ガウスの2次形式論とクロネッカー·ウェーバーの定理についての考察

三浦 正道

新潟大学大学院自然科学研究科博士前期課程
数理物質科学専攻

概要

本論文では, 著者が大学院で学んだ中で, ガウスの 2 次形式論とクロネッカー · ウェーバーの定理に特に興味を持った. ゼミの中でも著者が勉強してきた中で特に苦労し, 時間をかけた主題でもある. 本論文では, この 2 つの主題について証明をつけてまとめ, この 2 つの主題に関わる考察を行っている.

ガウスの 2 次形式論は, 特に整係数 2 元 2 次形式 $ax^2 + bxy + cy^2$ における理論である. まず, 1800 年代初頭に, ガウスにより提唱された. 1850 年代に入って, デデキントにより, この理論は 2 次体の整数論と対応していることがわかり, 2 次体のイデアルを 2 元 2 次形式に簡潔に表現されるようになった. 本論文では, ガウスが提唱した概念を紹介する. さらに 2 元 2 次形式が実際に 2 次体と対応できることも証明していく.

クロネッカー · ウェーバーの定理は, 任意の $\mathbb{Q}$ 上のアーベル体は円分体に含まれるという定理である :

$$\text{アーベル拡大 } K/\mathbb{Q} \text{ に対し, } K \subset \mathbb{Q}(\zeta_n) \text{ となる } n \in \mathbb{N} \text{ が存在する.}$$

この定理は 1853 年にクロネッカーにより述べられたが, 証明の一部が不完全であった. その後, 1886 年にウェーバーが証明を提出したが, ウェーバーによる証明も一部, 誤りを含んでいたという歴史がある. 本論文では, 最初に完全な証明を与えたヒルベルトによる証明を紹介する.

この 2 つの主題は, 現在著者が学んでいる, 1920 年代に高木貞治とアルティンが構築した類体論の枠組みの中で非常に関係している. 類体論において, アルティンの相互法則という定理がある. この定理は特に, 代数体 F に対し, K を F のヒルベルト類体とすると, ガロア群 $\mathrm{Gal}(K/F)$ と F のイデアル類群 Cl_F は同型であることが知られている :

$$\mathrm{Gal}(K/F) \simeq Cl_F.$$

特に F が類数 2 の虚 2 次体に対し, ガウスの 2 次形式論によりイデアル類群を 2 次形式で見ることができ, そのヒルベルト類体は $\mathbb{Q}$ 上アーベル拡大であるからクロネッカー · ウェーバーの定理を使って, F のヒルベルト類体と, F に対応する整係数 2 元 2 次形式 $f(x, y)$ が実際に対応していることを述べる.

本論文は, Richard A.Mollin 著の Algebraic Number Theory に従って進められているが, 証明については普段のゼミと同じように, 他の本なども参照し, 自分が完全に納得できるものにしている. 著者が参考にした文献は参考文献に載せている.

本論文は 5 つの章からなっている. 第 1 章では可換環論, ガロア理論, 代数的整数論の初歩的な定理や, 第 2 章以降で必要になってくる定理などを簡単にまとめた. 第 2 章では, ガウスの 2 次形式論について展開する. この章では 2 元 2 次形式に対して基本的なものを準備し, そこから 2 次体のイデアル類群と対応させている. 第 3 章では, 第 1 章で準備したこと使って, クロネッカー · ウェーバーの定理を証明している. 第 4 章では, 第 2 章や第 3 章を利用して著者が考察した, アルティンの相互法則の例である, 虚 2 次体上のヒルベルト類体と 2 次形式が関わることの具体例を述べている. 最後に, 第 5 章では著者の今後の研究の対象を挙げ, 将来解決したい問題を紹介している.

謝辞

本論文を作成するにあたり, 指導教員の星明考先生から非常に丁寧な指導を頂きました. ここに感謝の意を表します. また, 私に今後の研究に対する助言を与えてくださった三宅克哉先生と愛知教育大学の岸康弘先生に感謝申し上げます. 更に, この研究に対して様々な意見を出してくれた後輩の金井和貴君と長谷川寿人君にも感謝致します.

目 次

第1章　準備

この章では, 第 2 章以降に入るための準備を行う. 第 1 節で初等整数論のルジャンドル記号と無理数の連分数展開, 第 2 節ではイデアルやデデキント整域などの可換環について, 第 3 節では代数体の定義や, 類数の有限性などの代数的整数論について, 第 4 節ではガロア拡大の定義やガロア理論の基本定理, 第 5 節では素イデアル分解におけるヒルベルトの理論について, この章で準備する.

証明はすべて省くが, 参考文献において, 初等整数論は [4], 代数的整数論, ヒルベルトの理論は [1] から [6] と [16], ガロア理論は [4], [6], [7], [8] にこの内容が載っている.

1.1　初等整数論から

この章では, ルジャンドル記号と無理数の連分数展開について準備する. ルジャンドル記号は第 4 章で取り扱うための道具であり, 連分数展開については第 2 章で重要になってくる.

定義 1.1 $a \in \mathbb{Z}$ をとる. 奇素数 p に対して,

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & (x^2 \equiv a \pmod{p} \text{ となる } x \in \mathbb{Z} \text{ が存在するとき}), \\ 0 & (p \mid a \text{ のとき}), \\ -1 & (\text{それ以外}) \end{cases}$$

と定義する. 記号 $(\frac{a}{p})$ を**ルジャンドル記号** (または**平方剰余記号**) という.

このルジャンドル記号が満たす大事な定理を述べておく. この定理はルジャンドル記号を計算する際に非常に便利な定理であり, 第 4 章で実際に計算するときに利用する.

定理 1.2 $a, b \in \mathbb{Z}$, p, q を相異なる奇素数とする. このとき, 以下が成り立つ :

(1) $a \equiv b \pmod{p}$ ならば $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

(3) $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$;

(4) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$;

(5) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

続いて, 連分数展開について準備する. 第 2 章では主に無理数の連分数展開を行うが, ここではまず, 有理数の連分数展開についても述べていく.

まず, $a > b$ かつ $b \neq 0$ となる $a, b \in \mathbb{Z}$ をとり, ユークリッドの互除法を行っていく. すなわち,

$$\begin{cases} a = q_1 b + r_1 & (0 < r_1 < b), \\ b = q_1 r_1 + r_2 & (0 < r_2 < r_1), \\ \quad \vdots & \\ r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} & (0 < r_{n-1} < r_{n-2}), \\ r_{n-2} = q_n r_{n-1} + r_n & (0 = r_n) \end{cases}$$

というようにかけるとする. これは,

$$\begin{cases} \dfrac{a}{b} = q_1 + \dfrac{r_1}{b} & (0 < \frac{r_1}{b} < 1), \\ \dfrac{b}{r_1} = q_1 + \dfrac{r_2}{r_1} & (0 < \frac{r_2}{r_1} < 1), \\ \quad \vdots & \\ \dfrac{r_{n-3}}{r_{n-2}} = q_{n-1} + \dfrac{r_{n-1}}{r_{n-2}} & (0 < \frac{r_{n-1}}{r_{n-2}} < 1), \\ \dfrac{r_{n-2}}{r_{n-1}} = q_n & \end{cases}$$

となるから,

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}$$

とかくことができる. つまり, 有理数はユークリッドの互除法で現れた商でかくことができる. この展開のことを有理数 $\frac{a}{b}$ の**連分数展開**といい,

$$\frac{a}{b} = [q_1, q_2, \cdots, q_n]$$

とかく.

注意 1.3 $\frac{a}{b} = [q_1, q_2, \cdots, q_n]$ とかいたときに, q_1 は $\frac{a}{b}$ の整数部分である. また, q_2 は $\frac{b}{r_1}$ の整数部分である. さらに, $i \geq 3$ に対して q_i は $\frac{r_{i-1}}{r_i}$ の整数部分である. つまり, 小数部分の逆数の整数部分のことである.

また, 有理数が与えられたときにその連分数展開は一意であり, 有限に展開される.

無理数についても整数部分と小数部分があるので, 無理数に対しても連分数展開を拡張することができる. $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ に対して, $[\alpha]$ を α を超えない最大の整数, $(\alpha) := \alpha - [\alpha]$ と表すことにする. つまり, (α) は α の小数部分を表している.

このとき, 注意 1.3 のようにすると,

$$\begin{cases} \alpha = [\alpha] + (\alpha) & (0 < (\alpha) < 1), \\ (\alpha)^{-1} = [(\alpha)^{-1}] + ((\alpha)^{-1}) & (0 < ((\alpha)^{-1})) < 1), \\ \quad \vdots \end{cases}$$

というように展開できる. 無理数であるから, 無限に続くことに注意する. これが無理数のときの連分数展開である. また, 無理数を連分数展開したときに出てくる無理数のことを**中間連分数**という.

式ではわかりにくいので, 連分数展開の簡単な例を挙げておく.

例 1.4 ($\sqrt{2}$ の連分数展開) $[\sqrt{2}] = 1$ であるから, $(\sqrt{2}) = \sqrt{2} - 1 = \frac{1}{\sqrt{2}+1}$ である. つまり,

$$\sqrt{2} = 1 + \frac{1}{\sqrt{2}+1}$$

とかける. さらに, $[\sqrt{2}+1] = 2$ であるから, $(\sqrt{2}+1) = \sqrt{2} - 1 = \frac{1}{\sqrt{2}+1}$ である. つまり,

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{\sqrt{2}+1}}$$

とかける. 分母に同じものが出たため, 以降はこれを繰り返しやっていくことになるので,

$$\sqrt{2} = [1, 2, 2, 2, \cdots]$$

と展開される.

