > 0 \exists N \in \mathbb{N} \forall m, n > N. ||a_m - a_n|| < \epsilon$ が成り立つことをいう。

命題 5.5.
$\mathbb{Q}$ 上の乗法的ノルム $||\cdot||$ における Cauchy 列全体の集合を $C_{||\cdot||}$ で表す。$C_{||\cdot||}$ 上に二項関係 $\sim$ を $\{a_n\} \sim \{b_n\} \overset{\text{def}}{\Leftrightarrow} \forall\epsilon > 0 \exists N \in \mathbb{N} \forall m, n > N. ||a_m - b_n|| < \epsilon$ で定めるとこれは同値関係になっている。さらに、$q \in \mathbb{Q}$ を定数列 $\{q, q, \cdots\}$ の同値類と同一視し、Caucy 列 $\{a_n\}$ の同値類 $\{\bar{a_n}\}$ に対して $||\{\bar{a_n}\}|| = \lim_{n\to\infty}||a_n||$ と定めることでノルム $||\cdot||$ を $C_{||\cdot||}/\sim$ に拡張することができる。

ノルム $||\cdot||$ から $C_{||\cdot||}/\sim$ を得ることをノルム $||\cdot||$ で $\mathbb{Q}$ を完備化するという。Cauchy 列 $\{a_n\}$ の同値類を $\{\bar{a_n}\}$ で書く.$C_{||\cdot||}/\sim$ に自然な演算を定めることで $\mathbb{Q}$ の拡大体を得ることができる。

命題 5.6.
$\{\bar{a_n}\}, \{\bar{b_n}\} \in C_{||\cdot||}/\sim$ に対して加法、乗法を
$\{\bar{a_n}\} + \{\bar{b_n}\} = \{a_n \bar{+} b_n\}$
$\{\bar{a_n}\}\{\bar{b_n}\} = \{\bar{a_n b_n}\}$
で *(*代表元の選び方によらずに*)* 定めることができ、この演算で $C_{||\cdot||}/\sim$ は体になる。$q \in \mathbb{Q}$ を定数列 $\{q, q, \cdots\}$ の同値類と同一視することで、この体は $\mathbb{Q}$ の拡大体と考えることができる。

$\mathbb{Q}$ を p 進ノルムで完備化したものが $\mathbb{Q}_p$ と書き、p 進数体と呼ぶ。$\mathbb{Q}$ 上で定めた p 進付値を $\mathbb{Q}_p$ に拡張子、p 進付値が非負になる $\mathbb{Q}_p$ の元の集合として p進 整数環 $\mathbb{Z}_p$ を特徴づけることができる。

命題 5.7.
$x \in \mathbb{Q}_p$ に対して $v_p(x) = -[\log|x|_p]$ *(*ただし $[\cdot]$ はガウスの記号*)* と定めるとこれは例 *5.3* の p 進付値の $\mathbb{Q}_p$ への拡張になる。

定義 5.8.
$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid v_p(x) \geq 0\}$ は $\mathbb{Q}_p$ の部分環である。この環を p 進整数環と呼ぶ。

$\mathbb{Q}_p, \mathbb{Z}_p$ の基本的な性質として以下がある。

命題 5.9.
1. $x \in \mathbb{Z}_p$ について、$x \in \mathbb{Z}_p^\times \Leftrightarrow x \notin p\mathbb{Z}_p$
2. 0 でない $\mathbb{Q}_p$ の元は $p^{v_p(x)}u$ $(u \in \mathbb{Z}_p^\times)$ という形で一意に表すことができる。

重要な命題である Hensel の補題と近似補題について述べる。$\boldsymbol{x} \in \mathbb{Q}_p^m$ に対して $||\boldsymbol{x}||_p = \max(|x_1|_p, \ldots, |x_m|_p)$,$v_p(\boldsymbol{x}) = \min(v_p(x_1), \ldots, v_p(x_m))$ と定める。

命題 5.10. (Hensel の補題、*[SERR 1978]Chapter2, Theorem1*)
$f \in \mathbb{Z}_p[X_1, \ldots, X_m], \boldsymbol{x} \in \mathbb{Z}_p^m$ とする。$n, k, j \in \mathbb{Z}, 0 \leq j \leq m, 0 \leq 2k < n$ であって $v_p(f(\boldsymbol{x})) \geq nv_p(\frac{\partial f}{\partial X_j}(\boldsymbol{x})) = k$ となる n, k, j が存在するとき、$f(\boldsymbol{x}_p) = 0$ かつ $v_p(\boldsymbol{x}_p - \boldsymbol{x}) \geq n$ であるような $\boldsymbol{x}_p \in \mathbb{Z}_p^m$ が

存在する。

命題 5.11. (近似補題 *[CASS 1978]*CHAPTER3 LEMMA2.1)
$Q(\boldsymbol{x})$ を regular で $\mathbb{Q}$ 上 isotropic な *3* 変数以上の二次形式、P を素数からなる有限集合で $\epsilon > 0$ とする。また、各 $p \in P$ について $\boldsymbol{x}_p \in \mathbb{Q}_p^m$ が $Q(\boldsymbol{x}_p) = 0$ を満たしているとする。このとき、ある $\boldsymbol{z} \in \mathbb{Q}^m$ が存在して、$Q(\boldsymbol{z}) = 0$ かつ $||\boldsymbol{z} - \boldsymbol{x}_p||_p < \epsilon$ *(*$p \in P$*)* を満たす。

5.2 Hasse の原理

方程式 (1) を解く過程で $\mathbb{Q}$ 上の二次形式が $\mathbb{Q}$ 上 isotropic であるかどうかを判定する部分がある。

判定には Hasse の原理を用いる。Hasse の原理とは、ある性質が有理数体上で成り立つことと $\mathbb{R}$ および $\mathbb{Q}_p$ 上で成り立つことが同値であるという形の命題である。以下は二次形式の isotropic 性 (定義 3.35) については Hasse の原理がなりたつという事を主張している。

命題 5.12. (*[CASS 1978]*CHAPTER 6 Theorem 1.1)
$\mathbb{Q}$ 上の regular な二次形式 Q が $\mathbb{Q}$ 上 isotropic であることの必要十分条件は、Q が $\mathbb{R}$ 上 isotropic かつ、任意の素数 p について $\mathbb{Q}_p$ 上 isotropic であることである。

命題 5.12 により二次形式が $\mathbb{R}$ 上 isotropic か、および $\mathbb{Q}_p$ 上 isotropic かを調べればよいことがわかる。

5 変数以上の regular な二次形式については任意の素数 p に対し、$\mathbb{Q}_p$ 上 isotropic であることが知られている。

命題 5.13. (*[CASS 1978]*CHAPTER6 COROLLARY1)
5 変数以上の regular な $\mathbb{Q}$ 上の二次形式は各素数 p について $\mathbb{Q}_p$ 上 isotropic。

さらに、以下が言える。

補題 5.14.
2 変数以上の regular、indefinite な二次形式は $\mathbb{R}$ 上 isotropic

命題 5.15. (*[CASS 1978]*CHAPTER6 COROLLARY1)
5 変数以上の regular かつ indefinite な $\mathbb{Q}$ 上の二次形式は $\mathbb{Q}$ 上 isotropic

【証明】
命題 5.13 および補題 5.14 から明らか。 □

5.3 $\mathbb{R}$ 上二次形式及び $\mathbb{Q}_p$ 上の 3,4 変数二次形式

命題 5.15 により調べるべきは 3, 4 変数の場合であることがわかる。[CASS 1978]CHAPTER2、LEMMA1.4、LEMMA1.5 の議論から $\mathbb{Q}$ 上の regular 二次形式はある対角二次形式 $\sum_{i=1}^{m} a_i x_i^2$ と

$\mathbb{Q}$-equivalent であることがわかる。また分母を払うことで isotropic 性を調べるにあたっては $a_i \in \mathrm{Z}$ としても一般性を失わない。$\mathbb{Q}_p$ 上の isotropic 性を調べるのに Hilbert 記号 (定義 3.37) の $F = \mathbb{Q}_p$ の場合について計算が必要になる。以下 $(a,b)_{\mathbb{Q}_p}$ のことを $(a,b)_p$ とかく。

$\mathbb{Q}_p$ 上の Hilbert 記号の計算には命題 3.38 の公式に加え、以下を用いる。計算の上で p が 2 の場合と奇素数の場合とで異なる扱いをする。以下、Gauss に始まる平方剰余の議論について述べる。

$p = 2$ の場合

命題 5.16. (*[雪江 2013]* 命題 9.2.8 (5))
$a, b \in \mathbb{Z} \cap (\mathbb{Z}_2^{\times})$ とするとき、以下が成り立つ。

(1) $(a,b)_2 = (-1)^{\frac{(a-1)(b-1)}{4}}$

(2) $(a,2)_2 = (-1)^{\frac{(a^2-1)}{8}}$ *(a が奇数であるとき、a^2-1 は常に 8 の倍数であることに注意。)*

p が奇素数の場合

定義 5.17.
$a \in \mathbb{Z}, p$ を奇素数とする。a が mod p である平方数と合同であることを a は p を法として平方剰余であるという。平方剰余でないことを平方非剰余という。

命題 5.18. (*[雪江 2013]* 命題 9.2.2 (3)、命題 9.2.8 (4))
p を奇素数とする。

(1) $a, b \in \mathbb{Z}_p^{\times}$ であれば、$(a,b)_p = 1$
(2) $a \in \mathbb{Z}_p^{\times}$ であるとき、$(a,p)_p = 1 \Leftrightarrow a$ は p を法として平方剰余

以下、上記の Hilbert 記号を用いた isotropic 性の判定について述べる。

定義 5.19.
$Q'(\boldsymbol{x}) = \sum_{i=1}^{m} a_i x_i^2$ を整数係数の regular な二次形式とし、p を素数とする。$c_p(Q') = \prod_{i<j}(a_i, a_j)_p$ と定める。

3 変数の対角二次形式が $\mathbb{Q}_p$ 上 isotropic かどうかを判定するには以下の命題を用いる。

命題 5.20. *([CASS 1978]*CHAPTER4 LEMMA2.5*)*
Q' を $\mathbb{Q}_p$ 上の 3 変数整数係数の regular な対角二次形式とするとき、
Q' が $\mathbb{Q}_p$ 上 isotropic $\Leftrightarrow c_p(Q') = (-1, -d(Q'))_p$

4 変数の場合については以下の命題を使う。

命題 5.21.
Q' を $\mathbb{Q}_p$ 上の 4 変数整数係数の regular な対角二次形式とするとき、
Q' が $\mathbb{Q}_p$ 上 anisotropic であることの必要十分条件は、以下の *(1),(2)* がともに成り立つことである。

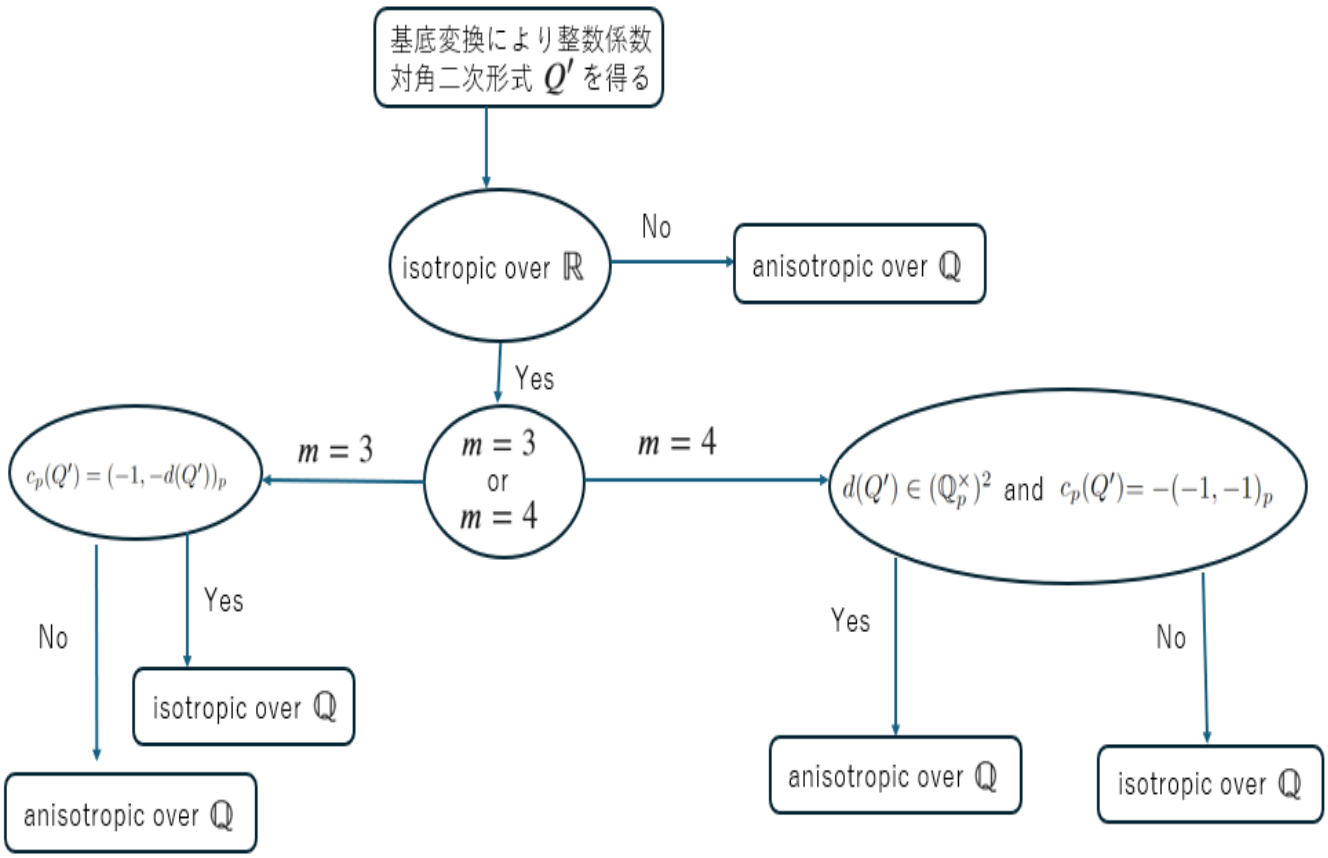
(1) $d(Q') \in (\mathbb{Q}_p^{\times})^2$
(2) $c(Q') = -(-1,-1)_p$

$d(Q') \in \mathbb{Z}$ が $\mathbb{Q}_p$ の平方元であるかを判定するには、$p = 2$ の場合は命題 5.22 を、p が奇素数の場合は命題 5.23 を用いる。

命題 5.22. (*[SERR 1978]*Chapter2 Theorem 3)
$2^n u \in \mathbb{Z}\,(u \in \mathbb{Z}_2^{\times})$ が $\mathbb{Q}_2$ の平方元であることの必要十分条件は n が偶数でありかつ $v_2(u-1) \geq 3$ がなりたつことである。

命題 5.23. (*[SERR 1978]*Chapter2 Theorem3)
p を奇素数とする。$p^n u \in \mathbb{Z}\,(u \in \mathbb{Z}_p^{\times})$ が $\mathbb{Q}_p$ の平方元であることの必要十分条件は n が偶数でありかつ u を p で割った余りが $\mathbb{F}_p$ の平方元になることである。

上記をまとめて isotropic 性を判定するアルゴリズムをまとめると以下のフローチャートのようになる。



6 $\mathbb{Q}$-群に対応する Lie 環の計算アルゴリズム

この章では本論文で用いる Lie 環について Lie 環の教科書としては [井ノ口 2017] を参照している。

6.1 Lie 環の基本事項

定義 6.1.
体 F 上のベクトル空間 $\mathcal{L}$ とその上に与えられたブラケット積と呼ばれる 2 項演算 $[\cdot,\cdot]:\mathcal{L}\times\mathcal{L}\to\mathcal{L}$ との組が以下の条件を満たしているとき、その組を体 F 上の Lie 環という。
1.*(双線形性)* 任意のスカラー $a,b\in F$ とベクトル $x,y,z\in\mathcal{L}$ について,$[ax+by,z]=a[x,z]+b[y,z]$ および $[z,ax+by]=a[z,x]+b[z,y]$ が成り立つ。
2.*(交代性)* 任意の $x\in\mathcal{L}$ について $[x,x]=0$ が成り立つ。
3.*(ヤコビ恒等式)* 任意の $x,y,z\in\mathcal{L}$ について, $[x,[y,z]]+[z,[x,y]]+[y,[z,x]]=0$ が成り立つ。

定義 6.2.
Lie 環 $\mathcal{L}$ の線形部分空間 W がイデアルであるとは、$[\mathcal{L}_{\mathbb{Q}}(G),W]\subseteq W$ が成り立つことをいう。

定義 6.3.
Lie 環 $\mathcal{L}$ が単純であるとは $\mathcal{L}$ が $\{\mathbf{0}\}$ と $\mathcal{L}$ 自身以外にイデアルを持たないことをいう。