次に, 連分数展開の性質を述べる.

$\lambda_1, \lambda_2, \cdots$ と変数とし, $[\lambda_1, \lambda_2, \cdots]$ を考えると, これは $\lambda_1, \lambda_2, \cdots$ の有理関数でかくことができる. 2 つ数列 P_n, Q_n を, 次のように定義する :

$$\begin{cases} P_n = \lambda_n P_{n-1} + P_{n-2} & (P_0 = 1, P_1 = \lambda_1), \\ Q_n = \lambda_n Q_{n-1} + Q_{n-2} & (Q_0 = 0, Q_1 = 1). \end{cases}$$

この数列に対し, 次のことが成り立つ :

定理 1.5 $n \in \mathbb{N}$ に対し,
(1) $[\lambda_1, \lambda_2, \cdots] = \frac{P_n}{Q_n}$.
(2) $P_n Q_{n-1} - P_{n-1} Q_n = (-1)^n$.

次に, 無理数に対して同値関係を定義する.

定義 1.6 $\alpha, \beta \in \mathbb{R}\backslash\mathbb{Q}$ とする.

(1) $\alpha \overset{+}{\sim} \beta \overset{\text{def}}{\iff} \beta = \dfrac{p\alpha+q}{r\alpha+s}$ かつ $ps-qr=1$ となる $p,q,r,s \in \mathbb{Z}$ が存在する.

(2) $\alpha \overset{-}{\sim} \beta \overset{\text{def}}{\iff} \beta = \dfrac{p\alpha+q}{r\alpha+s}$ かつ $ps-qr=-1$ となる $p,q,r,s \in \mathbb{Z}$ が存在する.

(1) が成り立つときに α と β は**正に同値**であるといい, (2) が成り立つときに α と β は**負に同値**であるという. また, (1) または (2) を満たすときに α と β は**同値**であるといい, $\alpha \sim \beta$ とかく.

この同値に対して成り立つことを 2 つ述べておく :

命題 1.7 $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ を連分数展開し, 定理 1.5 により,

$$\alpha = \frac{P_n\alpha_n + P_{n-1}}{Q_n\alpha_n + Q_{n-1}}$$

かつ

$$P_nQ_{n-1} - P_{n-1}Q_n = (-1)^n$$

を得る. このとき, n が偶数ならば $\alpha \overset{+}{\sim} \alpha_n$ であり, n が奇数ならば $\alpha \overset{-}{\sim} \alpha_n$ である.

定理 1.8 $\alpha, \beta \in \mathbb{R}\backslash\mathbb{Q}$ をとり, それぞれを連分数展開を,

$$\alpha = [a_0, a_1, \cdots, a_{l-1}, \alpha_l],$$
$$\beta = [b_0, b_1, \cdots, b_{m-1}, \beta_m]$$

とする.
(1) $\alpha \sim \beta$ ならば, $\alpha_l = \beta_m$ となる $l, m \in \mathbb{Z}_{\geq 0}$ が存在する.
(2) $\alpha \overset{+}{\sim} \beta$ ならば, (1) の l, m はどちらも奇数になるか偶数になるかのどちらかであり, $\alpha \overset{-}{\sim} \beta$ ならば, l, m は一方は偶数でもう一方は奇数になる.

1.2 可換環論から

この節では, 可換環論について準備していく. この節での目標はデデキント整域であり, この整域が非常に重要な概念である.

注意 1.9 環は乗法の単位元 1 を含む可換環であることを仮定する.

定義 1.10 R を環とする. $\alpha \in R$ が**単数** (**単元**ともいう) $\overset{\text{def}}{\iff}$ $\alpha\beta = 1$ となる $\beta \in R$ が存在する.
また, R の単数全体の集合は群をなす. その群を $R^\times$ とかく.

定義 1.11 環 R が**整域** $\overset{\text{def}}{\iff}$ $\alpha\beta = 0$ となる $\alpha, \beta \in R$ に対し, $\alpha = 0$ または $\beta = 0$ が成り立つ.

次に, イデアルを定義する.

定義 1.12 R を環とする. $\emptyset \neq I \subset R$ が R の**イデアル** $\overset{\text{def}}{\iff}$ 以下の条件を満たす :
(1) $\alpha, \beta \in I$ ならば $\alpha + \beta \in I$;
(2) $\alpha \in I, r \in R$ ならば $r\alpha \in I$.

定義 1.13 R を環とする.
(1) R のイデアル I が**素イデアル** $\overset{\text{def}}{\iff}$
$\alpha\beta \in I$ となる $\alpha, \beta \in R$ に対し, $\alpha \in \mathfrak{P}$ または $\beta \in \mathfrak{P}$ が成り立つ.
(2) D のイデアル I が**極大イデアル** $\overset{\text{def}}{\iff}$
$I \subset J \subset D$ となる R のイデアル J に対し, $J = D$ または $J = I$ が成り立つ.

素イデアルと極大イデアルに対し, 次の性質が成り立つ :

命題 1.14 極大イデアルならば素イデアルである.

注意 1.15 命題 1.14 の逆は一般には成り立たない. 例えば, $\mathbb{Z}$ 上の 1 変数多項式環 $\mathbb{Z}[X]$ のイデアル (X) は素イデアルであるが, 極大イデアルではない例の 1 つである.

一般に, イデアルは複数の元で生成されているが, 特にすべてのイデアルが 1 つの元で生成される整域を次に定義する.

定義 1.16 イデアルが単項生成となるとき**単項イデアル**という. また, すべてのイデアルが単項イデアルである整域を**単項イデアル整域 (PID)** という.

例 1.17 $\mathbb{Z}, \mathbb{Z}[\sqrt{-1}]$ は PID だが, $\mathbb{Z}[\sqrt{-5}]$, $\mathbb{Z}[\sqrt{-6}]$ は PID ではない.

次に, デデキント整域を定義する上で重要になる環について述べる.

定義 1.18 環 R が**ネーター環**である $\overset{\text{def}}{\iff}$ すべての R のイデアルの昇鎖

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$$

が定留的である.

この環について, 次が成り立つ :

命題 1.19 環 R に対し, 以下は同値である :
(1) R はネーター環である ;
(2) R のすべてのイデアルが有限生成である.

これから, デデキント整域を定義していく. その前に, 商体を定義する.

定義 1.20 整域 D に対し, 次の集合 $Q(D)$ で D の商体を定義する :

$$Q(D) := \left\{ \frac{a}{b} \,\middle|\, a, b \in D, b \neq 0 \right\}.$$

デデキント整域を定義する上で重要な概念である, 整閉について定義する.

定義 1.21 R を環とし, S を R の部分環と仮定する.
(1) $\alpha \in R$ が S **上整** $\overset{\text{def}}{\iff}$ $f(\alpha) = 0$ となる S 上の多項式で最高次係数が 1 である $f(X)$ が存在する.
(最高次係数が 1 である多項式を**モニック多項式**という)
(2) S が D において**整閉**である $\overset{\text{def}}{\iff}$ $\alpha \in S$ が D 上整ならば, $\alpha \in D$ である.

以上, 定義 1.19, 定義 1.21 から, デデキント整域が定義できる.

定義 1.22 整域 D が**デデキント整域**である $\overset{\text{def}}{\Longleftrightarrow}$ 以下の 3 つの条件を満たす：
(1) D はネーター整域である；
(2) (0) でない D の素イデアルは極大イデアルである；
(3) D は商体 $Q(D)$ 内で整閉である.

デデキント整域では, 次が成り立つ：

命題 1.23 D をデデキント整域とする. 以下は同値である：
(1) D は PID；
(2) D は UFD. [1]

一般の整域では PID ならば UFD は成り立つが, その逆は成り立たない. しかし, デデキント整域ではその逆も成り立つことを意味している.
次に, このデデキント整域の特徴づけを行う. そのために, 分数イデアルの概念を導入する.

定義 1.24 D を整域とする. $\emptyset \neq I \subset Q(D)$ が D の**分数イデアル** $\overset{\text{def}}{\Longleftrightarrow}$ 以下の 3 つの条件を満たす：
(1) $\alpha, \beta \in I$ ならば, $\alpha + \beta \in I$；
(2) $\alpha \in I, r \in D$ ならば, $r\alpha \in I$；
(3) $\gamma I \subset D$ となる $\gamma \in D \setminus \{0\}$ が存在する.

注意 1.25 分数イデアルは定義 1.12 で定義したイデアルにはならない. 区別するために, イデアルを整イデアルとも呼ぶこともある. 一般に整イデアルは分数イデアルである.

定義 1.26 D を整域とする. D の分数イデアル I が**可逆** $\overset{\text{def}}{\Longleftrightarrow}$ $IJ = D$ となる D の分数イデアル J が存在する.

この可逆の概念を導入することにより, 次の命題が示せる：

命題 1.27 デデキント整域 D の (0) でないすべてのイデアルは可逆である.

この命題を使って, 次のデデキント整域の最大の特徴である定理を示せる：

定理 1.28 デデキント整域 D のすべての真の整イデアルは一意に素イデアル分解できる.

定理 1.28 から, デデキント整域の特徴づけが可能になる.

定理 1.29 整域 D に対し, 以下の 5 つは同値である：
(1) D はデデキント整域である；
(2) すべての真の D の整イデアルは一意に素イデアル分解でき, (0) でないすべての D の素イデアルは可逆である；
(3) (0) でないすべての D の整イデアルは可逆である；
(4) (0) でないすべての D の分数イデアルは可逆である；
(5) (0) でない D の分数イデアル全体の集合はイデアルの乗法に関して, アーベル群をなす.

[1] UFD とは一意分解整域と呼ばれる整域で, 単数を除く任意の元が既約元で一意に分解される.

1.3　代数的整数論から

この節では, 代数的整数論について述べていく. 代数体に関する様々な概念の定義や定理を準備していく. 特に, この後で大切になってくるものがイデアル類群とその位数の有限性, ディリクレの単数定理である.

定義 1.30 (1) $\alpha \in \mathbb{C}$ が**代数的数** $\overset{\text{def}}{\iff} f(\alpha) = 0$ となる $\mathbb{Q}$ 上の多項式 $f(X)$ が存在する.
代数的数全体の集合を $\overline{\mathbb{Q}}$ とかく.
(2) $\alpha \in \mathbb{C}$ が**代数的整数** $\overset{\text{def}}{\iff} \alpha$ は $\mathbb{Z}$ 上整.
代数的整数全体の集合を $\overline{\mathbb{Z}}$ とかく.

例 1.31 (1) $a + bi$ $(a, b \in \mathbb{Q})$ は代数的数であるが, e, π は代数的数でない.
(2) $a + bi$ $(a, b \in \mathbb{Z})$ は代数的整数であるが, q $(q \in \mathbb{Q}\backslash\mathbb{Z})$ は代数的整数ではない.

$\overline{\mathbb{Q}}, \overline{\mathbb{Z}}$ については, 次のことが知られている :

命題 1.32 (1) $\overline{\mathbb{Q}}$ は代数的閉体である.
(2) $\overline{\mathbb{Z}}$ は $\mathbb{C}$ の部分環である.

$\overline{\mathbb{Q}}$ と $\overline{\mathbb{Z}}$ を使って代数体とその整数環を定義する.

定義 1.33 F は**代数体** $\overset{\text{def}}{\iff} F$ は $\overline{\mathbb{Q}}$ の部分体で $\mathbb{Q}$ 上有限次な体.
また, $F \cap \overline{\mathbb{Z}}$ を代数体 F の**整数環**といい, $\mathfrak{O}_F$ と表す.

次に, 環論の概念から離れて, ノルムやトレース, 判別式について定義する. これは代数的整数論では重要な概念である. そのために, 埋め込みを導入する.

定義 1.34 F を代数体とする. $f : F \to \mathbb{C}$ の $\mathbb{Q}$-単射準同型写像のことを F の**埋め込み**という.
さらに, $\mathrm{Im} f \subset \mathbb{R}$ となる F の埋め込みを F の**実埋め込み**といい, そうでないとき, F の**虚埋め込み**という.

この埋め込みについて, 次が成り立つ :

命題 1.35 $\mathbb{Q}$ 上 n 次代数体 F の埋め込みは n 本ある. また, F の実埋め込みの数を r_1, 虚埋め込みの数を r_2 とすれば, $n = r_1 + 2r_2$ が成り立つ.

埋め込みが定義できても, どのような写像になっているのかわからない. しかし, 代数体 F は $\mathbb{Q}(\alpha)$ となる $\alpha \in \mathfrak{O}_F$ が存在するため, この α がどのように写るかによる. 実際, α は恒等写像でなければ $\mathbb{Q}$ 上の最小多項式の別の根に写るしかない. ここで, α の $\mathbb{Q}$ 上の最小多項式とは, α を根にもつような $\mathbb{Q}$ 上既約な最小次数のモニック多項式のことである. $\mathbb{Q}$ 上の最小多項式は, $\mathbb{Q}$ を一般の代数体上の最小多項式に拡張できる.

例 1.36 $F = \mathbb{Q}(\sqrt[3]{2})$ とする. F の埋め込みは $\sqrt[3]{2}$ がどのように写るかによる. θ を F の埋め込みとするとき, $\theta(\sqrt[3]{2}) = \sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}{\zeta_3}^2$ となる.
$\sqrt[3]{2}$ の $\mathbb{Q}$ 上の最小多項式は $x^3 - 2$ であるから, $\sqrt[3]{2}$ の θ による像は $\sqrt[3]{2}$ の $\mathbb{Q}$ 上の最小多項式の根になっている.

埋め込みから, まずは元のノルム, トレースについて定義できる.

定義 1.37 F を $\mathbb{Q}$ 上 n 次代数体, $j=1,\cdots,n$ に対し θ_j を F の埋め込みとする. $\alpha\in F$ に対し

$$N_F(\alpha):=\prod_{i=1}^{n}\theta_i(\alpha)$$

を α の **(絶対) ノルム**といい,

$$T_F(\alpha):=\sum_{i=1}^{n}\theta_i(\alpha)$$

を α の **(絶対) トレース**という.

定理 1.38 F を代数体とすると, $\alpha,\beta\in F$ に対し, 以下が成り立つ :
(1) $N_F(\alpha),T_F(\alpha)\in\mathbb{Q}$;
(2) $N_F(\alpha\beta)=N_F(\alpha)N_F(\beta)$;
(3) $T_F(\alpha+\beta)=T_F(\alpha)+T_F(\beta)$.

基礎体である $\mathbb{Q}$ を上げ一般の代数体 F 上でも, 同じように埋め込みを考えることができ, ノルム, トレースを定義できる.

定義 1.39 基礎体を代数体 F とし, K を F 上 n 次代数体とすると, K は F 不変の埋め込みを n 本もつ. それらを $\theta_1,\cdots,\theta_n$ とすると, $\alpha\in K$ に対し,

$$N_{K/F}(\alpha):=\prod_{i=1}^{n}\theta_i(\alpha)$$

を α の **(相対) ノルム**といい,

$$T_{K/F}(\alpha):=\sum_{i=1}^{n}\theta_i(\alpha)$$

を α の **(相対) トレース**という. 特に, $F=\mathbb{Q}$ の時は, 定義 1.37 と同じである. 相対ノルム, 相対トレースは F の元であり, 定理 1.38 と同じような推移律が成り立つ.

絶対ノルムについては, 元が単数かどうかを判定することができる :

命題 1.40 代数体 F に対し, 以下は同値である :
(1) $\alpha\in\mathfrak{O}_F^{\times}$;
(2) $|N_F(\alpha)|=1$.

次に, 代数体の判別式について定義する. その前に, 基底の判別式を定義する.

定義 1.41 F を $\mathbb{Q}$ 上 n 次代数体とすると, F は $\mathbb{Q}$ 上の基底 $\mathfrak{B}=\{\alpha_1,\cdots,\alpha_n\}$ をもつ.
$j=1,\cdots,n$ に対し, θ_j を F の埋め込みとするとき,

$$\mathrm{disc}(\mathfrak{B}):=\det\begin{pmatrix}\theta_1(\alpha_1) & \cdots & \theta_1(\alpha_i) & \cdots & \theta_1(\alpha_n)\\ \vdots & \ddots & & & \vdots\\ \theta_j(\alpha_1) & \cdots & \theta_j(\alpha_i) & \cdots & \theta_j(\alpha_n)\\ \vdots & & & \ddots & \vdots\\ \theta_n(\alpha_1) & \cdots & \theta_n(\alpha_i) & \cdots & \theta_n(\alpha_n)\end{pmatrix}^2$$

を $\mathfrak{B}$ の**判別式**という.

一般に, $\mathbb{Q}$ 上 n 次代数体 F の整数環 $\mathfrak{O}_F$ は, 階数 n の自由 $\mathbb{Z}$ 加群である. つまり, $\mathbb{Z}$ 上の基底 $\mathfrak{B}' = \{\alpha'_1, \cdots, \alpha'_n\}$ をもつ. この基底を**整基底**という. 整基底により, 代数体の判別式が定義できる.

定義 1.42 代数体 F に対し, F の整基底 $\mathfrak{B}' = \{\alpha'_1, \cdots, \alpha'_n\}$ の判別式 $\mathrm{disc}(\mathfrak{B}')$ を F **の判別式**といい, Δ_F とかく.

後で述べるが, 素数を代数体に持ち上げたときに, その素数が代数体で分岐するための必要十分条件に判別式が使われる.

一般に, 代数体の判別式については次が成り立つ :

定理 1.43 K, F を代数体とする.
(1) $F \subset K$ ならば $\Delta_F \mid \Delta_K$.
(2) $\Delta_F \equiv 0, 1 \pmod 4$ かつ $|\Delta_F| \geq 1$ を満たす.
(3) $F = \mathbb{Q} \Longleftrightarrow \Delta_F = 1$.

ここで, 様々な代数体の判別式の例を挙げておく.

例 1.44 (1) $\mathbb{Q}$ 上の 2 次体の判別式は第 2 章で求めている.
(2) p を素数, $a \in \mathbb{N}$ とする. このとき, p^a 分体 $F = \mathbb{Q}(\zeta_{p^a})$ の判別式 Δ_F は,

$$\Delta_F = (-1)^{\frac{\phi(p^a)}{2}} p^{p^{a-1}(a(p-1)-1)}$$

である. [2]
(3) 行列のクロネッカー積を使うことにより, 一般の円分体の判別式を求めることができる. すなわち, $n \in \mathbb{N}$ を $n = \prod_{i=1}^{r} p_j^{a_j}$ と素因数分解したときに, $F = \mathbb{Q}(\zeta_n)$ の判別式 Δ_F は,

$$\Delta_F = \frac{(-1)^{\frac{r\phi(n)}{2}} n^{\phi(n)}}{\prod_{i=1}^{r} p_j^{\frac{\phi(n)}{p_j - 1}}}$$

である.