定義 6.4.
Lie 環 $\mathcal{L}$ が半単純であるとは単純な Lie 環の直和で $\mathcal{L}$ が表されることをいう。

定義 6.5.
Lie 環 $\mathcal{L}$ が可解であるとは、部分 Lie 環の列 $\mathcal{L}\supseteq[\mathcal{L},\mathcal{L}]\supseteq[[\mathcal{L},\mathcal{L}],[\mathcal{L},\mathcal{L}]]\supseteq\cdots$ がいずれ $\{\mathbf{0}\}$ に達することをいう。
ただし Lie 環 $\mathcal{L}$ に対して $[\mathcal{L},\mathcal{L}]$ とは $\{[x,y]|x,y\in\mathcal{L}\}$ のことをいう。

定義 6.6.
$\mathcal{L}$ を体 $\mathbb{Q}$ 上の Lie 環とする。$x\in\mathcal{L}$ に対して線形写像 $\mathrm{ad}(x):\mathcal{L}\to\mathcal{L}$ を $(\mathrm{ad}(x))(y)=(x,y)$ で定める。
体 $\mathbb{Q}$ 上の Lie 環 $\mathcal{L}$ に対して双線形形式 $K_{\mathcal{L}}:\mathcal{L}\times\mathcal{L}\to\mathbb{Q}$ を $K(x,y)=\mathrm{trace}(\mathrm{ad}(x)\circ\mathrm{ad}(y))$ で定めることができる。この $K_{\mathcal{L}}$ を Lie 環 $\mathcal{L}$ のキリング形式と呼ぶ。

定義 6.7.
$\mathcal{L}$ を体 F 上の有限次元 Lie 環として、$\{y_1,\ldots,y_s\}$ をその基底とする。$\mathcal{L}$ のキリング形式 $K_{\mathcal{L}}$ が非退化であるとは、$K_{\mathcal{L}}(y_i,y_j)$ を ij 成分とする行列が正則になることをいう。$K_{\mathcal{L}}$ が非退化かどうかは基底の取り方によらない。

以下が成り立つので、キリング形式を調べることで有限次元 Lie 環の半単純性およびに可解性を判定することができる。

命題 6.8.
Lie 環 $\mathcal{L}$ が半単純であることと、$\mathcal{L}$ のキリング形式 $K_{\mathcal{L}}$ が非退化であることは同値である。

命題 6.9.
Lie 環 $\mathcal{L}$ が可解であることと、任意の $a \in \mathcal{L}, b \in [\mathcal{L}, \mathcal{L}]$ について $K_{\mathcal{L}}(a, b) = 0$ が成り立つことは同値である。

6.2 Lie 環の直和分解と冪零イデアル

命題 6.10.
$\mathcal{L}$ を体 F 上の Lie 環で $\mathrm{M}_m(F)$ の部分集合であるとする。$\mathcal{L}$ の要素のうち、冪零行列を集めたものを $n(\mathcal{L})$ とかき、$\mathcal{L}$ の冪零イデアルと呼ぶ。実際、$n(\mathcal{L})$ は $\mathcal{L}$ のイデアルである。

Lie 環の一般論として、以下が知られている。

命題 6.11. (*[MOS 1956]*4.1)
$\mathcal{L}$ を体 F 上の Lie 環とし、$\mathrm{M}_m(F)$ の部分集合であるとする。このとき、以下の条件を満たすような直和分解 $\mathcal{L}_{\mathbb{Q}}(G) = A + B + C$ が存在する。
(1) C は $\mathcal{L}$ の部分 Lie 環で、半単純である。
(2) $A + B$ は $\mathcal{L}$ のイデアルである。
(3) $A + B$ は可解 Lie 環である。
(4) A は冪零行列によって生成される。
(5) B は可換で対角化可能行列によって生成される。
この直和分解のうち、半単純 Lie 環と可解 Lie 環との直和分解は Wedderburn 分解と呼ばれる.

このような直和分解が得られれば、$A = n(\mathcal{L})$ であることがわかる. 与えられた有限次元 Lie 環に対し、$\mathcal{L}$ の基底 $Y = \{y_1, \ldots, y_s\}$ およびその基底を 3 つの部分集合に分けることで直和成分 A, B, C を得たい。そのためには Y から部分集合 $X = \{x_1, \ldots, x_q\}$ を取ってきた際に X で生成される $\mathbb{Q}-$ ベクトル空間 $\langle X \rangle$ が上記 (1) (5) の条件を満たすかどうかを確認するアルゴリズムがあればよい。

アルゴリズム 6.12.
$\langle X \rangle$ が $\mathcal{L}$ の部分 Lie 環であるかどうかをチェックする。

【手順】任意の $x_i, x_j \in X$ について (x_i, x_j) が $y_1, \ldots, y_s$ と一次従属になるかを調べればよい。

アルゴリズム 6.13.
(1) の条件をチェックする、すなわち部分 Lie 環 $\langle X \rangle$ が半単純かどうかを調べる。

【手順】
$\langle X \rangle$ のキリング形式 $K_{\langle X \rangle}$ が非退化かどうかをみればよい。すなわち行列 $(K_{\langle X \rangle}(x_i, x_j))_{i,j}$ が正則かどうかを調べればよい。

アルゴリズム 6.14.
(2) の条件をチェックする、すなわち $\langle X \rangle$ が $\mathcal{L}$ のイデアルかどうかを調べる。

【手順】任意の $x_i \in X$ と $y_j \in Y$ に対して $(x_i, y_j) \in \langle X \rangle$ となるかどうかを調べるとよい。

アルゴリズム 6.15.
(3) の条件をチェックする、すなわち部分 Lie 環が $\langle X \rangle$ が可解かどうかを調べる。

【手順】
任意の $a \in \langle X \rangle, b \in (\langle X \rangle, \langle X \rangle)$ について、$K_{\langle X \rangle}(a, b) = 0$ が成り立つかどうかを調べればよい。$a \in \langle X \rangle, b \in (\langle X \rangle, \langle X \rangle)$ は、$a = \sum_l \mu_l x_l, b = \sum_{i,j} \nu_{ij}(x_i, x_j)$ と書き表せる。また (x_i, x_j) を計算することで $(x_i, x_j) = \sum_k \lambda_{ijk} x_k$ を満たす定数 $\lambda_{ijk} \in \mathbb{Q}$ を計算することができる。
あとは $K_{\langle X \rangle}(a, b) = K_{\langle X \rangle}(\sum_l \mu_l x_l, \sum_{i,j} \nu_{ij}(\sum_k \lambda_{ijk} x_k)) = 0$ が μ_l, ν_{ij} についての恒等式になるかどうかを調べればよいが、$K_{\langle X \rangle}$ が双線形形式であることを考えれば、$K_{\langle X \rangle}(x_i, x_j)$ を計算すればよいことがわかる。

アルゴリズム 6.16.
(4) の条件をチェックする、すなわち X の元がすべて冪零行列かどうかを調べる。

【手順】
各 $x \in X$ の固有値が 0 のみであるかどうかを調べればよい。

アルゴリズム 6.17.
(5) の条件をチェックする、すなわち X の元がすべて可換で対角化可能行列かどうかを調べる。

【手順】
可換かどうかを確かめるには実際に行列の積を計算すればよい。対角化可能かを確かめるには各 $x \in X$ の最小多項式 f_x が重根を持たないかどうかを確かめる、すなわち f_x と f_x' が互いに素かどうかを調べればよい。

今後扱う Lie 環としては $\mathbb{Q}$-群に対応する Lie 環を想定しており、これは有理数を成分に持つ m 次正方行列の集合である。したがって、$\mathbb{Q}$ 上有限次元ベクトル空間であり可算集合なので、以下のようにして直和分解を計算することができる。

アルゴリズム 6.18.
$\mathcal{L}$ を $\mathcal{L} \in \mathrm{M}_m(\mathbb{Q})$ な $\mathbb{Q}$ 上の Lie 環とし、*6.11* の (1)〜(5) を満たす直和分解 $\mathcal{L} = A + B + C$ を算出する。つまり A, B, C の基底を算出する。

【手順】
集合 $\mathcal{Y} = \{\, \{y_1, \ldots, y_s\} \mid \{y_1, \ldots, y_s\}$ は $\mathcal{L}$ の基底 $\}$ は可算集合なので、$\mathcal{L}$ の基底の各パターンを列挙することができる。各基底 $Y = \{y_1, \ldots, y_s\}$ に対してこれを 3 つに分割するやり方は有限通りなので、各分割に対してアルゴリズム 6.12〜6.17 を試せばよい。

6.3 冪零行列の Jordan 標準形への基底変換

この節では Lie 環の central-flag の定義及び計算方法について述べる。central-flag を計算する Lie 環としては冪零行列からなるものを想定している。冪零行列からなる Lie 環の central-flag を計算することで、行列を Jordan 標準形にする基底変換を得ることができる。この基底変換は 8 章で述べる冪単 (unipotent)$\mathbb{Q}$-群を

対角成分がすべて 1 の上三角行列のみからなる群からなる行列群に変換するのに用いられる。

定義 6.19.
$\mathcal{L} \subseteq M_m(\mathbb{Q})$ を Lie 環とする。$\mathbb{C}$-ベクトル空間の列 $\mathcal{E} : 0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_k = \mathbb{C}^m$ が $V_i = \{v \in \mathbb{C}^m \mid (v^\top \mathcal{L})^\top \subseteq V_{i-1}\}$ を満たすとき、$\mathcal{E}$ を Lie 環 $\mathcal{L}$ の central-flag という。この k は $\mathcal{E}$ の長さと呼ばれる。
上記の状況の時、$\mathbb{Z}^m$ の基底 $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_m\} \subset \mathbb{Z}^m$ であって、$V_i = \sum_{j=1}^{r_i} \mathbb{C}\boldsymbol{e}_j$ となるものがとれる。各 $i = 1, \cdots, k$ に対して $\dim_{\mathbb{C}} V_i = r_i$ である。組 $(r_1, \ldots, r_k)$ のことを $\mathcal{E}$ の型と言い、基底 $\mathcal{B} = \{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_m\}$ のことを $\mathcal{E}$ の整基底という。

アルゴリズム 6.20. Lie 環 $\mathcal{L} \subseteq M_m(\mathbb{Q})$ の central-flag $\mathcal{E} : 0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_k = \mathbb{C}^m$ が存在すれば計算する。存在しない場合には存在しないという結果を返す。central-flag が存在する場合はその整基底を得る。

【手順】
$\mathcal{L}$ の基底を $n_1, \ldots, n_l$ とする。
$V_1 = \{v \in \mathbb{C}^m \mid v^\top \mathcal{L} = 0\}$ なので v についての連立一次方程式
$v^\top n_i = 0$ (ただし $i = 1, \ldots, l$) を解くことで、(解があれば)V_1 の基底 $b_1^{(1)}, \ldots, b_{l^{(1)}}^{(1)}$ を得ることができる。この基底は有理数を成分とするベクトルで得られるので、適切に定数倍して $b_1^{(1)}, \ldots, b_{l^{(1)}}^{(1)} \in \mathbb{Z}^m$ かつこれらすべてが primitive であるようにしておく。次に
$V_2 = \{v \in \mathbb{C}^m \mid v^\top \mathcal{L} \subseteq V_1\}$ についてだが、$v \in V_2$ は各 n_i に対して $v^\top n_1 \in \langle b_1^{(1)}, \ldots, b_{l^{(1)}}^{(1)} \rangle$ が成り立つことと同値であるから連立方程式
$v^\top n_i^2 = 0$ (ただし $i = 1, \ldots, l$) を解くと基底ベクトル $b_1^{(2)}, \ldots, b_{l^{(2)}}^{(2)} \in \mathbb{Z}^m$ (primitive) が得られ、V_2 の次元もわかる。これらのうち V_1 の基底と一次独立なものを V_2 の次元数に達するまで付け加えることで V_2 の基底が得られる. 以下同様に連立方程式
$v^\top n_i^j = 0$ (ただし $i = 1, \ldots, l$) を解いて得られた基底ベクトルを V_{j-1} の基底に付け加えることを繰り返すことで $\mathcal{L}_{\mathbb{Q}}(N)$ の central-flag $\mathcal{E} : 0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_k = \mathbb{C}^m$ が得られる。さらに、V_k の基底が $\mathcal{E}$ の整基底である。ただし整基底が得られるまでに、連立方程式が解なしとなった場合は central-flag は存在しないという判定になる。

7 $\mathbb{Q}$-群とその Lie 環について

$\mathrm{GL}_m(\mathbb{C})$ の部分群であって有限個の多項式 $f_1, \ldots, f_s \in \mathbb{Q}[X_{11}, \ldots, X_{mm}]$ の共通零点集合と $\mathrm{GL}_m(\mathbb{C})$ の共通部分で表される群 G を $\mathbb{Q}$-群と呼び、$G_{\mathbb{Q}}$ の部分群 Γ が $|\Gamma : \Gamma \cap G_{\mathrm{Z}}|, |G_{\mathrm{Z}} : \Gamma \cap G_{\mathrm{Z}}| < \infty$ をみたすとき Γ を G の arithmetic-subgroup と呼ぶ. Borel らは $\mathbb{Q}$-群の arithmetic-subgroup は有限生成であることが示しており、([BHC 1962]) その証明をもとに Grunewald は arithmetic-subgroup の生成系を計算するアルゴリズムを構成的に示した。([GRUN 1980])

7.1 位相空間とザリスキ位相

位相空間の定義

定義 7.1.

X を集合とし,$\mathcal{O}$ を X のべき集合 $\mathcal{P}(X)$ の部分集合とする。$\mathcal{O}$ が以下の性質を満たすとき、組 $(X, \mathcal{O})$ を位相空間と呼ぶ。
1. $\emptyset, X \in \mathcal{O}$
2. 任意の $U_1, U_2 \in \mathcal{O}$ について $U_1 \cap U_2 \in \mathcal{O}$
3. 任意の族 $\{U_\lambda\}_{\lambda \in \Lambda} \subseteq \mathcal{O}$ について $\cup_{\lambda \in \Lambda} U_\lambda \in \mathcal{O}$

$(X, \mathcal{O})$ が位相空間であるとき、$\mathcal{O}$ の元を X の開集合という。

定義 7.2.
$(X, \mathcal{O})$ が位相空間であるとする。X の開集合 $U \in \mathcal{O}$ の補集合を X の閉集合という。

定義 7.1 より、閉集合については以下が成り立つ。

命題 7.3.
位相空間 $(X, \mathcal{O})$ の閉集合全体の族を $\mathcal{C}$ でかく。$\mathcal{C}$ について以下が成り立つ。
1. $\emptyset, X \in \mathcal{C}$
2. 任意の $F_1, F_2 \in \mathcal{C}$ について $F_1 \cup F_2 \in \mathcal{C}$
3. 任意の族 $\{F_\lambda\}_{\lambda \in \Lambda} \subseteq \mathcal{C}$ について $\cap_{\lambda \in \Lambda} F_\lambda \in \mathcal{C}$

位相空間の連結性と連結成分の定義を述べる。

定義 7.4.
位相空間 X が部分空間 X_1, X_2 の直和に分かれているというのは、X_1, X_2 が X の開集合であり $X = X_1 \cup X_2$ かつ $X_1 \cap X_2 = \emptyset$ が成り立っていることをいう。X が部分空間 X_1, X_2 の直和に分かれていれば X_1かX_2 のどちらかが空集合になるとき、X は連結であるという。位相空間 X の部分集合 A が連結であるとはそれが部分空間として連結であるという。

命題 7.5. (*[川崎 2020]* 定理 13.10)
X を位相空間とする。
1. $p \in X$ に対して p を含む最大の連結集合を $C(p)$ が存在する。
2. $C(p) \subseteq X$ は閉集合である。
3. $p, q \in X$ に対して $C(p) \cap C(q) = \emptyset$ または $C(p) = C(q)$ がなりたつ。

定義 7.6.
命題 *7.5* の $C(p)$ を連結成分という。

多項式の零点集合を閉集合として定められるザリスキ位相について述べる。

定義 7.7.
F を代数閉体とし、$\mathfrak{a} \subseteq F[X_1, \cdots, X_m]$ をイデアルとするとする。F^m の部分集合 $\{(x_1, \cdots, x_m) \in R^m | \forall f \in \mathfrak{a}. f(x_1, \cdots, x_m) = 0\}$ を $\mathfrak{a}$ の零点集合と呼び、$\mathcal{Z}(\mathfrak{a})$ と書く。あるイデアル $\mathcal{Z}(\mathfrak{a})$ という形で書ける F^m の部分集合を代数的集合と呼ぶ。

代数的集合は閉集合の性質を満たしており、これによって位相を定めることができる。この位相をザリスキ位相という。

命題 7.8. (*[Ha 2000]*propsition 1.1) F を代数閉体、$X = F^m$ とする。このとき、1. $\emptyset, X$ は代数的集合
2. Y_1, Y_2 が代数的集合であるとき、$Y_1 \cup Y_2$ も代数的集合
3. $\{Y_\lambda\}$ を代数的集合の族とするとき、$\cap_\lambda Y_\lambda$ もまた代数的集合