次に, イデアルのノルムについて定義する.

定義 1.45 F を代数体, I を F の整数環 $\mathfrak{O}_F$ のイデアルとする.

$$N^F(I) := |\mathfrak{O}_F / I|$$

をイデアル I **のノルム**という.

定理 1.46 I, J を代数体 F の整数環 $\mathfrak{O}_F$ のイデアルとすると, 以下が成り立つ :
(1) $N^F(IJ) = N^F(I)N^F(J)$;
(2) $\alpha \in \mathfrak{O}_F$ に対し, $I = (\alpha)$ ならば, $N^F(I) = |N_F(\alpha)|$ である.

注意 1.47 注意 1.39 と同様に, 定義 1.45 で定義したノルムは基礎体が $\mathbb{Q}$ であるが, 基礎体 $\mathbb{Q}$ を上げ, 一般の代数体 F 上でも同じようにイデアルのノルムを考えることができる. このノルムについては, ヒルベルトの理論で説明する.

[2] ζ_n は 1 の原始 n 乗根のことである. すなわち n 乗してはじめて 1 になる数のことである. また, $\phi(n)$ は, n のオイラー関数を表している.

イデアルのノルムと判別式には次のような関係がある：

定理 1.48 $I \neq (0)$ を代数体 F の整数環 $\mathfrak{O}_F$ のイデアルで $\mathbb{Z}$ 上の基底 $\mathfrak{B} = \{\alpha_1, \cdots, \alpha_n\}$ をもつと仮定すると,

$$N^F(I)^2 = \frac{\mathrm{disc}(\mathfrak{B})}{\Delta_F}$$

が成り立つ.

話を整数環に戻す. 一般に, 代数体 F の整数環 $\mathfrak{O}_F$ について, 次のことがいえる：

定理 1.49 代数体 F の整数環 $\mathfrak{O}_F$ はデデキント整域である.

定理 1.49 により, (0) でない整数環のイデアルは素イデアルに一意に素イデアル分解されることが分かった. 素イデアル分解についての理論がヒルベルトの理論であり, この後に載っている.

また, 定理 1.29 より (0) ではない代数体の整数環の分数イデアル全体の集合はアーベル群をなすことも分かった. 代数体 F が与えられたときに, (0) ではない分数イデアル全体のなすアーベル群を I_F とかき, それの部分群である単項分数イデアルからなる群を P_F とかく. これで, I_F を割ったアーベル群がイデアル類群である. 簡単にいえば, イデアルと数のずれを表す群になっている.

定義 1.50 F を代数体とする. $Cl_F := I_F/P_F$ を F の**イデアル類群**という.

注意 1.51 代数体 F の整数環 $\mathfrak{O}_F$ の分数イデアル I, J に対し, 次のような同値関係を導入する：

$$I \sim J \overset{\text{def}}{\iff} (\alpha)I = (\beta)J \text{ となる } \alpha, \beta \in \mathfrak{O}_F \text{ が存在する.}$$

この同値関係により, I_F を割った群をイデアル類群と見ることができ, 上の定義と同じであることがわかる.

次の命題は明らかであるが, PID であるための必要十分条件になっている：

命題 1.52 代数体 F に対し, $Cl_F = \{1\} \iff F$ の整数環 $\mathfrak{O}_F$ は PID.

イデアル類群の位数が有限かどうかについては, 数の幾何と呼ばれる概念を使えば示すことができる. 次の結果がそれであり, とても重要な結果である：

定理 1.53 代数体 F に対し, $|Cl_F| < \infty$ である.

代数体 F のイデアル類群 Cl_F の位数を F の**類数**といい, h_F とかく. 第 2 章では 2 次体についてではあるが, それを 2 元 2 次形式という別の概念を使って求めている.

この節の最後に, ディリクレの単数定理について述べる. これは, 命題 1.40 からペル方程式などの方程式の解の構造が分かるという有用な定理である.

定理 1.54 (ディリクレの単数定理) $\mathbb{Q}$ 上 n 次代数体 F に対し, F の実埋め込み, 虚埋め込みの数をそれぞれ r_1, r_2 とする. さらに, 複素数平面の単位円上にある F の整数環 $\mathfrak{O}_F$ の単数の位数を m とすると,

$$\mathfrak{O}_F^\times \simeq \mathbb{Z}^{r_1+r_2-1} \times \langle \zeta_m \rangle \simeq \langle u_1 \rangle \times \cdots \times \langle u_{r_1+r_2-1} \rangle \times \langle \zeta_m \rangle$$

となる $u_1, \cdots, u_{r_1+r_2-1} \in \mathfrak{O}_F^\times$ が存在する. この単数のことを**基本単数**という.

1.4　ガロア理論から

この節では, ガロア理論について準備する. これは, 次の節であるヒルベルトの分岐理論を述べるためにも重要であり, 数論を勉強していくためには, 必要不可欠な道具の一つでもある.

前の節で代数体 F の埋め込みについて定義したが, これの写した先を自分自身に制限する写像を考える. まず, その写像について定義する.

定義 1.55 K/F を体の拡大とする.
(1) $f : K \to K$ となる準同型写像のことを**自己同型写像**という. K の自己同型写像全体の集合は写像の合成に関して群をなす. この群を K の**自己同型群**といい, $\mathrm{Aut}(K)$ とかく.
(2) $\mathrm{Aut}(K)$ のうち, F 不変なものを **F-自己同型写像**という. K の F-自己同型写像全体の集合もまた写像の合成に関して群をなす. この群を **F-自己同型群**といい, $\mathrm{Aut}(K/F)$ とかく.

ここで, 自己同型群で動かない体を考える. この体を**不変体**という. 例 1.36 に対しては, $\mathrm{Aut}(F/\mathbb{Q}) = \{\mathrm{id}\}$ であるから, 代数体の拡大 $F/\mathbb{Q}$ における, $\mathrm{Aut}(F/\mathbb{Q})$ による不変体は F である.

しかし, F の拡大体 $K = F(\zeta_3)$ を考えると, 代数体の拡大 $K/\mathbb{Q}$ における $\mathrm{Aut}(K/\mathbb{Q})$ による不変体は $\mathbb{Q}$ となる. これが $\mathbb{Q}$ 上ガロア拡大の例の 1 つである.

一般に体の拡大 K/F に対し, $G = \mathrm{Aut}(K/F)$ とおいたとき, G による K の不変体を K^G とかく.

定義 1.56 K/F を体の有限次拡大, $G = \mathrm{Aut}(K/F)$ とする. K/F が**ガロア拡大** $\overset{\mathrm{def}}{\iff} K^G{=}F$.

このとき, G を**ガロア群**といい, $\mathrm{Gal}(K/F)$ とかく.

体の有限次拡大 K/F がガロア拡大のとき, ガロア群の位数は次のようになる :

定理 1.57 体の有限次拡大 K/F がガロア拡大のとき, $|\mathrm{Gal}(K/F)| = |K : F|$.

他の本では, 正規拡大や分離拡大を使って定義している. しかし, それらと上の定義が同値であることが次の命題から示される.

命題 1.58 体の有限次拡大 K/F に対して, 以下は同値である :
(1) K/F はガロア拡大 ;
(2) K/F は正規拡大かつ分離拡大 ;
(3) K/F は F 上のある分離多項式の最小分解体である.

注意 1.59 (2) において, F の標数が 0 の場合は, すべての拡大 K/F は分離拡大であることが示される. つまり, 標数が 0 の場合はガロア拡大かどうかを調べるには, 正規拡大かどうかを見ればよい.

次から, このガロア群に関する基本的な定理をいくつか述べていく. まずは, ガロアの基本定理について述べる. これは体と群が 1 対 1 に対応しているという定理である.

定理 1.60 (ガロア理論の基本定理) K/F をガロア拡大とし, $G = \mathrm{Gal}(K/F)$ とおく.
(1) K/F の任意の中間体 L に対して, K/L はガロア拡大.
(2) $\mathfrak{F}$ を K/F の中間体全体の集合, $\mathfrak{G}$ を G の部分群全体の集合とする. ここで, 写像 ϕ を,

$$\begin{array}{ccccc} \phi & : & \mathfrak{F} & \longrightarrow & \mathfrak{G} \\ & & \cup & & \cup \\ & & L & \longmapsto & \mathrm{Gal}(K/L) \end{array}$$

と定義し, 写像 ψ を

$$\begin{array}{ccccc} \psi & : & \mathfrak{G} & \longrightarrow & \mathfrak{F} \\ & & \cup & & \cup \\ & & H & \longmapsto & K^H \end{array}$$

と定義する. このとき, 写像 $\phi = \psi^{-1}$ である.
また, $H_1, H_2 \in \mathfrak{G}$ に対して,

$$\psi(H_1) \subset \psi(H_2) \Longleftrightarrow \phi(\psi(H_1)) = H_1 \supset H_2 = \phi(\psi(H_2))$$