7.2 $\mathbb{Q}$-群とその arithmetic-subgroup

定義 7.9.
$\mathrm{GL}_m(\mathbb{C})$ の部分群 G が $\mathbb{Q}$-群であるとは、G が *(*有限生成*)* イデアル $\mathfrak{a} \subseteq \mathbb{Q}[X_{11}, \cdots, X_{mm}]$ の零点集合 $\mathcal{Z}(\mathfrak{a})$ に対し、$G = \mathcal{Z}(\mathfrak{a}) \cap \mathrm{GL}_m(\mathbb{C})$ とあらわされることをいう。
R を $\mathbb{C}$ の部分環とする。$\mathbb{Q}$-群 G について,$G_R = G \cap \mathrm{GL}_m(R)$ とかく。R としては $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ を主に想定している。

定義 7.10.
G を $\mathbb{Q}$-群とする。G の部分群 $\Gamma \subseteq G_{\mathbb{Q}}$ が G の arithmetic-subgroup であるとは、$|G_{\mathbb{Z}} : \Gamma \cap G_{\mathbb{Z}}|$ と $|\Gamma : \Gamma \cap G_{\mathbb{Z}}|$ がともに有限であることをいう。

$\mathbb{Q}$-群の arithmetic-subgroup の重要な性質として、[BHC 1962] によって示された以下がある。

定義 7.11.
$\mathbb{Q}$-群の arithmetic-subgroup は有限生成である。

定義 7.12.
$\mathbb{Q}$-群 $G = \mathcal{Z}(\mathfrak{a}) \cap \mathrm{GL}_m(\mathbb{C})$ について、G の次元をイデアル $\mathfrak{a}$ の次元 $\dim(\mathfrak{a})$ で定める。命題 *2.44* により $\mathbb{Q}$-群の次元は有限である。

定義 7.13.
$\mathbb{Q}$-群 G の冪単根基 (unipotent-radical) を $u(G)$ とかく。$u(G)$ は冪単行列からなる G の正規部分群のうち極大なものである。

定義 7.14.
$\mathbb{Q}$-群 H が reductive であるとは、$u(H) = \{I_m\}$ であることをいう。

例 7.15.
$\mathfrak{a} = \langle X_{32} - (X_{32} - X_{33})^2, X_{11} - (X_{32} - X_{33})^3, X_{32}, X_{31}, X_{21}, X_{11}, X_{12}, X_{11} + X_{13}, X_{22} + X_{23} \rangle$ とし、$G = \mathcal{Z}(\mathfrak{a}) \cap \mathrm{GL}_m(\mathbb{C})$、$H = \left\{ \begin{pmatrix} t & 0 & 0 \\ 0 & t^2 & 0 \\ 0 & 0 & t^3 \end{pmatrix} \mid t \in \mathbb{C} \setminus \{0\} \right\}$ とすると、$V = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \in \mathrm{GL}_m(\mathbb{Z})$ にたいして $VGV^{-1} = H$ がなりたつ。H の元で冪単なものは単位行列のみなので、H は reductive であり、G も reductive となる。

定義 7.16.
G を $\mathbb{Q}$-群とし、$N = u(G)$ とする。$G = N \rtimes H$ となる reductive な $\mathbb{Q}$-群 H を N の reductive complement という。

arithmetic-subgroup の生成系を計算する手順の重要な部分に $\mathbb{Q}$-群 G を冪単根基 $N = u(G)$ を使って $G = N \rtimes H$ と半直積に分解する部分がある。次節で論じる $u(G)$ 計算の議論では G のザリスキ位相での連結性が仮定されている。そのため単位行列を含む $\mathbb{Q}$-群のザリスキ位相においての連結成分について述べておく。

定義 7.17. G を $\mathbb{Q}$-群とする。
G の (ザリスキ位相での) 連結成分のうち単位行列を含むものを G^0 と書く。

命題 7.18. (*[GRUN 1980]*THEOREM 3.3.1) G を $\mathbb{Q}$-群とする。G^0 を定義 *7.17* で定めたザリスキ位相での連結成分とする。$K \subseteq (G^0)_{\mathbb{R}}$ を $(G^0)_{\mathbb{R}}$ のユークリッド位相での連結成分であって単位行列を含むものとし、D を $G^0_{\mathbb{R}}$ の *(*実数の範囲で*)* 対角化可能行列からなる部分群であって、$\mathrm{M}_m(\mathbb{R})$ 上の代数的集合かつザリスキ位相で連結であるようなもののうち極大なものとする。このとき、$(G^0)_{\mathbb{R}} = KD$ と書ける。

G^0 について以下が成り立つため,$u(G)$ を計算するためには $u(G^0)$ が計算できれば良い。

命題 7.19.
$u(G) = u(G^0)$ である。

命題 7.19 より、unipotent-radical の計算にあたっては $\mathbb{Q}$-群のザリスキ位相での連結性を仮定してもよい、以下では $\mathbb{Q}$-群のザリスキ位相での連結性を仮定しており、議論の対象とする $\mathbb{Q}$-群としては連結成分 G^0 を想定している。

まずは G^0 を計算する必要がある。$\mathbb{Q}$-群 $G = \mathcal{Z}(\mathfrak{a}) \cap \mathrm{GL}_m(\mathbb{C})$ に対し、$G^0 = \mathcal{Z}(\mathfrak{b}) \cap \mathrm{GL}_m(\mathbb{C})$ となる $\mathfrak{a}$ の極小素イデアルを求める必要がある。具体的には以下が知られている。

命題 7.20. (*[GRUN 1980]*LEMMA 3.1.3)
$G = V(\mathfrak{a})$ を $\mathbb{Q}$-群とする。$\mathfrak{a}$ の極小素イデアルは有限個であり、その極小素イデアルを $\mathfrak{p}_1 = \langle f_{11}, \cdots, f_{1r_1} \rangle, \cdots, \mathfrak{p}_s = \langle f_{s1}, \cdots, f_{1r_s} \rangle$ とするとき、$f_{i1}(I_m) = \cdots = f_{ir_i}(I_m) = 0$ となるような番号 i がちょうど一つ存在する。この $\mathfrak{p}_i$ が G^0 を定める、すなわち $G^0 = V(\mathfrak{p}_i) \cap \mathrm{GL}_m(\mathbb{C})$ である。

7.3 $\mathbb{Q}$-群に対応する Lie 環の計算アルゴリズム

定義 7.21.
$x = (x_{ij}) \in \mathrm{M}_m(\mathbb{Q})$ に対してある写像 $\delta(x) : \mathbb{Q}[X_{11}, \cdots, X_{mm}] \to \mathbb{Q}[X_{11}, \cdots, X_{mm}]$ を
$\delta(x)(f) = -\sum_{l,m} \sum_j x_{lj} x_{lj} X_{jm} \frac{\partial f}{\partial X_{lm}}$
で定める。

定義 7.22.
$G = \mathcal{Z}(\mathfrak{a}) \cap \mathrm{GL}_m(\mathbb{C})$ を (Zariski 位相で) 連結な $\mathbb{Q}$-group とする。G の Lie 環 $\mathcal{L}_{\mathbb{Q}}(G)$ を
$\mathcal{L}_{\mathbb{Q}}(G) = \{x \in \mathrm{M}_m(\mathbb{Q}) | \delta(\mathfrak{a}) \subseteq \mathfrak{a}\}$
で定める。この $\mathcal{L}_{\mathbb{Q}}(G)$ は通常の和と交換子積 $[a, b] = ab - ba$ で Lie 環になっている。

アルゴリズム 7.23. $G^0 = \mathcal{Z}(\mathfrak{a}) \cap \mathrm{GL}_m(\mathbb{C})$ であるとし,$\mathfrak{a}$ の生成多項式を $f_1, \ldots, f_r$ とするとき, 対応する Lie

環 $\mathcal{L}_{\mathbb{Q}}(G^0)$ の $\mathbb{Q}$ 上の基底を算出する。

【手順】
$i = 1, \cdots, r$ に対して写像 $\lambda_i : \mathrm{M}_m(\mathbb{Q}) \to \mathbb{Q}$ を
$\lambda_i(x) = (\delta(x)(f))(I_m)$
で定める.$x \in \mathcal{L}_{\mathbb{Q}}(G^0) \Leftrightarrow x \in \cap_{i=1}^{r} \mathrm{Ker}\lambda_i$ が成り立つことが知られているので、これを利用する。$\delta(x)$ の定義から方程式 $\lambda_i(x) = 0$ $(i = 1, \cdots, r)$ は x_{ij} についての連立一次方程式なので、掃き出し法によって $\mathcal{L}_{\mathbb{Q}}(G^0)$ の基底となる行列を算出することができる。

8 幂単根基とその reductive-complement

8.1 $u(G)$ の計算

$u(G^0)$ の Lie 環 $n(\mathcal{L}_{\mathbb{Q}}(G^0)) = \mathcal{L}_Q(u(G^0))$ の基底を計算したいが冪単根基 $u(G^0)$ に対応する Lie 環は $\mathcal{L}_{\mathbb{Q}}(G^0)$ の冪零イデアルと同一であることが知られている。

命題 8.1. (*[MOS 1956]*Theorem 7.1)
$n(\mathcal{L}_Q(G^0)) = \mathcal{L}_Q(u(G^0))$

アルゴリズム 8.2. (*[GRUN 1980]*pp560) G^0 から $u(G)$ を計算する。

【手順】
$\mathcal{L}_Q(u(G^0))$ は $\mathrm{M}_m(\mathbb{Q})$ の部分空間なので, アルゴリズム 7.23 で $\mathcal{L}_Q(G^0)$ の基底を得ることができ, さらにアルゴリズム 6.18 によって,$n(\mathcal{L}_Q(G^0)) = \mathcal{L}_Q(u(G^0))$ の基底を計算することができ, そこから $\mathcal{L}_Q(u(G^0)) = \mathcal{Z}(\{P_1, \ldots, P_t\})$ となる 1 次多項式 $P_1, \ldots, P_t$ を得ることができる。多項式 $\log^*(X)$ を $\log^*(X) = -\sum_{i=1}^{m-1} i^{-1}(I_m - X)^i$ で定めると、
$u(G) = u(G^0) = \mathcal{Z}(\{(X-1)^m, P_1(\log^*(X)), \ldots, P_t(\log^*(X))\}) \cap \mathrm{GL}_m(\mathbb{C})$
である。

代数群と Lie 環の一般論と行列の指数・対数関数の議論から $u(G^0) = \exp(\mathcal{L}_Q(G^0)), \mathcal{L}_Q(G^0) = \log(u(G^0))$ であることがわかる。([BO 1969] 7.3) また,Lie 環の直和分解は Q-群では半直積分解に対応している。$\log^*(X)$ は $\log(X)$ の級数を有限の項で打ち切ったものであり、U が冪単行列である場合 $\log^*(U) = \log(U)$ となることが $u(G)$ を定義する多項式が計算できるポイントである。一方、reductive-complement に属する行列については log が有限項の多項式にならないので、次節のアルゴリズムで別途計算する必要がある。

8.2 reductive-complement の計算

まず準備として、$\mathbb{Q}$-群の central-flag について述べる。

定義 8.3.
G を $\mathbb{Q}$-群とする。G の central-flag $\mathcal{E} = \mathcal{E}(G)$ を $\mathbb{C}^m$ の部分空間の列
$\{\mathbf{0}\} = V_0 \subset V_1 \subset \cdots \subset V_k = \mathbb{C}^m$
であって、$V_i/V_{i-1} = \{\boldsymbol{x} \in V/V_{i-1} | g\boldsymbol{x} = \boldsymbol{x} \text{ for all } g \in G\}$ が成立するものとして定める。この k を $\mathcal{E}$ の長さ

と呼ぶ。
上記の状況の時、$\mathbb{Z}^m$ の基底 $\{\boldsymbol{e}_1,\ldots,\boldsymbol{e}_m\} \subset \mathbb{Z}^m$ であって、$V_i = \sum_{j=1}^{r_i} \mathbb{C}\boldsymbol{e}_j$ となるものがとれる。各 $i = 1,\cdots,k$ に対して $\dim_{\mathbb{C}} V_i = r_i$ である。組 $(r_1,\ldots,r_k)$ のことを $\mathcal{E}$ の型と言い、基底 $\mathcal{B} = \{\boldsymbol{e}_1,\ldots,\boldsymbol{e}_m\}$ のことを $\mathcal{E}$ の整基底という。

unipotent な $\mathbb{Q}$-群の centralflag について, 以下が成り立つ.

命題 8.4.
N を unipotent Q-群、$\mathcal{L}_{\mathbb{Q}}(N)$ をその Lie 環とするとき、N と $\mathcal{L}_{\mathbb{Q}}(N)$ は同一の central-flag をもつ。

この命題により、アルゴリズム 6.20 によって Lie 環 $\mathcal{L}_{\mathbb{Q}}(N)$ の central-flag を計算することで unipotent な Q-群 N の central-flag を計算することができる。

注 8.5.
N が冪単行列からなる $\mathbb{Q}$-群である場合、central flag $\mathcal{E} = \mathcal{E}(N)$ の整基底 $\mathcal{B} = \{\mathbf{e}_1,\ldots,\mathbf{e}_m\}$ を基底とするベクトル空間に N を作用させれば N の元はすべて対角成分がすべて 1 の上三角行列行列で表現される。したがって,N が冪単行列からなる $\mathbb{Q}$-群であれば、その整基底への基底変換によって N は $\mathbb{U}$ の部分群であるとみなしてよい。

定義 8.6.
$\mathcal{E}$ を unipotent な $\mathbb{Q}$-群 N の central flag とし、$\mathcal{B} = \{\mathbf{e}_1,\ldots,\mathbf{e}_m\}$ をその整基底とする。

$$\begin{cases} M(\mathcal{E}) = \{g \in \mathrm{GL}_m(\mathbb{C}) \mid gV_i = V_i \ i = 1,\cdots,k\} \\ W_i = W_i(\mathcal{B}) = \displaystyle\sum_{j=r_{i-1}+1}^{r_i} \mathbb{C}\mathbf{e}_j \\ U(\mathcal{E}) = \{g \in \mathrm{GL}_m(\mathbb{C}) \mid (g - I_m)V_i \subseteq V_{i-1} \ i = 1,\cdots,k\} \\ P = P(\mathcal{E},\mathcal{B}) = \{g \in M(\mathcal{E}) \mid gW_i = W_i\} \end{cases}$$

と定める。M は乗法で群をなし、G は M の部分群になっている。

以下 G を $\mathbb{Q}$-群、$N = u(G)$,$\mathcal{E} = \mathcal{E}(N)$、$\mathcal{E}$ の整基底を $\mathcal{B}$ とし、$M = M(\mathcal{E})$、$U = U(\mathcal{E})$,$P = P(\mathcal{E},\mathcal{B})$ とする。以下が知られている。

命題 8.7. (*[GRUN 1980]*LEMMA 1.4.4)
$U = u(M)$ かつ $M = U \ltimes P$

命題 8.8. (*[GRUN 1980]* LEMMA 1.4.6)
$G \subseteq M$ であり、$N = G \cap U$

系 8.9.
G を $\mathbb{Q}$-群、$N = u(G)$ とするとき、$G = N \ltimes H$ となる reductive-complement が存在する。

命題 8.10. (*[GRUN 1980]* LEMMA 3.5.2)
$H' \subset M$ を M の部分群で $\mathbb{Q}$-群であり、reductive であるとする。このとき、ある $\lambda \in U_{\mathbb{Q}}$ が存在して $H' = P^{\lambda}$

となる。このとき $H = G \cap H' = G \cap P^{\lambda}$ となる。

これを用いて reductive-complement の算出を行うことができる。

アルゴリズム 8.11. (*[GRUN 1980]* ALGORITHM 3.5.3)
$H = G \cap H' = G \cap P^{\lambda}$ となる $\lambda \in U_{\mathbb{Q}}$ を計算する。

【手順】
$N = u(G)$ の reductive complement を求めるには命題 8.10 における λ を算出すればよい。λ が有理数成分の行列を動くことが問題であるが、$U_{\mathbb{Q}}$ は可算集合なのでその要素を $\lambda_0, \lambda_1, \ldots$ と列挙し、論理式
$\lambda_i \in U_{\mathbb{Q}} \wedge [\forall g \in G \exists x \in N \exists y \in P.\, g = x\lambda_i^{-1} y \lambda_i]$ ・・・(☆)
の真偽を QE によって決定する。命題 8.10 よりある i において QE の結果が真となるはずで、その λ_i が求めるべき λ である。

注 8.12. 論理式 (☆) は $\lambda_i \in U_{\mathbb{Q}}$ を固定すれば実数を変数とする一階の論理式なので QE によって真偽を決定することができる。$U_{\mathbb{Q}}$ の要素の列挙の方法は例えば、$(\mathbb{Z} \times (\mathbb{N} \setminus \{0\}))^{m^2}$ に辞書式順序を考えることで $\mathrm{M}_m(\mathbb{Q})$ の要素 λ を *(*重複はありうるが*)* 列挙できる。そのうち $\det\lambda = 0$ であるもの及び U を定義する多項式の根にならないものを除くことで $U_{\mathbb{Q}}$ の要素を列挙することができる。