が成り立つ. つまり, ガロア群と不変体の包含関係は逆になる.
さらに,

$$|\psi(H_2) : \psi(H_1)| = |H_1 : H_2|$$

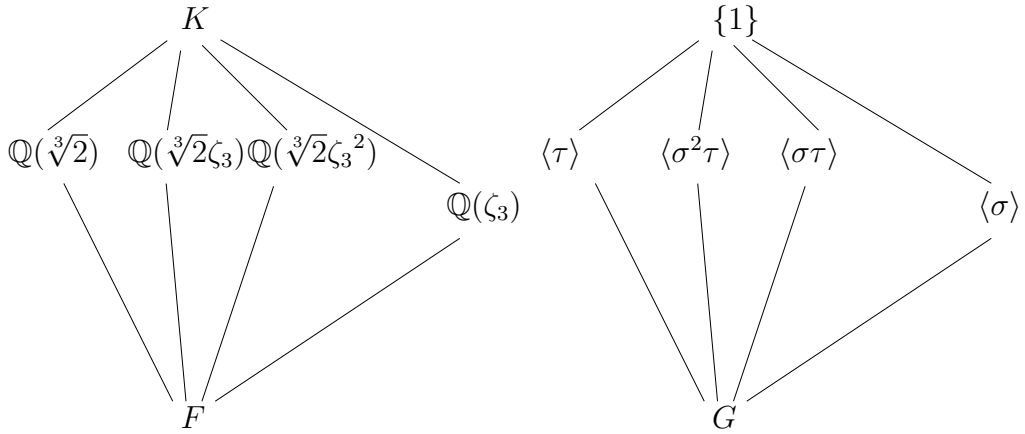
である.
(3) L を K/F の中間体とするとき, L/F はガロア拡大 $\Longleftrightarrow \mathrm{Aut}(K/L) \lhd G$.
($\mathrm{Aut}(K/L)$ は G の正規部分群であることをいっている)
さらに, L/F がガロア拡大ならば,

$$\mathrm{Gal}(L/F) \simeq \mathrm{Gal}(K/F)/\mathrm{Gal}(K/L)$$

が成り立つ.

主張だけではわからないので, ガロア拡大の例である $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ について考える.

例 1.61 $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3), F = \mathbb{Q}$ とおく. K/F はガロア拡大であり. $G = \mathrm{Gal}(K/F) = \langle \sigma, \tau \rangle \simeq S_3$ である. ただし, $\sigma : \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3$, $\tau : \zeta_3 \mapsto \zeta_3^2$ のように写す K の F-自己同型写像とする.
よって, これらによる群と体の対応は以下のようになる. このような対応を**ガロア対応**という. 群の包含関係は逆であることに注意する.



すると, 定理 1.60 (2) の写像を使えば, それぞれのハッセ図は対応していることがわかる. 主に, ガロア群が有限群のとき, それに対応する中間体を求めるときに使っていく.

最後に, このガロア群に対する定理を述べておく. この定理は第 3 章で述べるクロネッカー・ウェーバーの定理の証明で使う.

定理 1.62 $j=1,2$ に対し, K_j/F を有限次ガロア拡大とすると, 以下が成り立つ :
(1) $K_1K_2/K_1, K_1K_2/K_2$ はガロア拡大であり,

$$\mathrm{Gal}(K_1K_2/K_j) \simeq \mathrm{Gal}(K_j/K_1 \cap K_2) ;$$

(2) $K_1K_2/K_1 \cap K_2$ はガロア拡大であり,

$$\mathrm{Gal}(K_1K_2/K_1 \cap K_2) \simeq \mathrm{Gal}(K_1/K_1 \cap K_2) \times \mathrm{Gal}(K_2/K_1 \cap K_2) ;$$

(3) K_1/F, K_2/F がどちらもアーベル拡大[3] ならば, K_1K_2/F もアーベル拡大である.

1.5 ヒルベルトの理論から

基礎体が $\mathbb{Q}$ である代数体の拡大を**絶対拡大**といい, 基礎体が一般の代数体 $F \neq \mathbb{Q}$ である代数体の拡大を**相対拡大**という. この節では, 基礎体が $\mathbb{Q}$ のときだけではなく, 一般の代数体 F に対して展開させていく理論について述べていく.

代数体の拡大 K/F に対し, F の整数環 $\mathfrak{O}_F$ の素イデアル $\mathfrak{p}$ を K の整数環 $\mathfrak{O}_K$ に上げて考えることができる. 定理 1.49 より, $\mathfrak{p}$ を $\mathfrak{O}_K$ で素イデアル分解することが可能である. そのときに, $\mathfrak{p}$ が $\mathfrak{O}_K$ の素イデアルになったりならなかったりする. このことについて簡単な例を挙げる.

例 1.63 代数体の拡大 $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ を考える. ($\mathfrak{O}_{\mathbb{Q}} = \mathbb{Z}$, $\mathfrak{O}_{\mathbb{Q}(\sqrt{-1})} = \mathbb{Z}[\sqrt{-1}]$ である)
(a) $p_1 = (2)$ は $\mathbb{Z}$ の素イデアルであり, $\mathbb{Z}[\sqrt{-1}]$ まで上げて分解を考えると, $p = (1+\sqrt{-1})^2$ となる.
(b) $p_2 = (5)$ については, $p_2 = (2+\sqrt{-1})(2-\sqrt{-1})$ と分解される.
(c) $p_3 = (7)$ については, $\mathbb{Z}[\sqrt{-1}]$ でも素イデアルのままである.

1.5.1 完全分岐, 完全分解, 惰性

一般に, (a) のようになることを完全分岐, (b) のようになることを完全分解, (c) のようになることを惰性という. 形式的に定義するために, まず, 分岐指数, 分解数, 惰性次数を定義する.

定義 1.64 K/F を代数体の拡大, $\mathfrak{p}$ を F の整数環 $\mathfrak{O}_F$ の素イデアルとする. $\mathfrak{p}$ を K の整数環 $\mathfrak{O}_K$ に上げて分解したとき,

$$\mathfrak{p}\mathfrak{O}_K = \prod_{j=1}^{g} \mathfrak{P}_j^{e_j}$$

と分解したとする.
(1) e_j を $\mathfrak{P}_j$ の**分岐指数**といい, $e_{K/F}(\mathfrak{P}_j)$ と表す.
(2) g を $\mathfrak{p}$ の**分解数**といい, $g_{K/F}(\mathfrak{p})$ と表す.
(3) 体の拡大次数 $|\mathfrak{O}_K/\mathfrak{P}_j : \mathfrak{O}_F/\mathfrak{p}|$ を $\mathfrak{P}_j$ の**相対次数**といい, $f_{K/F}(\mathfrak{P}_j)$ と表す.

[3]ガロア拡大 K/F がアーベル拡大であるとは, そのガロア群 $\mathrm{Gal}(K/F)$ がアーベル群であるということである. またガロア群 $\mathrm{Gal}(K/F)$ が巡回群になるとき, ガロア拡大 K/F は巡回拡大であるという.

この分岐指数, 分解数, 相対指数を定義できたのでイデアルのノルムを基礎体を一般の代数体にして定義することができる.

注意 1.65 K/F を代数体の拡大, $\mathfrak{P}$ を K の整数環 $\mathfrak{O}_K$ の素イデアルとすると, $\mathfrak{P} \cap \mathfrak{O}_F$ は F の整数環 $\mathfrak{O}_F$ の素イデアルである.

定義 1.66 K/F を代数体の拡大, $\mathfrak{P}$ を K の整数環 $\mathfrak{O}_K$ の素イデアルとし, $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{O}_F$ とする.
このとき,

$$N^{K/F}(\mathfrak{P}) := \mathfrak{p}^{f_{K/F}(\mathfrak{P})}$$

を $\mathfrak{P}$ の **(相対) ノルム**という.

これは, K の整数環 $\mathfrak{O}_K$ の分数イデアルに拡張できる. I を K の整数環 $\mathfrak{O}_K$ の分数イデアルとし, I の素イデアル分解を,

$$I = \prod_{j=1}^{n} {\mathfrak{P}_j}^{a_j}$$

とすると, I の相対ノルムは,

$$N^{K/F}(I) = \prod_{j=1}^{n} {\mathfrak{p}_j}^{a_j f_{K/F}(\mathfrak{P}_j)}$$

と拡張できる. 特に $F = \mathbb{Q}$ のときは, 定義 1.45 をイデアルで表したものになる.

分岐指数, 惰性指数については次の推移律が成り立つ :

命題 1.67 $F \subset L \subset K$ となる代数体の塔をとる. $\mathfrak{P}$ を K の整数環 $\mathfrak{O}_K$ の素イデアルとし, $\mathfrak{P}' = \mathfrak{P} \cap \mathfrak{O}_L$ とおく.
(1) $e_{K/F}(\mathfrak{P}) = e_{K/L}(\mathfrak{P}) e_{L/F}(\mathfrak{P}')$.
(2) $f_{K/F}(\mathfrak{P}) = f_{K/L}(\mathfrak{P}) f_{L/F}(\mathfrak{P}')$.

惰性指数により, 分岐について定義できる.

定義 1.68 定義 1.64 において, $e_{K/F}(\mathfrak{P}_j) \geq 2$ のとき, $\mathfrak{P}_j$ は**分岐する**という.
また, $e_{K/F}(\mathfrak{P}_j) = 1$ のとき, $\mathfrak{P}_j$ は**不分岐である**という.