8.3 $(G_{\mathbb{Z}})^{\mu} \subseteq (N^{\mu})_{\mathbb{Z}}(H^{\mu})_{\mathbb{Z}} \subseteq (G^{\mu})_{\mathbb{Z}}$ を満たす行列 μ の計算

$\mathbb{Q}$-群 G の arithmetic-subgroup の生成元を計算するために前節までの議論で $G = N \ltimes H$ と unipotent な部分と reductive な部分に分ける半直積分解を得た。$N_{\mathbb{Z}}$ の有限生成系は 9.1 節の議論で、$H_{\mathbb{Z}}$ の有限生成系は 9.2 節の議論で計算できるので、この生成系計算アルゴリズムを用いて一般の $\mathbb{Q}$-群 G に対してその arithmetic-subgroup の生成元を計算したい。生成系を計算するのに必要な $N_{\mathbb{Z}}$ と $H_{\mathbb{Z}}$ の有限生成系からなる語の長さに上界があるようにするために $(N^{\mu})_{\mathbb{Z}}(H^{\mu})_{\mathbb{Z}}$ が $G_{\mathbb{Z}}$ に対して適切な包含関係を満たすような基底変換行列 μ をする必要がある。本節ではこの行列 μ の計算アルゴリズムについて述べる。
G を $\mathbb{Q}$-群とし、$N = u(G)$, その reductivecomplement を H とする。また、$\mathcal{E}$ を N の centralflag,$\mathcal{B}$ を $\mathcal{E}$ の整基底とする.$M = M(\mathcal{E})$,$U = U(\mathcal{E})$,$P = P(\mathcal{E}, \mathcal{B})$ とする。この節では、行列 $\mu \in \mathrm{GL}_m(\mathbb{Q}) \cap \mathrm{M}_m(\mathbb{Z})$ であって,$(G_{\mathbb{Z}})^{\mu} \leq (N^{\mu})_{\mathbb{Z}}(H^{\mu})_{\mathbb{Z}} \leq (G^{\mu})_{\mathbb{Z}}$ となるような μ の算出アルゴリズムを述べる。

定義 8.13.
$\mathbb{R}^m$ の部分集合 Λ が格子であるとは、$\mathbb{R}^m$ の基底 $\{v_1, \ldots, v_m\}$ を用いて、$\Lambda = \{\sum_{i=1}^{m} a_i v_i \mid a_i \in \mathbb{Z}\}$ と書けることをいう。

定義 8.14.
n を 2 以上の整数とする。$\mathrm{GL}_m(\mathbb{Z})$ の n を法とする原始合同部分群 γ_n を $\gamma_n = \{A \in \mathrm{GL}_m(\mathbb{Z}) \mid a_{kk} \equiv 1 \bmod n,\ a_{ij} \equiv 0 \bmod n,\ (i \neq j)\}$ で定める。

命題 8.15. (*[GRUN 1980]* LEMMA 1.4.9)
$\lambda \in U_{\mathbb{Q}}$, $\mu \in \mathrm{GL}_m(\mathbb{Q}) \cap M_m(\mathbb{Z})$ に対して
$(U_{\mathbb{Z}})^{\mu}((P^{\lambda})_{\mathbb{Z}})^{\mu} \subseteq (M_{\mathbb{Z}})^{\mu} \subseteq (U^{\mu})_{\mathbb{Z}}(P^{\lambda\mu})_{\mathbb{Z}}$
が成り立っているとする。このとき、

$(G_{\mathbb{Z}})^{\mu} \subseteq (N^{\mu})_{\mathbb{Z}}(H^{\mu})_{\mathbb{Z}} \subseteq (G^{\mu})_{\mathbb{Z}}$
がなりたつ。

前節で算出した λ から上記命題の条件を満たすような μ を計算することができればそれが求めるべき μ である。

アルゴリズム 8.16. (*[GRUN 1980]* ALGORITHM 3.5.4)
上記命題の条件を満たすような μ を計算する。すなわち
$\lambda \in U_{\mathbb{Q}}$ を入力として、
$(U_{\mathbb{Z}})^{\mu}((P^{\lambda})_{\mathbb{Z}})^{\mu} \subseteq (M_{\mathbb{Z}})^{\mu} \subseteq (U^{\mu})_{\mathbb{Z}}(P^{\lambda\mu})_{\mathbb{Z}}$
を満たす $\mu \in \mathrm{GL}_m(\mathbb{Q}) \cap M_m(\mathbb{Z})$ を算出する。(入力 λ はアルゴリズム *8.10* によって算出される λ を想定している)

【手順】
STEP1:$\lambda \in U_{\mathbb{Q}}$ に対して $e\lambda, e\lambda^{-1} \in M_m(\mathbb{Z})$ となる $e \in \mathbb{N}$,$\mathbb{Z}^m \subseteq \Lambda \subseteq e^{-2(k-1)}\mathbb{Z}^m$ かつ $\Lambda = U_{\mathbb{Z}}\Lambda = P_{\mathbb{Z}}\Lambda = (P_{\mathbb{Z}})^{\lambda}\Lambda$ を満たす格子 Λ(の基底) を求める。但し k は N の centralflag $\mathcal{E}$ の長さである。格子 Λ を求めるには、$\mathbb{Z}^m \subseteq \Lambda \subseteq e^{-2(q-1)}\mathbb{Z}^m$ を満たす格子 Λ について、$\Lambda = U_{\mathbb{Z}}\Lambda = P_{\mathbb{Z}}\Lambda = (P_{\mathbb{Z}})^{\lambda}\Lambda$ が成り立つかどうかを判定しなければならない。$\Lambda = U_{\mathbb{Z}}\Lambda, \Lambda = P_{\mathbb{Z}}\Lambda, \Lambda = (P_{\mathbb{Z}})^{\lambda}\Lambda$ のそれぞれについて、以下のようにして判定を行う。([GRUN 1980] pp563 (iii))

$\Lambda = U_{\mathbb{Z}}\Lambda$: $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_m$ を N の整基底とし、i 行目が $\boldsymbol{e}_i^{\top}$ であるような行列 $\beta \in \mathrm{GL}_m(\mathbb{Z})$ を考えると、$\beta U_{\mathbb{Z}}\beta^{-1} = \{g \in \mathbb{U} \cap \mathrm{M}m(\mathbb{Z}) \mid g_{ij} = 0\ (r_{i-1} < i < j \leq r_i), (i = 1, \ldots, k)\}$ であるから $U_{\mathbb{Z}}$ を法 $e^{2(k-1)}$ の原始合同部分群で割った剰余群の代表系 T を算出することができる.$\Lambda = U_{\mathbb{Z}}\Lambda \Leftrightarrow \forall x \in T.\, x^{\top}\Lambda \subseteq \Lambda$ なのでこれは有限の手続きでチェックできる。

$\Lambda = P_{\mathbb{Z}}\Lambda$: ,$\beta P_{\mathbb{Z}}\beta^{-1} = \mathrm{diag}(\mathrm{GL}_{r_1}(\mathbb{Z}), \mathrm{GL}_{r_2-r_1}(\mathbb{Z}), \ldots, \mathrm{GL}_{r_k-r_{k-1}}(\mathbb{Z}))$ である。$i = 1, \ldots, k$ に対して $\sigma_i : \mathbb{Q}^m \to \mathbb{Q}^{r_i-r_{i-1}}$ を第 $r_{i-1}+1$ 成分から第 r_i 成分までを射影する写像とすると、$\Lambda = P_{\mathbb{Z}}\Lambda \Leftrightarrow \sigma_i((\beta^{-1})^{\top}\Lambda)$ が群 $\mathrm{GL}_{r_i-r_{i-1}}$ 上不変 $\Leftrightarrow \exists m_i \in \mathbb{Q}\, \sigma_i((\beta^{-1})^{\top}\Lambda) = m_i\mathbb{Z}^{r_i-r_{i-1}}\ (i = 1, \ldots, k)$ であり最後の条件は $\sigma_i((\beta^{-1})^{\top}\Lambda)$ の基底を調べることで確かめることができる。

$\Lambda = (P_{\mathbb{Z}})^{\lambda}\Lambda$: Λ を $\lambda^{\top}\Lambda$ に置き換えて前項目のステップを踏めばよい。

STEP2:STEP1 で求めた Λ に対して $\mu\Lambda = \mathbb{Z}^m$ を満たす μ を求めればこれが求めるべき μ である。

9 arithmetic-subgroup の生成元計算

9.1 unipotent な $\mathbb{Q}$-群 N における $N_{\mathbb{Z}}$ の生成元の計算

注 8.5 により unipotent な $\mathbb{Q}$-群 $N \subseteq \mathrm{GL}_m(\mathbb{C})$ はその整基底による基底変換で $\mathbb{U}$ の部分群とみなせる。以下 $N \subseteq \mathbb{U}$ と仮定する。

定義 9.1.
$\delta > 0$ に対して、
$B_{\delta} = \{g \in \mathrm{GL}_m(\mathbb{R}) \mid \det g = 1, |g_{ij} - \delta_{ij}| < \delta\}$
と定める。但し、δ_{ij} はクロネッカーのデルタである。

定義 9.2.
$i = 1, \ldots, m$ に対して N の部分群 $N^{(i)}$ を対角成分の上 $i-1$ 個以上が 0 である行列からなる部分群と定める。(例えば $N^{(1)} = N, N^{(m)} = \{I_m\}$ である) $\mathcal{L}_{\mathbb{Q}}(N^{(i)})$ の基底を $\{a_1^{(i)}, \ldots, a_{t_i}^{(i)}\}$ と書く。

アルゴリズム 9.3. (*[GRUN 1980]* ALGORITHM 4.2.1)
$N_{\mathbb{R}} = (N \cap B_\Delta \cdot N_{\mathbb{Z}})$ を満たす正の有理数 Δ を算出する。

【手順】
STEP1:$i = 1, \ldots, m$ に対して、$m_i = \frac{1}{2}\max_{j=1,\ldots,t_i}\{a_j^{(i)}$ の成分の絶対値 $\} \cdot t_i$ を計算する。
STEP2: 行列 $M_i = \begin{pmatrix} m_i & \cdots & m_i \\ \vdots & \ldots & \vdots \\ m_i & \cdots & m_i \end{pmatrix}$ について $\exp M_i$ を計算する。$\exp(M_i)$ の成分の絶対値を上から抑える正の有理数 β_i をとる。
STEP3: 正の有理数 Δ_i を漸化式
$$\begin{cases} \Delta_1 = \beta_1 \\ \Delta_i = \beta_i + (n-i-1)\Delta_{i-1}\beta_i + \Delta_{i-1} \end{cases}$$
によってさだめ、$\Delta = \Delta_{n-1}$ とする。

アルゴリズム 9.4. (*[GRUN 1980]* ALGORITHM 4.2.2)
アルゴリズム *9.3* で求めた Δ に対して

- $I_m \in F_1(\Delta) = F_1(\Delta)^{-1}$
- $F_1(\Delta) \supseteq B_\Delta^{-1} B_\Delta \cap \mathrm{GL}_m(\mathbb{Z})$

を満たす有限集合 $F_1(\Delta) \subseteq \mathrm{GL}_m(\mathbb{Z})$ を算出する。

【手順】
STEP1:$\Delta' = m!(1+\Delta)^m + 1$ とおき、F を $|g_{ij} - \delta_{ij}| < \Delta'$ を満たす行列 $g \in \mathrm{GL}_m(\mathbb{Z})$ の集合とする。
STEP2:$F_1(\Delta) = F \cup F^{-1}$ とする。

以下の命題が成り立つため、これで $N_{\mathbb{Z}}$ の生成元を算出することができる。

命題 9.5. (*[GRUN 1980]* PROPOSITION 1.5.4)
$F_1(\Delta) \cap N_{\mathbb{Z}}$ は $N_{\mathbb{Z}}$ の生成系である。

9.2 reductuve な $\mathbb{Q}$-群 H における $H_{\mathbb{Z}}$ の生成元の計算

定義 9.6.
$H \subseteq \mathrm{GL}_m(\mathbb{C})$ を reductive な $\mathbb{Q}$-群であるとする。$H_{\mathbb{R}} = H \cap \mathrm{GL}_m(\mathbb{R})$ が自己随伴 (self-adjoint) であるとは、$x \in H_{\mathbb{R}} \Rightarrow x^{\mathrm{T}} \in H_{\mathbb{R}}$ が成り立つことをいう。

アルゴリズム 9.7. $H = \mathcal{Z}(\mathfrak{a}) \cap \mathrm{GL}_m(\mathbb{C})$ を reductuve な $\mathbb{Q}$-群とする。
$H_{\mathbb{R}}^{\xi}$ *is* self-adjoint になるような $\xi \in \mathrm{GL}_m(\mathbb{R})$ を近似的に算出する。

【手順】$[\forall g \in H_{\mathbb{R}}.\, \xi(\xi^{-1}g\xi)^{\top}\xi^{-1} \in H]$ を QE で探索。

定義 9.8.
F を体とする。行列の形をした不定元 $X = (X_{ij})$ $(1 \leq i, j \leq m)$ を考え、$F[X] = R[X_{11}, \ldots, X_{mm}]$ とかく。また、$F[X_{11}, \ldots, X_{mm}, (\det X)^{-1}] \subseteq F(X_{11}, \ldots, X_{mm})$ のことを $F[X, (\det X)^{-1}]$ と書く。

定義 9.9.
係数が *1* の単項式たちの集まり $\{X_{11}^{e_{11}} \cdots X_{mm}^{e_{mm}} \,|\, (e_{11}, \ldots, e_{mm}) \in \mathbb{N}^{m^2}\}$ に対して $\mathbb{N}^{m^2}$ における辞書式順序によって順序を定める。この順序を辞書式単項式順序と呼ぶ.

定義 9.10.
$g \in \mathrm{GL}_m(\mathbb{C})$ に対して、$g \cdot (\det X)^{-m} f(X) = (\det gX)^{-m} f(gX)$ によって作用を定義する。

定義 9.11.
斉次多項式 $f_1, \ldots, f_q \in \mathbb{Z}[X_{11}, \ldots, X_{mm}]$ に対して組 $Q = ((\det X)^{-m_1} f_1(X), \ldots, (\det X)^{-m_q} f_q(X))$ を考える。f_i の次数を d_i とおく。

定義 9.12.
$e = (e_{11}, \ldots, e_{mm}) \in \mathbb{N}^{m^2}$ に対して X^e で単項式 $X_{11}^{e_{mm}} \cdots X_{11}^{e_{mm}}$ を表す。

定義 9.13.
係数が *1* で次数が d_i の単項式の個数, 即ち集合 $W_{d_i} = \{X_{11}^{e_{mm}} \cdots X_{11}^{e_{mm}} | \sum_{r,s} e_{rs} = d_i\}$ の集合の要素の個数を t_i とおく。W_{d_i} を辞書式単項式順序で並べて r 番目に来る単項式を X^{e_r} で表し, これを r 番単項式と呼ぶ。

定義 9.14.
$\theta_i : \mathrm{GL}_m(\mathbb{C}) \to \mathrm{GL}_{t_i}(\mathbb{C})$ を $g \in \mathrm{GL}_m(\mathbb{C})$ そのを rs 成分が $(\det g)^{-m_i} c_{rs}$ であるような行列 $(\theta_i(g))$ に送る写像として定める。ただし、c_{rs} は $(gX)^{e_r}$ を展開した際の s 番単項式の係数とする。

定義 9.15.
$Q = ((\det X)^{-m_1} f_1(X), \ldots, (\det X)^{-m_q} f_q(X))$ に対して $t_1 + \cdots + t_q = m_Q$ とおく。$\theta_Q : \mathrm{GL}_m(\mathbb{C}) \to \mathrm{GL}_{m_Q}(\mathbb{C})$ を $\theta_Q(A) = \mathrm{diag}(\theta_1(A), \ldots, \theta_q(A))$ で定める。

定義 9.16.
ベクトル $v_Q \in \mathbb{Z}^{m_Q}$ をその第 $t_1 + \cdots + t_{i-1} + j$ 成分 $(1 \leq j \leq t_i)$ が $f_i(X)$ の j 番単項式の係数であるようなものとして定める。

ここで、与えられた reductuve な $\mathbb{Q}$-群 H について、$H_{\mathbb{Z}}$ の生成系を算出するアルゴリズムについて記述する。

アルゴリズム 9.17. (*[GRUN 1980]* Algorithm 5.3.1)
与えられた reductuve な $\mathbb{Q}$-群 H について、$H_{\mathbb{Z}}$ の生成系を算出する。

【手順】
STEP A: H^{ξ} が self-adjoint になるような $\xi \in \mathrm{GL}_m(\mathbb{R})$ をアルゴリズム 9.7 近似的に得る。
STEP B: アルゴリズム 9.19、9.20、9.21 により以下条件を満たす $Q, m_Q, v^{(Q)}, \theta_Q$ を得る。

(i) $v_Q^\top\theta_Q(\mathrm{GL}_m(\mathbb{C}))$ が $\mathbb{C}^{m_Q}$ のザリスキ位相で閉集合

(ii) $U=(U_{ij})_{1\le i,j\le m}$ を X と異なる不定元として、$h_{i,Q}=f_i(XU)-(\det X)^{m_i}f_i(U)\in(\mathbb{Z}[X])[U]$ $(i=1,\dots,q)$ を考える。イデアル $\mathfrak{b}\subseteq\mathbb{Q}[X]$ を $h_{i,Q}$ $(i=1,\dots,q)$ の係数たちで生成されるイデアルとする。このとき $H=\mathcal{Z}(\mathfrak{b})\cap\mathrm{GL}_m(\mathbb{C})$ となる。

STEP C: STEPB で得られた Q に対してアルゴリズム 9.23 によって $v_Q^\top\theta(\xi\mathfrak{Q}_{t,u})\cap\mathbb{Z}^{m_Q}$ のベクトルの成分の絶対値の上界になる自然数 c を計算する。

STEP D:K をユークリッド位相における $H_{\mathbb{R}}$ の連結成分のうち単位行列を含むものとする。$H_{\mathbb{R}}$ の K における右剰余類の代表元 $y_1,\dots,y_s$ を得る。

STEP E: 有理数 $t>\frac{2}{\sqrt{3}}, u>\frac{1}{2}$ を任意にとっておく。有限集合 $F_3(t,u)$ をアルゴリズム 9.29 によって算出する。

STEP F:STEP E でとっていた有理数 $t>\frac{2}{\sqrt{3}}, u>\frac{1}{2}$ に対して、$\frac{2}{\sqrt{3}}<t'<t$, $\frac{1}{2}\le u'<u$ である有理数 t',u' を新たにとる。各 y_i $(i=1,\dots,s)$ に対して $\exists f_i\in F_{4,i}[\xi^{-1}y_if_i\in\mathfrak{Q}_{t',u'}]$ を満たす有限集合 $F_{4,i}$ をアルゴリズム 9.30 によって算出する。

$q=(2c+1)^{m_Q}$、$F_5=\cup_{i=1}^s F_3^{q-1}F_{4,i}^{-1}$ とすると、有限集合 $F_5^{-1}F_3F_5\cap H_{\mathbb{Z}}$ が $H_{\mathbb{Z}}$ の生成系である。

アルゴリズム 9.17 の STEP B ～ STEP F については項を分けて以下詳細を記述する。

STEP B：条件 (i)、(ii) の確認アルゴリズム

定義 9.18.

$A=\mathbb{C}[Y_1,\dots,Y_{m_Q}]$ とする。$f\in A$ に対して写像 $\chi:\mathrm{GL}_m(\mathbb{C})\to\mathbb{C}$ を $\chi(A)=f(v_Q^\top\theta_Q(A))$ によって定める。$\chi(A)$ は $a_{11},\dots,a_{mm},(\det A)^{-1}$ の多項式で表せ、したがってこれは $\mathbb{C}[X,(\det X)^{-1}]$ の要素を定める。$\psi_Q(f)$ を $\chi(X)$ が定める $\mathbb{C}[X,(\det X)^{-1}]$ の要素とすることで準同型 $\psi_Q:A\to R'$ を定める。

アルゴリズム 9.19.

$\mathrm{Ker}\psi_Q$ の生成系 $\phi_0,\phi_1,\dots,\phi_l$ を求める。

【手順】

$B=\mathbb{Q}[Y_1,\dots,Y_{m_Q}]$ とおくとこれは可算集合なので要素を列挙することができる。B の要素を順に列挙し、$\mathrm{Ker}\psi_Q$ に入っているかをしらべることで列 $\phi_0,\phi_1,\dots\subseteq\mathrm{Ker}\psi_Q$ を得ることができる.$l\in\mathbb{N}$ に対して $P_l=\sum_{j=0}^l\phi_jB$ を考え, これが

■素イデアルである

■次元がちょうど $\dim(\mathrm{GL}_m(\mathbb{C}))-\dim(\theta^{-1}(\mathrm{Stab}_{GL_{m_Q}(\mathbb{C})}v_Q))$

を満たすとき、$\phi_0,\phi_1,\dots,\phi_l$ が求めるべき生成系である。($\theta^{-1}(\mathrm{Stab}_{GL_{m_Q}(\mathbb{C})}v_Q)$ は $\mathbb{Q}$-群なので次元を計算できる。)

アルゴリズム 9.20.

(i) の条件をチェックする。

【手順】

$\mathrm{Ker}\psi_Q$ の生成系 $\phi_0,\phi_1,\dots,\phi_l$ に対して、

$\exists a\in\mathbb{C}^{m_Q}.[(\phi_1(a)=0\wedge\cdots\wedge\phi_l(a)=0)\wedge\neg(\exists g\in\mathrm{GL}_m(\mathbb{C})v_Q^\top\theta_Q(g)=a)]$ を QE で判定する。これが

FALSE になったとき (i) の条件が真になる。

アルゴリズム 9.21.
(ii) の条件をチェックする。

【手順】
$H = \mathcal{Z}(\mathfrak{a}) \cap \mathrm{GL}_m(\mathbb{C})$ とする。(ii) の条件は $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{b}}$ と同値なのでこれを判定すればよい。イデアルの根基の素イデアル分解を準素分解パッケージ計算することでイデアルの根基は計算でき、その被約グレブナー基底を計算し比較することで $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{b}}$ かどうかの判定ができる。(命題 2.52、命題 2.58)

定義 9.22.
$\delta > 0$ に対して、
$B'_\delta = \{g \in \mathrm{M}_m(\mathbb{R}) \mid |g_{ij} - \delta_{ij}| < \delta\}$
$A_\delta = \{\mathrm{diag}(a_1, \ldots, a_m) \mid 0 < a_i \leq \delta a_{i+1} \text{ for } 1 \leq i \leq m\}$
$N_\delta = \{A \in \mathrm{M}_m(\mathbb{R}) \mid a_{ii} = 1 \text{ for } 1 \leq i \leq m, |a_{ij}| \leq \delta \text{ for } 1 \leq i < j \leq m\}$ と定める。

STEP C：ベクトルの成分の絶対値の上界になる自然数 c の算出
アルゴリズム 9.23. (*[GRUN 1980]* Algorithm 5.2.1)
$v_Q^\top \theta(\xi \mathfrak{Q}_{t,u}) \cap \mathbb{Z}^{m_Q}$ のベクトルの成分の絶対値の上界になる自然数 c を算出する.

【手順】
STEP1:$\forall a \in A_t, \forall b \in N_u . aba^{-1} \in N_{c(1)} \wedge a^2 b (a^{-1})^2 \in N_{c(3)}$ を満たす有理数 $c(1), c(3)$ を QE により算出する。
STEP2:$\forall k \in O_m(\mathbb{R}), \forall b \in N_{c(1)} . ||\psi^*(\xi k b)|| \leq c(2)$ を満たす有理数 $c(2)$ を QE により算出する。
STEP3:$\eta = c(2)^2 + \max_{1 \leq i \leq m_Q} |v_i^{(Q)}|$ とおき、以下の条件を満たす正の有理数 δ と有限個の行列 $g_1, \ldots, g_l \in \mathrm{GL}_m(\mathbb{Q})$ を算出する。
(条件)$\forall g \in B_\delta . |\det g| \geq \frac{1}{2} \wedge B'(v^{(Q)}, \eta) \cap Y \subseteq \psi^*(\cup_{i=1}^l B_\delta g_i)$
STEP4:g を $\cup_{i=1}^l (\xi \xi^\top B_\delta^{-1} (g_i^{-1})^\top N_{c(3)}^\top N_u)$ の範囲で動かした際の $\psi^*(g)$ の成分の絶対値を上からおさえる自然数 c を算出する. これが求めるべき c である。

アルゴリズム 9.23 の STEP3 の部分は以下のアルゴリズムで計算できる。

アルゴリズム 9.24. (*[GRUN 1980]* Algorithm 5.2.2)
与えられた正の有理数 η に対してアルゴリズム *9.23STEP3* の条件を満たす正の有理数 δ と有限個の行列 $g_1, \ldots, g_l \in \mathrm{GL}_m(\mathbb{Q})$ を算出する。

【手順】
STEP1:$\forall g \in B'_\delta [|\det g| \geq \frac{1}{2}]$ を満たす正の有理数 δ を算出する。算出のためには QE により δ を実数の範囲で近似的に求め、それよりも大きい有理数を δ とすればよい。
STEP2: 自然数 k に対して $Y_k = Y \cap B'(v^{(Q)}, k^{-1})$ と定める。Y_k

定義 9.25.

$S \subseteq \{1, \ldots, m\}$ に対して、
$\eta_S = \mathrm{diag}(\epsilon_1, \ldots, \epsilon_m)$
$\bar{\eta}_S = \mathrm{diag}(\delta_1, \ldots, \delta_m)$
と定める。ただし、$i \notin S$ に対して $\epsilon_i = 1$, $\delta_i = 0$, $i \in S$ に対して $\epsilon_i = -1$, $\delta_i = 1$ とする。

STEP D：$H_{\mathbb{R}}$ の $K_{\mathbb{R}}$ における右剰余類の代表元集合の計算アルゴリズム

アルゴリズム 9.26.
H を reductuve な $\mathbb{Q}$-群とする。$H_{\mathbb{R}}$ のユークリッド位相での連結成分であって単位行列を含むものを K とする。$H_{\mathbb{R}}$ の $K_{\mathbb{R}}$ における右剰余類の代表元集合 $X = \{h_1, \ldots, h_a\}$ を近似的に算出する。

【手順】
STEP1:H^0 を計算する。(この H^0 は定義 7.17 に従ったノーテーションである.)
STEP2:$H_{\mathbb{R}}$ の $(H^0)_{\mathbb{R}}$ における右剰余類の代表元集合 $Y = \{h'_1, \ldots, h'_{a'}\}$ を近似的に算出する。
STEP3:$(H^0)_{\mathbb{R}}$ の K における右剰余類の代表元集合 $Z = \{h''_1, \ldots, h''_{a''}\}$ を近似的に算出する。
以上から、$X = YZ = \{yz \mid y \in Y, z \in Z\}$ と計算できる。

STEP2、STEP3 の計算はそれぞれアルゴリズム 9.27、9.28 で行う。

アルゴリズム 9.27.
H を reductuve な $\mathbb{Q}$-群とする。$H_{\mathbb{R}}$ の $(H^0)_{\mathbb{R}}$ における右剰余類の代表元 $h'_1, \ldots, h'_{a'}$ を近似的に算出する。

【手順】
$l \in \mathbb{N}$ を固定し $t_1, \ldots, t_l$ を $m \times m$ 行列の形の不定元とする。$P(t_1, \ldots, t_l)$ を $\forall x \in H_{\mathbb{R}} \exists y \in (H^0)_{\mathbb{R}}[x = yt_1 \vee x = yt_2 \vee \cdots x = yt_l]$ を表すステートメントとする。$\exists t_1, \ldots, t_l \in H_{\mathbb{R}} P(t_1, \ldots, t_l)$ の真偽は QE により決定することができ、これが真になる l が $|H_{\mathbb{R}} : \Gamma(H^0)_{\mathbb{R}}|$ であり、$P(g_1, \ldots, g_l)$ が真になる行列 $g_1, \ldots, g_l$ が求めるべき代表元である。これは QE によって近似的に得ることができる。

アルゴリズム 9.28. (*[GRUN 1980]* Algorithm 3.3.5)
H を reductuve な $\mathbb{Q}$-群とする.$H_{\mathbb{R}}$ のユークリッド位相での連結成分であって単位行列を含むものを K とする。$(H^0)_{\mathbb{R}}$ の K における右剰余類の代表元 $h''_1, \ldots, h''_{a''}$ を近似的に算出する。

【手順】
STEP1:$\mathcal{L}_{\mathbb{Q}}(H^0)$ の基底 $\{b_1, \ldots, b_k\} \subseteq M_m(\mathbb{Q})$ を計算する。
STEP2:X を $m \times m$ 行列、$Y^{(l)}$ を $l \times k$ 行列の形をした変数として論理式 $P_l(X, Y^{(l)})$ を「$\det X \neq 0 \wedge \mathrm{rank} Y^{(l)} = l \wedge X^{-1}(\sum_{j=1}^{k} Y_{ij}^{(l)} a_j)X$ がすべての $i = 1, \ldots, l$ で対角行列」を表したものとする。$Q_l(X, Y^{(l)})$ で命題 $\exists X \in \mathrm{M}_m(\mathbb{R}), \exists Y^{(l)} \in \mathbb{R}^{l \times k} P_l(X, Y^{(l)})$ を指す。各 $l = 1, \ldots, k$ に対して $Q_l(X, Y^{(l)})$ の真偽を QE で決定し、真になる l のうち最大のものを r とする。
STEP3:$S_1, \ldots, S_{2^r} \subseteq \{1, \ldots, m\}$ を相異なる部分集合とし、$C = \{S_1, \ldots, S_{2^r}\}$ とする. ステートメント「$\exists Y^{(r)} \in \mathbb{R}^{r \times k}[P_r(X, Y^{(r)})$ かつ各 $S \in C$ について、$\bar{\eta}_S$ が $\{X^{-1}(\sum_{j=1}^{k} Y_{ij}^{(r)} b_j)X \mid i = 1, \ldots, r\}$ で生成される実ベクトル空間の元になる。]」を $T_C(X)$ で表す。C を固定すれば $\exists X T_C(X)$ の真偽は QE で決定でき、真になる C において $T_C(\alpha)$ を満たす。$\alpha \in \mathrm{GL}_m(\mathbb{R})$ を近似的に得ることができる。$\eta_{S_1}^{(\alpha^{-1})}, \ldots, \eta_{S_{2^r}}^{(\alpha^{-1})}$ が求めるべき代表元である。

STEP E：有限集合 $F_3(t,u)$ の計算アルゴリズム

アルゴリズム 9.29. (*[GRUN 1980]* Algorithm 4.1.1)
与えられた $t,u>0$ に対して、有限集合 $F_3(t,u)=\{g\in \mathrm{GL}_m(\mathbb{Z}) \mid \mathfrak{Q}_{t,u}g\cap\mathfrak{Q}_{t,u}\neq\emptyset\}$ を算出する。

【手順】
STEP1:$M_1(t,u)=(t^2)(1+u^2\sum_{j=1}^{m-1}t^{2j})$
$M_2(t,u)=\max\{\sqrt{M_1(t,u)},\frac{1}{2}\sqrt{\sum_{j=1}^{m-1}t^{2j}}\}$
$M_3(t,u)=m!M_2^m(1+u)^{m^2}$
を計算する。
STEP2: 有限集合 $F=\{g\in \mathrm{GL}_m(\mathbb{Z}) \mid |g_{ij}|\leq M_3(t,u)\}$ から要素 g を 1 つずつとり、以下の命題の真偽を QE により確認する。

- $\exists k,k'\in O_m(\mathbb{R})$
- $\exists a,a'\in A_t$
- $\exists x,x'\in N_u$. $kaxg=k'a'x'$

STEP3:STEP2 で真になった g たちを集めた集合を $F_3(t,u)$ とする。

STEP F：有限集合 $F_4(t,u,x)\subseteq \mathrm{GL}_m(\mathbb{Z})$ の計算アルゴリズム

アルゴリズム 9.30. (*[GRUN 1980]* Algorithm 4.1.2)
$t>\frac{2}{\sqrt{3}},u\geq\frac{1}{2}$ が与えられており、また $x\in \mathrm{GL}_m(\mathbb{R})$ が近似的に与えられているとする。このとき、以下の条件を満たす有限集合 $F_4(t,u,x)\subseteq \mathrm{GL}_m(\mathbb{Z})$ を算出する。
*(*条件*)* 少なくとも一つの $f\in F_4(t,u,x)$ について $xf\in\mathfrak{Q}_{t,u}$ がなりたつ。

【手順】
STEP1:$x^\top x$ の固有値の下界となる正の有理数 $\epsilon>0$ を算出する。
STEP2: ノルムが $\epsilon^{-1}||x_1||$ 以下であり primitive なベクトル $\boldsymbol{z}\in\mathbb{Z}^m$ をすべて列挙する。
STEP3:STEP2 で列挙したベクトル $\boldsymbol{z}$ それぞれについて、これを 1 列目に持つ行列 $Z\in \mathrm{GL}_m(\mathbb{Z})$ を構成する、こうして得られた行列たちの集合を $F_4(t,u,x)$ とする。

9.3 arithmetic-subgroup と $\mathrm{GL}_m(\mathbb{Z})$ の共通部分の生成系計算アルゴリズム

以上をサブルーチンとして用いて以下のアルゴリズムで arithmetic-subgroup の生成系を計算することができる.