分岐指数, 分解数, 惰性指数には次のような関係が成り立つ :

定理 1.69 K/F を代数体の拡大とする. F の整数環 $\mathfrak{O}_F$ の素イデアル $\mathfrak{p}$ を K の整数環 $\mathfrak{O}_K$ に上げたとき,

$$\mathfrak{p}\mathfrak{O}_K = \prod_{j=1}^{g} {\mathfrak{P}_j}^{e_j}$$

と分解したとする. 簡単のため, $e_j = e_{K/F}(\mathfrak{P}_j)$, $f_j = f_{K/F}(\mathfrak{P}_j)$, $g = g_{K/F}(\mathfrak{p})$ とおくと,

$$\sum_{j=1}^{g} e_j f_j = |K : F|$$

となる. さらに, K/F がガロア拡大のときは, 分岐指数と相対次数は一定になる. つまり, $j \neq k$ に対し, $e_j = e_k, f_j = f_k$ となり, $e_j = e, f_j = f$ とすると,

$$efg = |K : F|$$

である.

次に完全分解, 完全分岐, 惰性を定義する.

定義 1.70 K/F を代数体の拡大, $\mathfrak{p}$ を F の整数環 $\mathfrak{O}_F$ の素イデアルとする. $\mathfrak{p}$ を K の整数環 $\mathfrak{O}_K$ に上げたとき,

$$\mathfrak{p}\mathfrak{O}_K = \prod_{j=1}^{g} \mathfrak{P}_j{}^{e_j}$$

と分解したとする.
(1) $\mathfrak{p}$ は**完全分岐する** $\overset{\text{def}}{\iff}$ $e_{K/F}(\mathfrak{P}_j) = |K : F|$ となる j が存在する.
(2) $\mathfrak{p}$ は**完全分解する** $\overset{\text{def}}{\iff}$ $g_{K/F}(\mathfrak{p}) = |K : F|$.
(3) $\mathfrak{p}$ は**惰性する** $\overset{\text{def}}{\iff}$ 任意の $1 \leq j \leq g$ に対し, $f_{K/F}(\mathfrak{P}_j) = |K : F|$.

定理 1.69 により, 次のことがわかる :

系 1.71 K/F を代数体の素数次ガロア拡大とすると, 定理 1.69 より F の整数環 $\mathfrak{O}_F$ の素イデアルは K の整数環 $\mathfrak{O}_K$ で分解すると, 完全分解するか完全分岐するか惰性するかの 3 通りしかない.

1.5.2 共役差積と相対判別式

この節では相対判別式などについて述べていく. 最も重要になってくるものが共役差積と判別式であり, これらは第 3 章以降で重要な役割をもつ. まず, 双対集合について述べていく.

定義 1.72 D を商体 $Q(D)$ が代数体 F となる整域とし, K を F の拡大体となる代数体とする. $M \subset K$ に対して,

$$M^* := \left\{\alpha \in K \mid T_{K/F}(\alpha M) \subset D\right\}$$

を M の**双対集合**という.

定義より, $M_1 \subset M_2$ ならば $M_1^* \supset M_2^*$ が成り立つことがわかる. さらに, M が次に述べるような特別な場合のときには, M^* が非常に求めやすくなる.

命題 1.73 定義 1.72 の仮定の下, $f(X) \in D[X]$ を α の F 上の最小多項式とするとき,

$$M = D[\alpha] \text{ ならば } M^* = \frac{M}{f'(\alpha)}.$$

注意 1.59 により分離拡大であるから, 前の命題が適用できる. さらに, M を単なる部分集合ではなく, 分数イデアルにすると定理 1.29 により可換性が成り立つから, 次のような性質が得られる :

命題 1.74 K を代数体とする.
(1) J が K の整数環 $\mathfrak{O}_K$ の分数イデアルならば J^* も $\mathfrak{O}_K$ の分数イデアルで, $JJ^* = \mathfrak{O}_K{}^*$ である.
(2) I が K の整数環 $\mathfrak{O}_K$ のイデアルならば, $(I^*)^{-1}$ も $\mathfrak{O}_K$ のイデアルである.

上の命題 1.74 (2) により, 相対拡大での共役差積を定義できる.

定義 1.75 K/F を代数体の拡大, $J \in I_K$ とする. $(J^*)^{-1}$ を F **上** J **の共役差積**といい, $D_{K/F}(J)$ とかく. 特に, $D_{K/F}(\mathfrak{O}_K)$ を**拡大** K/F **の共役差積**といい, 単に $D_{K/F}$ とかく.

この共役差積については, 次のような性質をもつ :

命題 1.76 $F \subset L \subset K$ を代数体の塔とする.
(1) J が K の整数環 $\mathfrak{O}_K$ の分数イデアルならば, $D_{K/F}(J) = JD_{K/F}$.
(2) $D_{K/F} = D_{K/L}D_{L/F}$.

最小多項式の根の差積も共役差積という. 具体的に, 代数体の拡大 K/F に対し, $\alpha \in K$ の F 上の最小多項式を $f(X)$ とおくと, その共役差積は $f'(\alpha)$ である. 拡大 K/F の共役差積 $D_{K/F}$ と元の共役差積は非常に関係ある. それが次の定理である :

定理 1.77 代数体の拡大 K/F に対し, $D_{K/F}$ は任意の $\alpha \in \mathfrak{O}_K$ の共役差積から生成される K の整数環 $\mathfrak{O}_K$ のイデアルである.

この共役差積を使って, 相対拡大における判別式を定義する.

定義 1.78 K/F を代数体の拡大とする. $N^{K/F}(D_{K/F})$ を K/F **の相対判別式**といい, $\Delta_{K/F}$ と表す.

相対判別式には, 次のような性質がある :

命題 1.79 代数体の拡大 $F \subset L \subset K$ とする.
(1) $\Delta_{F/\mathbb{Q}} = (\Delta_F)$.
(2) $\Delta_{K/F} = \Delta_{L/F}^{|K:L|} N^{K/F}(\Delta_{K/L})$.

命題 1.79 (2) を使って 第 4 章で述べる不分岐拡大についてみていくときに, 実際に不分岐拡大かどうかを確かめる. 不分岐拡大についてはこの節の最後に定義する.
この判別式や共役差積により, 前節で述べた分岐する素イデアルがどのような素イデアルか特徴づけできる. それが次の定理である :

定理 1.80 K/F を代数体の拡大とする.
(1) K の整数環 $\mathfrak{O}_K$ の素イデアル $\mathfrak{P}$ が K/F で分岐する $\iff \mathfrak{P} \mid D_{K/F}$.
(2) F の整数環 $\mathfrak{O}_F$ の素イデアル $\mathfrak{p}$ が K で分岐する $\iff \mathfrak{p} \mid \Delta_{K/F}$.

特に, 定理 1.80 において, 素数 p が代数体 K で分岐することは p が K の判別式 Δ_K を割ることと同値であることが命題 1.79 (1) からわかる. 最後に, 不分岐拡大を定義する.

定義 1.81 K/F を代数体の拡大とする.

$$K/F \text{ は不分岐拡大} \overset{\text{def}}{\iff} F \text{ の整数環 } \mathfrak{O}_F \text{ の素イデアルはすべて } K \text{ で分岐しない.}$$

一般に, 基礎体が $\mathbb{Q}$ の場合, 定理 1.43 (3) より不分岐拡大は存在しないことがわかる.

1.5.3　分解群と惰性群, 高次分岐群

この節では, クロネッカー · ウェーバーの定理を証明する上で重要になる分解群と惰性群, 高次分岐群について述べていく. この概念は前節の分解指数や惰性指数と関わりがある. さらに, 完全分解する素イデアルの特徴づけを様々な観点で見ていく.

定義 1.82 K/F を代数体のガロア拡大, $\mathfrak{P}$ を K の整数環 $\mathfrak{O}_K$ の素イデアルとする. $G = \mathrm{Gal}(K/F)$ とおく.
(1)

$$D_{\mathfrak{P}}(K/F) := \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

を $\mathfrak{P}$ の**分解群**という. $\mathfrak{P}$ の分解群による不変体 $K^{D_{\mathfrak{P}}(K/F)}$ を $\mathfrak{P}$ の**分解体**といい, $Z_{\mathfrak{P}}(K/F)$ とかく.
(2)

$$I_{\mathfrak{P}}(K/F) := \{\sigma \in G \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}}\ (\forall \alpha \in \mathfrak{O}_K)\}$$

を $\mathfrak{P}$ の**惰性群**という. $\mathfrak{P}$ の惰性群による不変体 $K^{I_{\mathfrak{P}}(K/F)}$ を $\mathfrak{P}$ の**惰性体**といい, $T_{\mathfrak{P}}(K/F)$ とかく.

注意 1.83 定義 1.82 における mod は, イデアルに対するものである. すなわち, I を環 R のイデアルとする. $\alpha, \beta \in R$ に対し,

$$\alpha \equiv \beta \pmod{I} \overset{\text{def}}{\iff} \alpha - \beta \in I$$

ということを表している.

分解群, 惰性群の性質は次のようである :

定理 1.84 K/F を代数体のガロア拡大, $\mathfrak{P}$ を $\mathfrak{O}_K$ の素イデアルとする. $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{O}_F$ とおく.
(1) $|D_{\mathfrak{P}}(K/F)| = e_{K/F}(\mathfrak{p}) f_{K/F}(\mathfrak{p})$.
(2) $I_{\mathfrak{P}}(K/F) \lhd D_{\mathfrak{P}}(K/F)$.
(3) $|I_{\mathfrak{P}}(K/F)| = e_{K/F}(\mathfrak{p})$.