アルゴリズム 9.31. (*[GRUN 1980]* Algorithm B)
$G\in \mathrm{GL}_m(\mathbb{C})$ を $\mathbb{Q}$-群、$\Gamma\subset G$ をその arithmetic-subgroup として以下条件
1. $\mathbb{Q}$-群 G を定める多項式 $f_1,\ldots,f_s\in\mathbb{Q}[X_{11},\ldots,X_{mm}]$ が与えられている。
G の arithmetic-subgroup Γ について、

2. $|\Gamma : G \cap \mathrm{GL}_m(\mathbb{Z})| < \infty$ でありかつその上界が与えられている。
3. 各 $g \in G \cap \mathrm{GL}_m(\mathbb{Z})$ に対して $g \in \Gamma$ かどうかを判定するためのアルゴリズムが存在する。
を満たす場合に arithmetic-subgroup Γ の有限生成系を計算する。

【手順】
STEP1:G^0 を計算する、すなわち $G^0 = \mathcal{Z}(g_1, \cdots, g_s) \cap \mathrm{Gl}_m(\mathbb{C})$ となる多項式 $g_1, \cdots, g_s$ を算出する。
STEP2:$N = u(G)$,N の reductive complement H, 行列 $\mu \in \mathrm{GL}_m(\mathbb{Q}) \cap \mathrm{M}_m(\mathbb{Z})$ であって、$(G_{\mathbb{Z}})^{\mu} \leq (N^{\mu})_{\mathbb{Z}}(H^{\mu})_{\mathbb{Z}} \leq (G^{\mu})_{\mathbb{Z}}$ となるような μ の算出。ここで、$u(G)$ が連結であることから $u(G) = u(G^0)$ である.$u(G)$ を算出アルゴリズムの議論で G が連結であることが仮定されているため、STEP1 で G^0 を算出する必要がある。
STEP3:$(N^{\mu})_{\mathbb{Z}}$,$(H^{\mu})_{\mathbb{Z}}$ の有限生成系 X_1, X_2 をそれぞれ算出する.
ここで、$A = (N^{\mu})_{\mathbb{Z}}(H^{\mu})_{\mathbb{Z}}$ とおく.
A は有限集合 $Y = (X_1 \cup X_2)^{\mu^{-1}}$ で生成されかつ Γ を含んでいる。ここで A を Γ で割った右剰余類の集合を T とおくと Γ は $TYT^{-1} \cap \Gamma$ で生成されることが [MKS 1966] の Theorem2.7 の議論からわかる。
STEP4:$D \geq |A : \Gamma|$ なる数 D をひとつとり、Y の要素の D 個以下の積の集まり $W_D(Y) = \cup_{i=1}^{D}\{A_1 \cdots A_i | A_j \in Y\}$ を考える。D の定義の仕方から $W_D(Y)$ の要素で各右剰余類をとりつくすことができるので、$W_D(Y) \cap \Gamma$ は Γ を生成する。

10 二次ディオファントス方程式の可解性判定アルゴリズム

この章では、二次ディオファントス方程式 (1) の可解性判定アルゴリズムについて述べる。二次形式が singular な場合については簡単 (1 節、2 節) であり、regular な場合についてがメインとなる。$\mathbb{Z}$ 上の二次形式 $Q(\boldsymbol{x}) = \boldsymbol{x}^{\top} A \boldsymbol{x}$ が regular な場合、以下の命題で方程式 (1) の可解性を判定できる。

命題 10.1. (*[GRUN 1981]* PROPOSITION 1)
$d = \det A, \boldsymbol{h} = \tilde{A}\boldsymbol{b}, c^* = 4d^2c + Q(\boldsymbol{h})$ とおくと、
方程式 (*1*) が整数解 $\boldsymbol{x} \in \mathbb{Z}^m$ をもつ $\Leftrightarrow$ $\exists \boldsymbol{z} \in \mathbb{Z}^m\, (Q(\boldsymbol{z}) = c^* \wedge \boldsymbol{z} = \boldsymbol{h} \pmod{2d})$

【証明】
$\boldsymbol{x}^{\top} A\boldsymbol{h} = \boldsymbol{x}^{\top} A\tilde{A}\boldsymbol{b} = dL(\boldsymbol{x})$,$Q(2d\boldsymbol{x} + \boldsymbol{h}) = 4d^2(Q(\boldsymbol{x}) + L(\boldsymbol{x})) + Q(\boldsymbol{h})$ なので
$Q(\boldsymbol{x}) + L(\boldsymbol{x}) = c \Leftrightarrow Q(2d\boldsymbol{x} + \boldsymbol{h}) = c^*$

この命題を軸に可解性判定アルゴリズムは記述される。

10.1 $A = O$ の場合

$A = O$ の場合方程式 (1) は 1 次ディオファントス方程式になる。1 次ディオファントス方程式はユークリッドの互除法を一般化した議論により解くことができる。まず整数解の有無自体は以下の命題により容易に判定できる、

命題 10.2.
整数 $a_1, \cdots, a_n$ で生成される $\mathbb{Z}$ のイデアル $I = \langle a_1, \cdots, a_n \rangle$ は $\gcd(a_1, \cdots, a_n)$ で生成される単項イデアルである。したがって、
1 次ディオファントス方程式 $b_1x_1 + \cdots + b_mx_m = c$ が整数解をもつ $\Leftrightarrow$ c が $\mathrm{g.c.d}(b_1, \cdots, b_m)$ の倍数

解が存在する場合解の媒介変数表示を計算することができる。2 変数 1 次ディオファントス方程式については以下のやり方で解の媒介変数表示を得ることができる。

命題 10.3.
2 変数 1 次ディオファントス方程式 $ax + by = 1$ $(\gcd(a, b) = 1)$ が整数解 (x_0, y_0) を持つとする。この方程式のすべての解を媒介変数 t の 1 次式で表すことができる。

【証明】
(x, y) が解であれば、
$$\begin{cases} ax + by = 1 \\ ax_0 + by_0 = 1 \end{cases}$$
から辺々引いて $a(x - x_0) + b(y - y_0) = 0$ を得ることができる。$\gcd(a, b) = 1$ であることから、整数 $t \in \mathbb{Z}$ を用いて $x - x_0 = -bt, y - y_0 = at$ とかける。逆に任意の $t \in \mathbb{Z}$ に対して $x = x_0 - bt, y = y_0 + at$ とおくと、$ax + by = a(x_0 - bt) + b(y_0 + at) = ax_0 + by_0 = 1$ となり (x, y) が解であることがわかる。
2 変数の場合をもとに帰納法で 3 変数以上の 1 次ディオファントス方程式も解の媒介変数表示を得ることができる。

命題 10.4.
方程式 $b_1x_1 + b_2 + \cdots + b_mx_m = c$ $((b_1, \ldots, b_m) \neq (0, \ldots, 0))$ に整数解が存在する場合、$x_i = a_{0i} + s_1a_{1i} + \cdots + s_ka_{ki}$ と媒介変数 $s_i \in \mathbb{Z}$ の一次式で一般解を表せる。

【証明】
$b_1, \ldots, b_m$ のうち b_j が絶対値最小とする。
$b_1 = q_1b_j + r_1, \cdots, b_{j-1} = q_{j-1}b_j + r_{j-1}, b_{j+1} = q_{j+1}b_j + r_{j+1}, \cdots, b_m = q_mb_j + r_m$ $(0 \leq r_i < |b_j|)$ とすると,$b_1x_1 + b_2 + \cdots + b_mx_m = b_j(x_m + q_1x_1 + \cdots + q_mx_m) + r_1x_1 + \cdots + r_mx_m$,
$a_1^{(1)} = b_j, a_2^{(1)} = r_1, \ldots, a_m^{(1)} = r_m, X_1^{(1)} = x_m + q_1x_1 + \cdots + q_mx_m, X_2^{(1)} = x_1, X_3^{(1)} = x_2, \ldots, X_m^{(1)} = x_m$ とおくと,$b_1x_1 + b_2 + \cdots + b_mx_m = a_1^{(1)}X_1^{(1)} + \cdots + a_m^{(1)}X_m^{(1)}$ となる。同様の操作を繰り返して、$a_1^{(N)}X_1^{(N)} + \cdots + a_m^{(N)}X_m^{(N)}$ を得ることができるが $a_l^{(N)} = 0$ となる l が存在する N が存在する。このとき $X_l^{(N)} = x_l$ である。すると $m - 1$ 変数一次方程式がのこり $X_l^{(N)} = x_l = s$ $(s \in \mathbb{Z})$ とすることができるので帰納法の仮定から $X_1^{(N)}, \ldots, X_{l-1}^{(N)}, X_{l+1}^{(N)}, \ldots, X_m^{(N)}$ の一般解の媒介変数表示を得ることができる。$X_1^{(N)}, \ldots, X_m^{(N)}$ の構成をさかのぼることで $x_1, \ldots, x_m$ の媒介変数表示を得ることができる。

例 10.5.
1 次ディオファントス方程式 $16x + 53y + 25z + 17w = 1$ を考える。
$16x+53y+25z+17w = 16x+(16\times3+5)y+(16\times1+9)z+(16\times1+1)w = 16(x+3y+z+w)+5y+9z+w$
なので、$X_1 = x + 3y + z + w, X_2 = y, X_3 = z, X_4 = w$ とおけば、
$16x+53y+25z+17w = 16X_1+5X_2+9X_3+X_4 = X_4+(16\times1+0)X_1+(5\times1+0)X_2+(9\times1+0)X_3 =$

$1(X_4+16X_1+5X_2+9X_3)+0X_1+0X_2+0X_3$ なので、媒介変数 $s_1,s_2,s_3\in\mathbb{Z}$ をもちいて、
$X_1=s_1,X_2=s_2,X_3=s_3,X_4=1-16s_1-5s_2-9s_3$, すなわち、$x+3y+z+w=s_1,y=s_2,z=s_3,w=1-16s_1-5s_2-9s_3$ が得られるので、$x=17s_1+2s_2+8s_3-1,y=s_2,z=s_3,w=1-16s_1-5s_2-9s_3$ が得られる。

10.2 Q が singular な場合

補題 10.6.
$\boldsymbol{v}_1=(v_{11},\cdots,v_{m1})^\top\in\mathbb{Z}^m$ が *primitive* でかつ $v_{11}\neq 0$ あるとき、$\boldsymbol{v}_1$ を *1* 列目としていて $\det V=1$ であるような行列 $V=(\boldsymbol{v}_1,\cdots,\boldsymbol{v}_m)\in \mathrm{M}_m(\mathbb{Z})$ が得られる。

【証明】
m についての帰納法で示す。
$m=2$ の場合、$\boldsymbol{v}_1=(v_{11},v_{21})$. 仮定より v_{11} と v_{21} が互いに素なので $sv_{11}+tv_{21}=1$ となる $s,t\in\mathbb{Z}$ が存在するので、$V=\begin{pmatrix}v_{11}&-t\\v_{21}&s\end{pmatrix}$ とすればよい。
$m<k$ で主張が成り立っていると仮定して,$m=k$ の場合にも主張が成り立つことを示す。
$\boldsymbol{v}_1=(v_{11},\cdots,v_{k1})^\top\in\mathbb{Z}^k$ が primitive でかつ $v_{11}\neq 0$ あるとし、$g=\mathrm{g.c.d}(v_{11},\cdots,v_{k-1\,1})$ とする。$(v_{11},\cdots,v_{k-1\,1})^\top=g\boldsymbol{v}_1'=g(v_{11}',\cdots,v_{k-1\,1}')^\top$ とすると $\boldsymbol{v}_1'\in\mathbb{Z}^{k-1}$ は primitive であり、$v_{11}'\neq 0$ だから帰納法の仮定より $\boldsymbol{v}_1'$ を 1 列目にもち行列式が 1 になる $k-1$ 次正方行列 $V'=\begin{pmatrix}v_{11}'&\cdot&v_{1\,k-1}'\\\cdot&\cdot&\cdot\\v_{k-1\,1}'&\cdot&v_{k-1\,k-1}'\end{pmatrix}$ を得ることができる。ここで、v_{k1} と g は互いに素なので、$sv_{k1}+tg=1$ となる $s,t\in\mathbb{Z}$ が存在する。したがって、$e=\pm1$ を適切に選んで $V=\begin{pmatrix}gv_{11}'&\cdot&v_{1\,k-1}'&esv_{11}'\\\cdot&\cdot&\cdot&\cdot\\gv_{k-1\,1}'&\cdot&v_{k-1\,k-1}'&esv_{k-1\,1}'\\v_{k\,1}&0&\cdots&t\end{pmatrix}$ とすれば V の 1 列目は $\boldsymbol{v}_1$ であり $\det V=1$ である。
行の入れ替えは行列式の符号のみを変えるので、以下を系として得ることができる。

系 10.7.
$\boldsymbol{v}_1=(v_{11},\cdots,v_{m1})^\top\in\mathbb{Z}^m$ が primitive であるとき、$\boldsymbol{v}_1$ を *1* 列目としていて $V\in\mathrm{GL}_m(\mathbb{Z})$ であるような行列 $V=(\boldsymbol{v}_1,\cdots,\boldsymbol{v}_m)$ が得られる。

アルゴリズム 10.8.
$\det A=0$ の場合に方程式 (1) を解く。

【手順】
$\det A=0$ の場合,A は 0 を固有値にもつので $A\boldsymbol{v}_1=\boldsymbol{0}$ となるベクトル $\boldsymbol{v}_1\in\mathbb{Q}^m$ が存在する、適切に定数倍することで $\boldsymbol{v}_1$ はすべての要素が整数で、primitive なベクトルであるとしてよい。系 10.7 を用いると、行列

$V=(\boldsymbol{v}_1,\cdots,\boldsymbol{v}_m)\in \mathrm{GL}_m(\mathbb{Z})$ を計算することができる。V^{-1} も $\mathrm{GL}_m(\mathbb{Z})$ の要素だから、任意の $\boldsymbol{x}\in\mathbb{Z}^m$ に対してある $\boldsymbol{y}=(y_1,\cdots,y_m)^\top\in\mathbb{Z}^m$ が存在して $\boldsymbol{x}=V\boldsymbol{y}$ となる。
$Q(V\boldsymbol{y})=\boldsymbol{y}^\top V^\top AV\boldsymbol{y}$ であるが $V^\top AV$ の ij 成分は $\boldsymbol{v}_i^\top A\boldsymbol{v}_j$ なので、$Q(V\boldsymbol{y})$ は $m-1$ 変数の 2 次形式 Q_1 を用いて $Q(V\boldsymbol{y})=Q_1(y_2,\cdots,y_m)$ と表すことができる.$L(V\boldsymbol{y})$ についても,$y_2,\cdots,y_m$ の 1 次式 $L_1(y_2,\cdots,y_m)$ 及び $\lambda=\boldsymbol{b}^\top\boldsymbol{v}_1$ を用いて $L(V\boldsymbol{y})=L_1(y_2,\cdots,y_m)+\lambda y_1$ と書ける。したがって方程式 (1) は $Q_1(y_2,\cdots,y_m)+L_1(y_2,\cdots,y_m)=c-\lambda y_1$ と等価になる。
(i)$\lambda=0$ の場合
方程式 (1) は $Q_1(y_2,\cdots,y_m)+L_1(y_2,\cdots,y_m)=c$ となるので変数の数を減らした 2 次ディオファントス方程式に帰着できる。
(ii)$\lambda\neq 0$ の場合
方程式 (1) の可解性は $Q_1(y_2,\cdots,y_m)+L_1(y_2,\cdots,y_m)\equiv c \pmod{|\lambda|}$ の可解性と等価になるので、$(\mathbb{Z}/|\lambda|\mathbb{Z})^{m-1}$ の $|\lambda|^{m-1}$ 個の元について、左辺の値を確認すればよい。

例 10.9.
方程式 $x_1^2+x_2^2+x_3^2-2x_2x_3+x_1+x_2+x_3=3$ を考える。この方程式中の二次形式 $Q(\boldsymbol{x})=\boldsymbol{x}^\top A\boldsymbol{x}$ に対応する行列は、$A=\begin{pmatrix}1&0&0\\0&1&-1\\0&-1&1\end{pmatrix}$ であり、singular である。$(0,1,1)^\top$ は A の零固有ベクトルであり、$V=\begin{pmatrix}0&0&1\\1&1&0\\1&0&0\end{pmatrix}\in\mathrm{GL}_m(\mathbb{Z})$ による基底変換で、$Q(V\boldsymbol{y})=(y_1,y_2,y_3)\begin{pmatrix}0&0&0\\0&1&0\\0&0&0\end{pmatrix}\begin{pmatrix}y_1\\y_2\\y_3\end{pmatrix}=y_2^2$ となり基底変換した後の方程式は $y_2^2+y_2+y_3=3-2y_1$ となる。この方程式が整数解 (y_1,y_2,y_3) が解をもつことの必要十分条件は mod 2 で解をもつことであり、例えば $(y_1,y_2,y_3)=(1,0,1)$ が解になる。

10.3 Q が regular かつ definite な場合

$Q(\boldsymbol{x})=\boldsymbol{x}^\top A\boldsymbol{x}$ が regular でかつ definite である場合について論じる。この場合は命題 10.1 における c^* について、$Q(\boldsymbol{x})=c^*$ をみたす $\boldsymbol{x}\in\mathbb{Z}^m$ の候補が有限個になることがわかり、全探索を行うことができる。
regular でかつ definite である場合、$T\in\mathrm{GL}_m(\mathbb{R})$ があって,$Q(T\boldsymbol{x})=g(\boldsymbol{x})=\sum_{i=1}^m\lambda_i x_i^2$ (λ_i はすべて正かすべて負のどちらか) と書ける。$g(\boldsymbol{x})=c^*$ であるとき、$|x_i|\leq\sqrt{\frac{|c^*|}{|\lambda_i|}}$ である。つまり $||\boldsymbol{x}||\leq\sqrt{\sum_{i=1}^m\frac{|c^*|}{|\lambda_i|}}$ である。T のスペクトルノルムを α とすると、$Q(\boldsymbol{y})=Q(T\boldsymbol{x})=c^*$ であるとき $||\boldsymbol{y}||\leq\alpha\sqrt{\sum_{i=1}^m\frac{|c^*|}{|\lambda_i|}}$ なので有限個の $\boldsymbol{y}\in\mathbb{Z}^m$ を探索し,$Q(\boldsymbol{y})=c^*$ となる $\boldsymbol{y}$ があればその中から mod $2d(Q)$ で $\boldsymbol{h}$ と合同なものがあるかを調べればよい。