注意 1.85 $D_{\mathfrak{P}}(K/F)$ は $\mathrm{Gal}(K/F)$ の部分群であるが, 正規部分群ではない場合がある.
もし $D_{\mathfrak{P}}(K/F) \lhd \mathrm{Gal}(K/F)$ ならば, $\mathfrak{O}_F$ の素イデアル $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{O}_F$ は K で完全分解する.

また, 分解体, 惰性体の性質も次のように示される :

命題 1.86 K/F を代数体のガロア拡大, $\mathfrak{P}$ を $\mathfrak{O}_K$ の素イデアルとする. $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{O}_F$ とおく.
(1) $\mathfrak{P}$ の分解体 $Z_{\mathfrak{P}}(K/F)$ は, $\mathfrak{P}_L = \mathfrak{P} \cap \mathfrak{O}_L$ が $\mathfrak{O}_K$ で分解したときに, 素因子が $\mathfrak{P}$ しかないような K/F の最小の中間体 L である.
(2) $\mathfrak{P}$ の分解体 $Z_{\mathfrak{P}}(K/F)$ は, $e_{L/F}(\mathfrak{P}_L) = f_{L/F}(\mathfrak{P}_L) = 1$ となるような K/F の最大の中間体 L である.
(3) $\mathfrak{P}$ の惰性体 $T_{\mathfrak{P}}(K/F)$ は, $e_{L/F}(\mathfrak{P}_L) = 1$ となるような K/F の最大の中間体 L である.
(4) $\mathfrak{P}$ の惰性体 $T_{\mathfrak{P}}(K/F)$ は, $e_{K/L}(\mathfrak{P}) = |K : L|$ となるような K/F の最大の中間体 L である.
(5) $\pi \in \mathfrak{P} \backslash \mathfrak{P}^2$ となる元をとると, $K = T_{\mathfrak{P}}(K/F)(\pi)$ とかける.

さて, 定理 1.84 (2) を示すときに次の群の同型を示すことになる :

$$D_{\mathfrak{P}}(K/F)/I_{\mathfrak{P}}(K/F) \simeq \mathrm{Gal}((\mathfrak{O}_K/\mathfrak{P})/(\mathfrak{O}_F/\mathfrak{p})).$$

ここで, K の整数環 $\mathfrak{O}_K$ の素イデアル $\mathfrak{P}$ が K/F で不分岐のとき $e_{K/F}(\mathfrak{P}) = 1$ であるから, 上の同型は

$$D_{\mathfrak{P}}(K/F) \simeq \mathrm{Gal}((\mathfrak{O}_K/\mathfrak{P})/(\mathfrak{O}_F/\mathfrak{p}))$$

となる. したがって, $\mathfrak{P}$ の分解体 $D_{\mathfrak{P}}(K/F)$ は位数 $f_{K/F}(\mathfrak{P})$ の巡回群となる. この結果から, 数論で重要なフロベニウス自己同型写像, アルティン写像を定義できる.

定義 1.87 K/F を代数体のガロア拡大, $\mathfrak{P}$ を K/F で不分岐な $\mathfrak{O}_K$ の素イデアルとすると, $D_{\mathfrak{P}}(K/F)$ は巡回群で生成元をもつ. この生成元のことを**フロベニウス自己同型写像**といい, $\left(\frac{K/F}{\mathfrak{P}}\right)$ とかく. 対応としては, $\alpha \in \mathfrak{O}_K$ に対し,

$$\Big(\frac{K/F}{\mathfrak{P}}\Big)(\alpha) \equiv \alpha^{N^F(\mathfrak{p})} \pmod{\mathfrak{P}}$$

で与えられる.

特に, K/F がアーベル拡大のとき, フロベニウス自己同型写像は $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{O}_F$ のみに依存し,

$$\Big(\frac{K/F}{\mathfrak{p}}\Big)(\alpha) \equiv \alpha^{N^F(\mathfrak{p})} \pmod{\mathfrak{p}\mathfrak{O}_K}$$

となる. $\left(\frac{K/F}{\mathfrak{p}}\right)$ を**アルティン記号**という.

このフロベニウス自己同型写像を用いて, 完全分解する素イデアルの特徴づけができる.

定理 1.88 代数体のガロア拡大 K/F に対し, $\mathfrak{P}$ を K の整数環 $\mathfrak{O}_K$ の素イデアルとすると, 以下は同値である :
(1) $\mathfrak{P}$ は完全分解する ;
(2) $\left(\frac{K/F}{\mathfrak{P}}\right) = 1$.

このアルティン記号はアーベル拡大 K/F で不分岐な F の整数環 $\mathfrak{O}_F$ の素イデアルを素因子にもつ分数イデアルに対して拡張することができる. この条件を満たす分数イデアル $\mathfrak{a}$ をとり,

$$\mathfrak{a} = \prod_{j=1}^{n} {\mathfrak{p}_j}^{c_j}$$

と素イデアル分解されたと仮定する. $c_j \in \mathbb{Z}$, $\mathfrak{p}_j$ は K/F で不分岐な $\mathfrak{O}_F$ の素イデアルである. このとき,

$$\Big(\frac{K/F}{\mathfrak{a}}\Big) := \prod_{j=1}^{n} \Big(\frac{K/F}{\mathfrak{p}_j}\Big)^{c_j}$$

とすれば, 一般の K/F で不分岐な $\mathfrak{O}_F$ の分数イデアルに拡張できる. この写像を**アルティン写像**という.

K/F がアーベル拡大であるから,

$$\Big(\frac{K/F}{\mathfrak{a}\mathfrak{b}}\Big) = \Big(\frac{K/F}{\mathfrak{a}}\Big)\Big(\frac{K/F}{\mathfrak{b}}\Big)$$

となる. これは, 不分岐な分数イデアル全体の集合からガロア群 $\mathrm{Gal}(K/F)$ への準同型写像であることを意味している.

最後に, 惰性群をさらに細かく分けた高次分岐群について述べる.

定義 1.89 K/F を代数体のガロア拡大, $\mathfrak{P}$ を K の整数環 $\mathfrak{O}_K$ の素イデアルとする.
$j \in \mathbb{Z}_{\geq 0}$ に対し,

$$v_j := \left\{\sigma \in I_{\mathfrak{P}}(K/F) \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}^{j+1}} \ (\forall \alpha \in \mathfrak{O}_K)\right\}$$

を $\mathfrak{P}$ の第 j 次分岐群という. これの不変体 K^{v_j} を $\mathfrak{P}$ の第 j 次分岐体といい, $V_{\mathfrak{P}}^{(j)}(K/F)$ とかく.

注意 1.90 $v_0 = I_{\mathfrak{P}}(K/F)$, $V_{\mathfrak{P}}^{(0)}(K/F) = T_{\mathfrak{P}}(K/F)$ である.

高次分岐群の性質は次のとおりである :

命題 1.91 K/F を代数体のガロア拡大とする. K の整数環 $\mathfrak{O}_K$ の素イデアル $\mathfrak{P}$ をとり, $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{O}_F$, $(p) = \mathfrak{P} \cap \mathbb{Z}$ とする.
(1) $i < j$ に対し, $v_j \lhd v_i$.
(2) $v_n = \{1\}$ となる $n \in \mathbb{Z}_{\geq 0}$ が存在する.
(3) v_0/v_1 は $(\mathfrak{O}_K/\mathfrak{P})^\times$ の部分群とみれる.
特に, v_0/v_1 は位数が p で割れない巡回群と同型になる.
(4) $j \geq 2$ に対し, v_{j-1}/v_j は $\mathfrak{O}_K/\mathfrak{P}$ を加法群とみた, その部分群とみれる.
特に, v_{j-1}/v_j は基本アーベル p 群である.
(5) v_1 は p 群である.
(6) $\mathfrak{P}$ の分解群 $D_{\mathfrak{P}}(K/F)$ がアーベル群のとき, $q = N^F(\mathfrak{p})$ とおくと, $|v_0/v_1| \,\big|\, (q-1)$ となる.

第 1 章の最後に, 惰性群の元が何次の分岐群に含まれているのかを特徴づける.

命題 1.92 K/F を代数体のガロア拡大とし, K の整数環 $\mathfrak{O}_K$ の素イデアル $\mathfrak{P}$ をとる. $\gamma \in \mathfrak{P}/\mathfrak{P}^2$ をとり固定する. $\sigma \in I_{\mathfrak{P}}(K/F)$ に対し, 以下は同値である :
(1) $\sigma \in v_m$;
(2) $\sigma(\gamma) \equiv \gamma \pmod{\mathfrak{P}^{m+1}}$.

第2章　ガウスの2次形式論

この章では2次体の整数論の中では大変関係のある整係数2元2次形式 $ax^2+bxy+cy^2$ $(a,b,c\in\mathbb{Z})$ についてまとめておく. この理論ははガウスが提唱したものである. これを導入することにより, のちに述べる $\mathbb{Q}$ 上の2次体のイデアル類群の代表元や構造がとても分かりやすくなる.

第1節では2元2次形式の基本的なことと, 同値関係を導入した後に成り立つことを述べている. 第2節では第1節で定義した同値関係による代表元として簡約形式という2元2次形式をとることを示す. さらに, その取り方が有限個であることも示し, 簡約形式をまとめた表も載せている. 第3節では2元2次形式に演算を定義し, 2元2次形式の集合を同値関係で割ったが群になることを示している. 第4節では, 第3節で定義した群と2次体のイデアル類群との関係を述べている.