以後 $Q(\boldsymbol{x})=\boldsymbol{x}^\top A\boldsymbol{x}$ は regular かつ indefinite である場合のみを考えればよい、次は c^* が 0 か否かで大きな場合分けが生じる。

10.4 $c^* = 0$ の場合

$S_Q = \{\boldsymbol{x} \in \mathbb{Z}^m : Q(\boldsymbol{x}) = 0\}$ とおく。$e = 4d^2$ とおいて、$\pi_e(S_Q)$ を計算する。$\pi_e(S_Q)$ を計算した後は各 $\bar{\boldsymbol{x}} \in \pi_e(S_Q)$ に対して $\pi_e(\boldsymbol{h})$ と $\bmod 2d(Q)$ で合同かどうかを判定するとよい。$\pi_e(S_Q)$ の計算にあたって $m = 2$ の場合と $m \geq 3$ の場合とで場合分けが生じる。

$m = 2$ の場合は S_Q を直接計算することができる。2 変数二次形式 $Q(x, y) = ax^2 + 2bxy + cy^2$ $(a, b, c \in \mathbb{Z})$ に対して S_Q を計算する。$a = 0$ の場合は方程式 $2bx + cy = 0$ を一次方程式の場合と同じようにして解くことで解の媒介変数表示が得られるためこれに射影 π_e を施せばよい。$a \neq 0$ の場合は二次方程式の解の公式より $x = \pm\frac{1}{a}(b + \sqrt{b^2 - ac})y, \pm\frac{1}{a}(b - \sqrt{b^2 - ac})y$ と書けるので $b^2 - ac$ が $\mathbb{Q}$ の平方元でなければ $S_Q = \{(0, 0)\}$ である. 平方元である場合を考える。$a, b + \sqrt{b^2 - ac}, b - \sqrt{b^2 - ac}$ を素因数分解することで、既約分数への変形

$\frac{1}{a}(b + \sqrt{b^2 - ac}) = \frac{q_1^{f_1} \cdots q_s^{f_s}}{p_1^{e_1} \cdots p_r^{e_r}}$

$\frac{1}{a}(b - \sqrt{b^2 - ac}) = \frac{u_1^{g_1} \cdots u_i^{g_i}}{v_1^{h_1} \cdots v_j^{h_j}}$

$(q_1, \ldots, q_s, p_1, \ldots, p_r, u_1, \ldots, u_i, v_1, \ldots, v_j$ は素数)

を得られる。これにより整数解の媒介変数表示 $(x, y) = \pm(q_1^{f_1} \cdots q_s^{f_s} k, p_1^{e_1} \cdots p_r^{e_r} k), (u_1^{g_1} \cdots u_i^{g_i} l, v_1^{h_1} \cdots v_j^{h_j} l)$ $(k, l \in \mathbb{Z})$ が得られるのでこれに射影 π_e を施せば $\pi_e(S_Q)$ を計算することができる。

次に $m \geq 3$ の場合について述べる。まず $Q(\boldsymbol{x})$ が $\mathbb{Q}$ 上 isotropic かどうかを判定する。anisotropic であった場合は $\pi_e(S_Q) = \{\boldsymbol{0}\}$ である。isotropic である場合については以下の命題を用いて $\pi_e(S_Q)$ を計算する。

命題 10.10. (*[GRUN 1981]* PROPOSITION 4)
$m \geq 3$ で Q は regular かつ $\mathbb{Q}$ 上 isotropic であるとする。また、
$d = \det A$,e は $4d^2 | e$ なる正の整数とする。このとき、
$\pi_e(S_Q) = \cup_{\lambda \in \mathbb{Z}/e\mathbb{Z}} \lambda \pi_e(\{\boldsymbol{x} \in \mathbb{Z}^m | \boldsymbol{x} : \text{primitive}, Q(\boldsymbol{x}) \equiv 0 \bmod e^2\})$

【証明】定理の証明のために以下の 2 つの主張を示す。

主張 1 $\boldsymbol{x} \in \mathbb{Z}^m$ は primitive で $Q(\boldsymbol{x}) \equiv 0 \pmod{e^2}$,$d$ は $d = p_0^{l_0'} p_1^{l_1} \cdots p_q^{l_q}$ ($p_0 = 2$,$i \geq 1$ について p_i は奇素数で $l_0' \geq 0, l_1, \cdots, l_q \geq 1$) と素因数分解できるとする。また、$l_0 = l_0' + 1$ とする。この時 $\boldsymbol{x}_{\boldsymbol{p_i}} \in \mathbb{Z}_{p_i}$ $(i = 0, \cdots, q)$ が存在して $Q(\boldsymbol{x}_{p_i}) = 0$ $(i = 0, \cdots, q)$ かつ $v_{p_i}(\boldsymbol{x} - \boldsymbol{x}_{p_i}) \geq 2l_i$ $(i = 0, \cdots, q)$ を満たす。

主張 2 $\boldsymbol{x} \in \mathbb{Z}^m$ が primitive で $Q(\boldsymbol{x}) \equiv 0 \pmod{e^2}$ であるとき、$Q(\boldsymbol{y}) = 0$ かつ $\boldsymbol{y} \equiv \boldsymbol{x} \bmod e$ を満たす $\boldsymbol{y} \in \mathbb{Z}^m$ が存在する。

(**主張** 1 の証明) $Q(\boldsymbol{x}) \equiv 0 \pmod{e^2}$ であることから、$v_{p_i}(Q(\boldsymbol{x})) \geq 4l_i$ である。また、A が対称行列であることから $\frac{\partial}{\partial X_k} Q(\boldsymbol{X}) = 2\sum_j a_{kj} X_j$ である。ここで各 i を fix し、すべての k で $2\sum_j a_{kj} x_j$ の p_i 進付値が l_i より大きいと仮定すると矛盾することを示す。$2\sum_j a_{kj} x_j$ は $2A\boldsymbol{x}$ の第 k 成分なので、仮定より $2A\boldsymbol{x}$ の各成分の p_i 進付値が l_i より大きいことになるが、$\tilde{A} \in \mathrm{M}_m(\mathbb{Z})$ なので、$2\tilde{A}A\boldsymbol{x}$ の各成分の p_i 進付値も l_i より大きくなるはずである。しかし,$2\tilde{A}A\boldsymbol{x} = 2d\boldsymbol{x}$ であり $\boldsymbol{x}$ が primitive なのでこれは矛盾である。よって、少なくとも一つの $k^{(i)}$ について、

$0 \leq v_{p_i}(\frac{\partial}{\partial X_{k^{(i)}}} Q(\boldsymbol{x})) = v_{p_i}(2\sum_j a_{k^{(i)}x_j}) \leq l_i < 2l_i$ が言えるのでヘンゼルの補題より、$Q(\boldsymbol{x}_{\boldsymbol{p_i}}) = 0$ かつ $\boldsymbol{v}_p(\boldsymbol{x} - \boldsymbol{x}_{p_i}) \geq v_{p_i}(Q(\boldsymbol{x})) - v_{p_i}(\frac{\partial}{\partial X_{k^{(i)}}} Q(\boldsymbol{x})) \geq 2l_i$ を満たす $\boldsymbol{x}_p \in \mathbb{Z}_p^m$ が存在する。

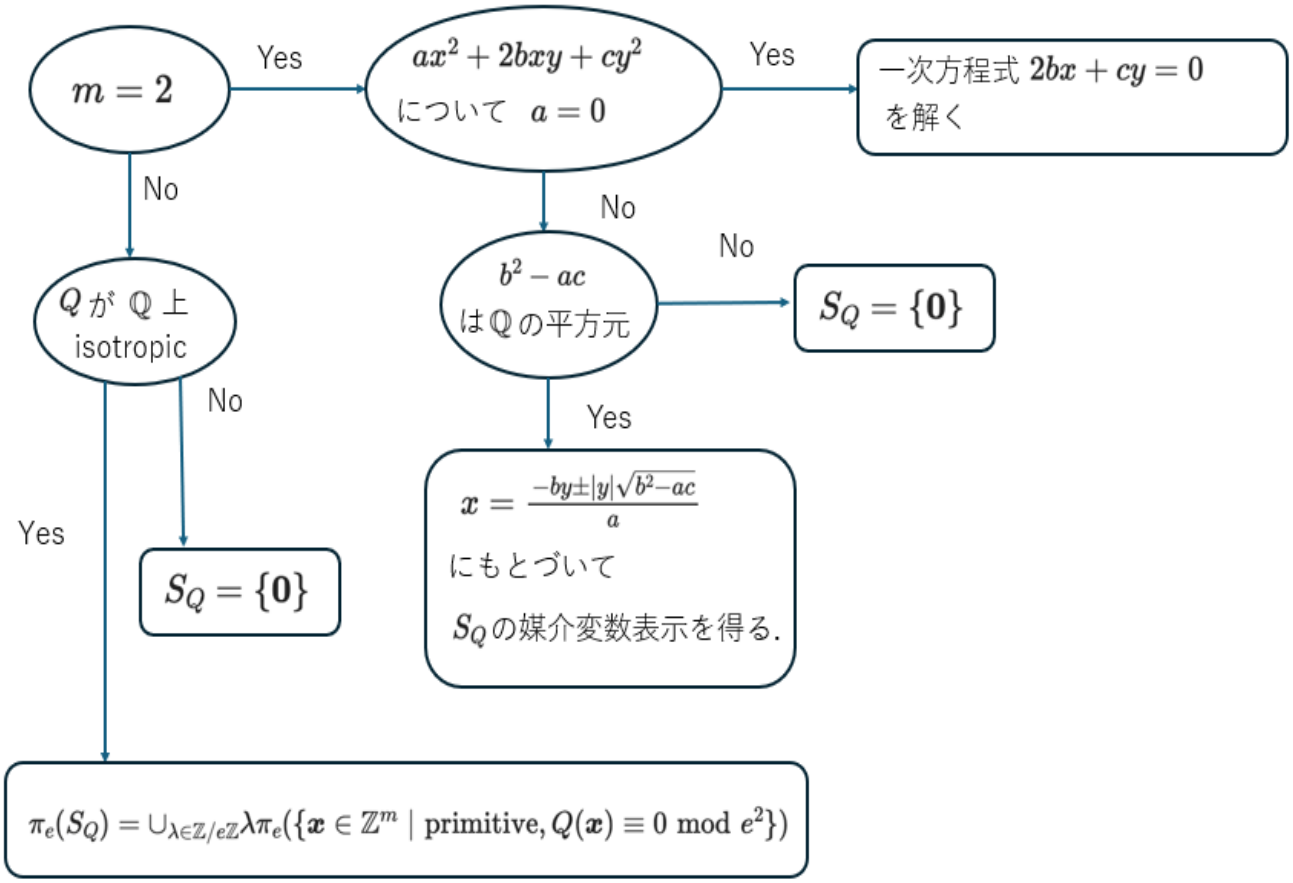
(**主張** 2 の証明) $P=\{p_0,p_1,\cdots,p_q\}$ に対して近似補題を適用すると、$\epsilon>0$ に対して $Q(\boldsymbol{z})=0$ かつ $||\boldsymbol{z}-\boldsymbol{x}_{p_i}||_{p_i}<\epsilon$ を満たす $\boldsymbol{z}\in\mathbb{Q}^m$ が存在する。$\boldsymbol{v}_{p_i}(\boldsymbol{z})\geq\min\{\boldsymbol{v}_{p_i}(\boldsymbol{z}-\boldsymbol{x}_{p_i}),\boldsymbol{v}_{p_i}(\boldsymbol{x}_{p_i})\}$ なので、ϵ を十分小さくとることですべての i で $\boldsymbol{z}\in\mathbb{Z}_{p_i}^m$ となるように $\boldsymbol{z}$ をとれる。したがって、e と互いに素になる整数 s であって、$s\boldsymbol{z}\in\mathbb{Z}^m$ となるようなものが存在する。$\pi_e(s)\in(\mathbb{Z}/e\mathbb{Z})^\times$ なので $ts\equiv 1 \mod e$ となる整数 t が存在する。$\boldsymbol{y}=ts\boldsymbol{z}$ とおくと $Q(\boldsymbol{y})=0$ で $\boldsymbol{y}\equiv\boldsymbol{z}\equiv\boldsymbol{x} \mod e$ である。
($\boldsymbol{y}-\boldsymbol{x}=(\boldsymbol{y}-\boldsymbol{z})+(\boldsymbol{z}-\boldsymbol{x}_{p_i})+(\boldsymbol{x}_{p_i}-\boldsymbol{x})$ であって、$(\boldsymbol{y}-\boldsymbol{z}),(\boldsymbol{z}-\boldsymbol{x}_{p_i}),(\boldsymbol{x}_{p_i}-\boldsymbol{x})$ なので,$\boldsymbol{v}_{p_i}(\boldsymbol{y}-\boldsymbol{x})\geq\min\{\boldsymbol{v}_{p_i}(\boldsymbol{y}-\boldsymbol{z}),\boldsymbol{v}_{p_i}(\boldsymbol{z}-\boldsymbol{x}_{p_i}),\boldsymbol{v}_{p_i}(\boldsymbol{x}_{p_i}-\boldsymbol{x})\}\geq 2l_i$)
主張を示すことができたので、これを用いて命題を示す。
(命題の証明) 記号の簡略化のため、$\{\boldsymbol{x}\in\mathbb{Z}^m|\boldsymbol{x}:\text{primitive},Q(\boldsymbol{x})\equiv 0 \bmod e^2\}$ を X とおく。
$\lambda\pi_e(\boldsymbol{x})\in\cup_{\lambda\in\mathbb{Z}/e\mathbb{Z}}\lambda\pi_e(X)$ とすると,$\pi_e(\boldsymbol{x})=\pi_e(\boldsymbol{y})$ かつ $Q(\boldsymbol{y})=0$ となる $\boldsymbol{y}\in\mathbb{Z}^m$ があるので,$\lambda\pi_e(\boldsymbol{x})=\pi_e(\lambda\boldsymbol{y})\in\pi_e(S_Q)$.
逆に、$\pi_e(\boldsymbol{y})\in\pi_e(S_Q)$ とすると、$\boldsymbol{y}=g\boldsymbol{y}'$ ($\boldsymbol{y}'$ は primitive で g は $\boldsymbol{y}$ の成分の最大公約数) と書けて、$\boldsymbol{y}'\in X$ だから、$\pi_e(\boldsymbol{y})\in\cup_{\lambda\in\mathbb{Z}/e\mathbb{Z}}\lambda\pi_e(X)$

注 10.11. $\pi_e(\{\boldsymbol{x}\mid\boldsymbol{x}:\text{primitive},,\ Q(\boldsymbol{x})\equiv 0 \mod e^2\})$ を算出するためには $\pi_{e^2}\{\boldsymbol{x}\mid\boldsymbol{x}:\text{primitive}\}$ を算出する必要がある。この過程では各 $\boldsymbol{a}\in\{0,1,\ldots,e^2-1\}$ に対して

$$(a_1+k_1e^2)c_1+\cdots+(a_m+k_me^2)c_m=1 \tag{2}$$

を満たす整数 $k_1,\ldots,k_m,c_1,\ldots,c_m$ が存在するかを判定することになる。この方程式は $k_1,\ldots,k_m,c_1,\ldots,c_m$ を変数とする 2 次ディオファントス方程式であるが二次形式が 4 変数以上で regular, indefinite でかつ $c^*\neq 0$ の場合に当てはまる。実際、*(2)* 式の二次形式に対応する行列は $\begin{pmatrix}O_{m,m}&I_m\\I_m&O_{m,m}\end{pmatrix}$ でありその行列式は $(-1)^m$ である。さらに、$\boldsymbol{h}=(-1)^m\begin{pmatrix}O_{m,m}&I_m\\I_m&O_{m,m}\end{pmatrix}\begin{pmatrix}0\\\vdots\\0\\a_1\\\vdots\\a_m\end{pmatrix}=\begin{pmatrix}a_1\\\vdots\\a_m\\0\\\vdots\\0\end{pmatrix}$ なので $c^*=4\{(-1)^m\}^2+a_1^2+\cdots+a_m^2=4+a_1^2+\cdots+a_m^2>0$ なので、命題 *10.12* より,*(2)* 式は $\bmod 8(4+a_1^2+\cdots+a_m^2)^2$ で解けばよいことがわかる。

$\pi_e(S_Q)$ の計算アルゴリズムについてフローチャートでまとめると以下の通りとなる。



10.5 $c^* \neq 0$ の場合

変数の数が 4 以上の場合は以下の命題により容易に方程式を解くことができる。

命題 10.12. (*[GRUN 1981]* PROPOSITION 2)
2 次ディオファントス方程式 $\boldsymbol{x}^\top A\boldsymbol{x} + \boldsymbol{b}\boldsymbol{x} = c$ について、変数の数が 4 以上であり、A が regular かつ indefinite であるとする。このとき、方程式が整数解を持つ。$\Leftrightarrow$ 方程式が $\bmod 8(\det Ac^*)^2$ で解を持つ。

定義 10.13.
$G_Q = \{B \in \mathrm{GL}_m(\mathbb{C}) \mid \forall \mathbf{x}.\, Q(B\boldsymbol{x}) = Q(\boldsymbol{x})\}$, $\Gamma_Q = \{B \in \mathrm{GL}_m(\mathbb{Z}) \mid \forall \mathbf{x}.\, Q(B\boldsymbol{x}) = Q(\boldsymbol{x})\}$ とする.
Γ_Q は二次形式 Q の直交群と呼ばれる。

$\boldsymbol{x}$ についての恒等式 $Q(B\boldsymbol{x}) = Q(\boldsymbol{x})$ の係数比較をすることで、G_Q は $\mathbb{Q}$-群であり、Γ_Q はその arithmetic-subgroup であることがわかる。したがって、Γ_Q は有限生成であり, アルゴリズム 9.31 によってその生成系を計算することができる。

定義 10.14.
$\mathbb{Z}^m$ に同値関係 $\sim_Q$ を $\mathbf{x} \sim_Q \mathbf{y} \Leftrightarrow \exists B \in \Gamma_Q[\mathbf{y} = B\mathbf{x}]$ で定める。各同値類 $C \in \mathbb{Z}^m/\sim_Q$ の元を Γ_Q-軌道といい、各 Γ_Q-軌道から代表元を *1* つずつとってきて作った集合 T_Q を Γ_Q-軌道の完全代表系という。

$c^* \neq 0$ の場合の求解アルゴリズムには以下を計算する必要がある。
(i)Γ_Q の生成系 $\Gamma'_Q \subseteq \Gamma_Q$
(ii)Γ_Q-軌道の完全代表系 T_Q の部分集合 $T'_Q = \{\mathbf{v} \in T_Q | Q(\mathbf{v}) = c^*\}$
(i) はアルゴリズム 9.31 によって計算することができる。(ii) は以下のようにして計算することができる.

定義 10.15.
$\mathbb{Z}$ 係数二次形式 Q と整数 $c^* \neq 0$ に対して、$R_Q(c^*) = \{\boldsymbol{x} \in \mathbb{Z}^m \mid Q(\boldsymbol{x}) = c^*\}$
$R_Q^{(0)}(c^*) = \{\boldsymbol{x} \in \mathbb{Z}^m, \text{primitive} \mid Q(\boldsymbol{x}) = c^*\}$

明らかに以下が成り立つ。

補題 10.16.
$R_Q(c^*) = \cup_{r^2|c^*} r R_Q^{(0)}(c^* r^{-2})$

アルゴリズム 10.17. (*[GRUN 1981]* chapter5)
$r^2|c^*$ なる r を固定し、$h = c^* r^{-2}$ とおく。$\mathbb{Q}$ 上の二次形式 Q に対して、Γ_Q-軌道の完全代表系 T_Q の部分集合 $T_Q'^{(h)} = T_Q \cap R_Q^{(0)}(h)$ を算出する。

【手順】
STEP1: 以下の条件を満たす有限集合 T_1 を構成する。
(条件)
・T_1 は $d(\phi) = h^{m-2} d(Q)$ を満たす $m-1$ 変数二次形式からなる。
・任意の $m-1$ 変数 regular 二次形式 ϕ' に対して ϕ' と $\mathbb{Z}$-equivalent な $\phi \in T_1$ が存在する。
STEP2: 有限集合 $T_2 = \{\psi | \psi(\mathbf{x}) = (hx_1 + \nu_2 x_2 + \cdots + \nu_m x_m)^2 + \phi(x_2, \ldots, x_m), \phi \in T_1, |\nu_j| \leq h\}$ を構成し、各 $\psi \in T_2$ に対して ψ が hQ と $\mathbb{Z}$-equivalent かどうかを判定する。
STEP3:T_2 の要素のうち、hQ と $\mathbb{Z}$-equivalent なものたちの集合を T_3 とおく。$\psi \in T_3$ に対して、$hQ(B_\psi \boldsymbol{x}) = \psi(\boldsymbol{x})$ となる $B_\psi \in \mathrm{GL}_m(\mathbb{Z})$ をもとめ、$\{\mathbf{v} | \mathbf{v}$ はある $\psi \in T_3$ に対して B_ψ の 1 列目になる $\}$ を求める。これが求めるべき $T_Q'^{(h)}$ である。

アルゴリズム 10.18 の STEP $1, 2$ を行うには以下の 2 つを行うアルゴリズムが本質的である. これはアルゴリズム 4.24 により実行できる。
・与えられた $d \neq 0$ に対して、$d(Q) = d$ となる Hermite-reduced な二次形式をすべて含む有限集合 T_d を算出する。
・与えられた 2 つの $\mathbb{Z}$ 係数二次形式 Q, Q' が $\mathbb{Z}$-equivalent かどうかを判定するこれはアルゴリズム 4.25 により実行できる。

アルゴリズム 10.18. (*[GRUN 1981]* chapter5)

$\mathbb{Q}$ 上の二次形式 Q に対して、Γ_Q-軌道の完全代表系 T_Q の部分集合 $T'_Q = \{\mathbf{v} \in T_Q | Q(\mathbf{v}) = c^*\}$ を算出する。

【手順】
アルゴリズム 10.17 によって算出した $T'^{(h)}_Q$ について、$T'_Q = \cup_{r^2|c^*} rT'^{(h)}_Q$ とすればよい。
(i),(ii) で計算したものをもとに以下のようにして方程式 (1) を解く。

命題 10.19.
有限群 $\mathrm{GL}_m(\mathbb{Z}/2d\mathbb{Z})$ の要素の個数よりも大きい数 M をひとつとり、$X = \cup_{i=0}^{M}\{g_1 \cdots g_i \mid g_1, \ldots, g_i \in \Gamma'_Q\}$、$\pi_{2d} : \mathrm{M}_m(\mathbb{Z}) \to \mathrm{M}_m(\mathbb{Z}/2d\mathbb{Z})$ を自然な射影とする. このとき鳩ノ巣原理により $\pi_{2d}(X) = \pi_{2d}(\Gamma_Q)$ である.

アルゴリズム 10.20. 上記 (i),(ii) で計算した Γ'_Q および T'_Q を用いて、方程式 (*1*) の可解性を判定する。

【手順】
STEP1: 有限群 $\mathrm{GL}_m(\mathbb{Z}/2d\mathbb{Z})$ の要素の個数よりも大きい数 M をひとつとる. 例えば $M = (2d)^{m^2} + 1$ とすればよい。
STEP2: 命題 10.19 の X の各要素 g と T'_Q の各要素 $\boldsymbol{v}$ に対して $g\boldsymbol{v}$ が $\bmod 2d$ で $\boldsymbol{h}$ と合同なものがあるかを調べる。
STEP3:STEP2 で探索したものがあれば方程式 (1) には整数解がある. ない場合は整数解はない。

11 拡張及び今後の課題

11.1 単一の 2 次不等式の場合

単一の 2 次不等式

$$Q(\boldsymbol{x}) + L(\boldsymbol{x}) \leq c \tag{3}$$

はラグランジュの 4 平方和定理と呼ばれる初等整数論の以下の命題により簡単に 2 次方程式に帰着することができる。

命題 11.1. (ラグランジュの 4 平方和定理)
任意の自然数は 4 つの整数の平方和で表すことができる。

命題 11.1 より、不等式 3 を解くには 2 方程式

$$Q(\boldsymbol{x}) + L(\boldsymbol{x}) + u_1^2 + u_2^2 + u_3^2 + u_4^2 = c \tag{4}$$

を解けばよいことになる。

11.2　1 次等式制約を加えた場合について

ディオファントス制約

$$\begin{cases} Q(\boldsymbol{x}) + L(\boldsymbol{x}) = c \\ a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m = 0 \\ \cdot \\ \cdot \\ a_{l1}x_1 + a_{l2}x_2 + \cdots + a_{lm}x_m = 0 \end{cases}$$

を解くアルゴリズムを構成することができる。

まず、1 番目の等式制約 ϕ_1 : $a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m = 0$ に着目して制約を満たす $\boldsymbol{x}$ が存在する場合は ϕ_1 を満たす $\boldsymbol{x}$ の媒介変数表示を得る。ここで得た媒介変数表示を、2 番目の等式制約 ϕ_1 : $a_{21}x_1 + a_{22}x_2 + \cdots + a_{2m}x_m = 0$ に代入して、・・・という操作を逐次的に各 1 次等式制約に対して繰り返すことで単一の 2 次ディオファントス方程式に代入するため $\boldsymbol{x}$ の媒介変数表示を得ることができるので、単一の 2 次方程式の場合に帰着できる。

11.3　今後の課題

最後に、今後に残された課題について簡単に述べる。Farkas 補題を用いたループ不変式生成への応用にあたっては一般には複数の二次制約からなる連立二次制約を解くことになる。ラグランジュの 4 平方和定理により不等式制約をすべて等式制約に変え、辺々の平方和をとることで単一の 4 次ディオファントス方程式に帰着させることができるがこれは一般には決定不能である。今後のアプローチの方針としては以下が考えられる。

(1) PIA は単一の二次不等式と任意有限個の一次制約 (不等式を含んでいてもよい) の可解性決定問題が NP に属していると主張している。([PIA 2017]) ただしこの論文から構成的なアルゴリズムが抽出できるかは非自明でありこれを調べることで単一の二次制約に一次不等式制約が加わった場合に適用できるアルゴリズムを構成できる可能性がある。

(2) JONES は再帰的可算集合が何変数何次のディオファントス方程式で表現できるかを算出することで、方程式が決定不能になる変数の数 v と次数 d のペア (v, d) を求める方法について論じている。([JONE 1982]) この研究は変数の個数及び次数に基づいて決定可能性の境界を探ることができる可能性を示唆している。

(3) Colon が例として出しているループ不変式生成への応用で現れる二次ディオファントス制約は例えば $\mu\lambda + \lambda' = 0$ のような二次の項が交差項のみの形をしている。([COLO 2003]) 応用上現れる二次制約の形を特定し、その特殊性を用いて決定アルゴリズムを構成できないかを探求することも重要である。例えば [RABO 2012] では、x_i, y_j を未知変数とする

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}x_iy_j = b \ (a_{ij}, b \in \mathbb{Z}) \tag{5}$$

の形をした二次ディオファントス方程式を解くアルゴリズムが提案されている。

(4) 決定アルゴリズムが存在しない場合でも離散最適化問題の確率的アルゴリズムで応用上有用なものがある可能性がある。多項式の二乗和 $f_1^2 + \cdots f_s^2$ を最小化する問題を考えることでディオファントス制約の求解問題を離散最適化の問題に帰着できる。He らは遺伝的アルゴリズムによる離散最適化アルゴリズ

ムの収束レートについてマルコフ過程の理論を用いて論じている。[He 1999] 多くの離散最適化アルゴリズムについての研究は定義域が有限集合であることが前提となっているがこの研究では定義域はコンパクト測度空間であればよいとされている。$\mathbb{Z}^m$ に無限遠点を加えた空間を m 次元球面に射影すればディオファントス制約を解く確率的アルゴリズムを構成できるのではないかと予想している。

(5) 三次ディオファントス方程式の決定可能性は未解決であるが、これは今回の研究で用いたものとは全く異なるアプローチが必要となることが予想される。

(6) 本研究の対称であった単一の二次ディオファントス方程式についても、よりシンプルな別解を模索したい。特に、3 変数以下の場合についてはアルゴリズムの随所に可算集合の要素を列挙する部分があったため、このままでは計算量の上界が不明確である。2 変数の場合については二次曲線の初等的計算による解法が [Alpertron 2016] に記述されている。そのため、別解の模索については 3 変数の場合が本質的課題である。

参考文献

[GRUN 1981] Grunewald et.al. *How to solve a quadratic equation in integers.* Mathematical Proceedings of the Cambridge Philosophical Society 89 (1) 1-5, 1981

[GRUN 1980] Grunewald et.al. *Some General Algorithms. I: Arithmetic Groups.* Annals of Mathematics 112 (3) 531-583 , 1980

[CASS 1978] Cassels *RATIONAL QUADRATIC FORMS.* Academic Press London, 1978

[COLO 2003] Colon et.al. *Linear Invariant Generation Using Non-Linear Constraint Solving.* CAV 2003: CVCS 420 – 432, 2003

[COLL 1975] Collins *Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition.* LNCS 32. Springer Verlag, 1975.

[JONE 1976] Jones et.al. *Diophantine Representation of the Set of Prime Numbers.* The American Mathematical Monthly 83(6) 449 – 464, 1976

[PIA 2017] Pia et.al. *Mixed-integer Quadratic Programming is in NP.* Mathematical Programming 162 225 – 240, 2017

[JONE 1980] Jones *Undecidable diophantine equations.* Bull. Amer. Math. Soc. 3 (2) 859-862, 1980

[JONE 1982] Jones *Universal Diophantine equation.* THE JOURNAL OF SYMBOLIC LOGIC Volume 47 Number 3, 1982

[TAR 1951] Tarski *Decision Methods for Elementary Algebra and Geometry.* Berkeley: Univ.of California Press, 1951

[SERR 1978] SerreCHV *A Course in Arithmetic.* Springer, 1978

[MATI 1970] Matijasevic *Enumerable sets are Diophantine.* English translation: Soviet Math. Doklady, (11) 354-357,1970

[MATI 1971] Matijasevic *Diophantine representation of enumerable predicates.* (Russian) Izv. Akad. Nauk SSSR, Ser. Mat. (35) 3-30,1971

[DAVI 1973] M.Davis *Hilbert's Tenth Problem is Unsolvable.* The American Mathematical Monthly, 80 (3) 233-269, 1973

[BHC 1962] Borel, Chandra *Arithmetic subgroups of algebraic groups.* Ann of Math, (75) 485-535, 1962

[MKS 1966] W.Magnus, A.Karass, D.solitar *Combinatorial group theory.* New York, Wiley, 1966

[CHV 1947] Chevalley, C. *Algebraic Lie Algebras.* The Annals of Mathematics, 48(1), 91-100,1947

[MOS 1955] G.D. MOSTOW *Self-adjoint groups.* The Annals of Mathematics, 62, 44-55,1955

[MOS 1956] G.D. MOSTOW *Fully reducible subgroups of algebraic groups.* Amer. J. Math. 78 200-221.1956

[BO 1969] Borel *Linear Algebraic Groups.* notes by H.Bass, New York, Benjamin. 1969

[Ha 2000] Hartshorne *Algebraic Geometry.* springer, 2000

[ATY 1994] Atiyah,MacDonald *Introduction to Commutative Algebra.* Westview Press 1994

[He 1999] He, Kang *On the convergence rates of genetic algorithms.* Theoretical Computer Science 229 23 – 39,1999

[RABO 2012] Raboky, Amiri *Diophantine Quadratic Equation and Smith Normal Form Using Scaled Extended Integer Abaffy – Broyden – Spedicato Algorithms.* J Optim Theory Appl 152 75 – 96,2012

[NORO 2011] Masayuki Noro *noro_pd.* noro_pd User' s Manual Edition 1.0 Feb 2011 http://www.math.sci.kobe-u.ac.jp/OpenXM/Current/doc/asir-contrib/ja/noro_pd-html/noro_pd-ja.html (参照 2024-12-24)

[Alpertron 2016] Alpertron *Methods to solve quadratic Diophantine equations.* Methods to solve quadratic Diophantine equations 2016-05-02 https://www.alpertron.com.ar/METHODS.HTM (参照 2024-12-17)

[日比 2011] 日比 他**グレブナー道場**. 共立出版 2011

[穴井 2003] 穴井 *Quantifier Elimination* — **アルゴリズム・実装・応用** —. 数式処理 J.JSSAC Vol. 10, No. 1, pp. 3 – 12, 2003

[雪江 2013] 雪江**整数論** *1* **初等整数論から** *p* **進数へ**. 日本評論社 2013

[雪江 群 2010] 雪江**群論入門**. 日本評論社 2010

[雪江 群 2010] 雪江**群論入門**. 日本評論社 2010

[雪江 環 2010] 雪江**環と体とガロア理論**. 日本評論社 2010

[板井 2020] 板井**幾何的モデル理論入門 改訂版**. 日本評論社 2020

[川崎 2020] 川崎**位相空間 例と演習**. 共立出版 2020

[斉藤 1966] 齋藤**線型代数入門**. 東京大学出版会 1966

[井ノ口 2017] 井ノ口**はじめて学ぶリー群-線型代数から始めよう**. 現代数学社 2017

[井ノ口 2018] 井ノ口**はじめて学ぶリー環-線型代数から始めよう**. 現代数学社 2018