参考文献において, [3], [6], [9] から [12] と [15] を参考にした.

2.1　2元2次形式の基本事項と同値関係の導入

この節では, 2元2次形式の基本的な事柄について述べ, それから同値関係を導入する.

定義 2.1 $f(x,y)=ax^2+bxy+cy^2$ とおく.
(1) f は**原始形式** $\overset{\text{def}}{\iff}\gcd(a,b,c)=1$.
(2) f が $n\in\mathbb{Z}$ を**表現する** $\overset{\text{def}}{\iff} f(x,y)=n$ となる $(x,y)\in\mathbb{Z}^2$ が存在する.
(3) f が $n\in\mathbb{Z}$ を**原始的に表現する** $\overset{\text{def}}{\iff} f(x,y)=n$ かつ $\gcd(x,y)=1$ となる $(x,y)\in\mathbb{Z}^2$ が存在する.
(4) b^2-4ac を f の**判別式**という.
(5) f の判別式 $b^2-4ac>0$ のとき f を**不定形式**という. f の判別式 $b^2-4ac<0$ かつ $a>0$ のとき f を**正定値形式**, f の判別式 $b^2-4ac<0$ かつ $a<0$ のとき f を**負定値形式**という. [4]

注意 2.2 以下の2つのことに注意する：
(1) f が負定値形式のとき, 各項を -1 倍すれば $-f$ という正定値形式を得るので, 負定値形式については考えない.
(2) f の判別式 D は, $D\equiv 0,1 \pmod 4$ を満たす. 以降, 判別式が平方数でない2元2次形式を考えていく.

今後, $f(x,y)=ax^2+bxy+cy^2$ を単に f とかいたり, 係数を並べた (a,b,c) というようにかく. また, 2元2次形式を簡単に2次形式ということにする.

次に, 2次形式に対して同値関係を導入する.

定義 2.3 2つの2次形式 f と g に対し,

[4] 判別式が0の2次形式については考えない.

$f \sim g \overset{\text{def}}{\iff} f(x,y) = g(px+qy, rx+sy)$ かつ $ps-qr=1$ となる $p,q,r,s \in \mathbb{Z}$ が存在する.

注意 2.4 一般に 2 次形式 $ax^2+bxy+cy^2$ は行列を用いて,

$$ax^2+bxy+cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

となるので, 定義 2.3 の同値関係は $f=(a,b,c)$, $g=(A,B,C)$ と具体的にかくと,

$$\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} = {}^t\begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} A & \frac{B}{2} \\ \frac{B}{2} & C \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

となる

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

が存在することと同値である. このようにして行列の形にかくことができる.

これらを踏まえると, 次の 3 つの基本的な性質が成り立つ :

命題 2.5 $f \sim g$ ならば f の判別式と g の判別式は一致する.

証明. $f=(a,b,c)$ の判別式 D は行列を使って,

$$D = b^2-4ac = -4 \begin{vmatrix} a & \frac{b}{2} \\ \frac{b}{2} & b \end{vmatrix}$$

とかけるので, 注意 2.4 により, $f \sim g$ ならば f と g の判別式は一致する. □

命題 2.6 2 次形式 f に対し, 以下は同値である :
(1) f が $n \in \mathbb{Z}$ を原始的に表現する ;
(2) $f \sim g$ かつ $g=(n,B,C)$ $(B,C \in \mathbb{Z})$ となる g が存在する.

証明. $(\Longrightarrow)$ $f=(a,b,c)$ とする. n が f により原始的に表現されるから,

$$f(x,y)=n \text{ かつ } \gcd(x,y)=1$$

となる $(x,y) \in \mathbb{Z}^2$ が存在する. $\gcd(x,y)=1$ であるから,

$$px+qy=1$$

となる $p,q \in \mathbb{Z}$ が存在する. よって,

$$\begin{aligned} B &= -2y(ap+cq)+b(px-qy), \\ C &= cx^2-bxy+ay^2 \end{aligned}$$

とすると,

$$\begin{pmatrix} n & \frac{B}{2} \\ \frac{B}{2} & C \end{pmatrix} = {}^t\begin{pmatrix} p & -y \\ q & x \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} p & -y \\ q & x \end{pmatrix}$$

となるので, 注意 2.4 より, $f \sim (n,B,C)$ である.
$(\Longleftarrow)$ $g=(n,B,C)$ とすると $f \sim g$ より,

$$g(x,y) = f(px+qy, rx+sy) \text{ かつ } ps-qr=1$$

となる $p,q,r,s \in \mathbb{Z}$ が存在する. よって, $f(p,r) = g(1,0) = n$ かつ $\gcd(p,r)=1$ より n は f により原始的に表現される. □

命題 2.7 原始形式と同値な 2 次形式は原始形式である.

証明. $f=(a,b,c)$ とする. $g=(A,B,C)$ が $f \sim g$ を満たすと仮定すると,

$$f(x,y) = g(px+qy, rx+sy) \text{ かつ } ps-qr=1$$

となる $p,q,r,s \in \mathbb{Z}$ が存在する. ここで, $p' \mid \gcd(A,B,C)$ となる素数 p' が存在すると仮定すると, 各係数を比較して

$$\begin{aligned} a &= Ap^2+Bpr+Cr^2, \\ b &= 2Apq+B(ps+qr)+2Crs, \\ c &= Aq^2+Bqs+Cs^2 \end{aligned}$$

であるから, $p' \mid \gcd(a,b,c)$ である. つまり, この命題の対偶が示されたことになるので, 元の命題も示されたことになる. □

注意 2.8 原始形式でないものは, 同値関係の定義により, 同値な 2 次形式も係数に同じ素因子をもつ.

$D \equiv 0,1 \pmod 4$ かつ平方数でない $D \in \mathbb{Z}$ が与えられたとき, D を判別式としてもつ原始形式の集合を C_D とかく. 命題 2.7 により, この集合を考えれば, 全ての 2 次形式の様子がわかってくる.

明らかに, C_D は無限集合で全く特徴がつかめない. そこで, 次節から C_D を同値関係で割った集合 $C_D/\sim$ について考えていく. 次の節から 2 次形式はすべて原始形式であると仮定する.

2.2 簡約形式

この節では, C_D を定義 2.3 で定義した同値関係で割った集合 $C_D/\sim$ の代表元となる元の特徴を見ていく. 同値類で割ったことにより, C_D が分類されたが, その代表元である元が非常に重要になってくる. その代表元が簡約形式と呼ばれる 2 次形式である. この節では, 判別式の符号によって場合分けして考えていく.

2.2.1 正定値形式の簡約形式

まずは, 判別式が負の場合について述べていく. この場合については非常に簡単で, 代表元を求めやすい場合になっている.

定義 2.9 $f=(a,b,c)$ を正定値形式とする.
f が**簡約形式** $\overset{\text{def}}{\iff} |b| \le a \le c$ かつ「$|b|=a$ または $a=c$ ならば $b \ge 0$」.

実際, この定義が何を意味しているか見た目では分からないが, 次の命題により特徴づけることができる. 証明は省略するが, 2 次方程式の解の公式を評価していく.

命題 2.10 2 次形式 $f=(a,b,c)$ に対し, 以下は同値である :
(1) f は簡約形式である ;
(2) $f(x,1)=ax^2+bx+c=0$ の虚部が正の根 $\frac{-b+\sqrt{b^2-4ac}}{2a}$ が基本領域にある.

基本領域というものは, 上半平面 $H:=\{z\in\mathbb{C}\mid \mathrm{Im}(z)\geq 0\}$ に対し,

$$F:=\{z\in H\ \big|\ |z|\geq 1, -\tfrac{1}{2}\leq \mathrm{Re}(z)<\tfrac{1}{2}\}$$

のことである. 話は変わるが, この基本領域は保型形式の分野においても定義されている.

なぜ簡約形式を定義したのか疑問をもつと思われるが, 実は次の性質がある :

定理 2.11 全ての正定値形式 f に対して, $f\sim g$ となる簡約形式 g が一意に存在する.

証明. $f=(a,b,c)$ を任意の正定値形式とし, $n\in\mathbb{N}$ を f で原始的に表現される最小の自然数とする. 命題 2.6 より, $f\sim g$ かつ $g=(n,B,C)$ $(B,C\in\mathbb{Z})$ となる g が存在する. 任意の $z\in\mathbb{Z}$ に対し, 変数変換 $(x,y)\mapsto(x-zy,y)$ を行うと f と同値な新たな 2 次形式

$$g=(n,B-2nz,nz^2-Bz+C)$$

を得る. 特に, $z\in\mathbb{Z}$ を $|B-2nz|\leq n$ を満たすようにとると, これは簡約形式になる. (このアルゴリズムを簡約化という)

次に, 一意性について示す. そのために, 2 つの簡約形式 f,g をとり, $f\sim g$ と仮定する. 具体的に $f=(a,b,c), g=(A,B,C)$ とおくと,

$$|b|\leq a\leq c \text{ かつ } |B|\leq A\leq C$$

を満たしている. 一般性を失うことなく $a\geq A>0$ と仮定してよい. $f\sim g$ であるから,

$$g(x,y)=f(px+qy,rx+sy) \text{ かつ } ps-qr=1$$

となる $p,q,r,s\in\mathbb{Z}$ が存在する. それぞれを代入し, 項を比較すると

$$\begin{aligned} A &= ap^2+bpr+cr^2,\\ B &= 2apq+b(ps+qr)+2crs,\\ C &= aq^2+bqs+cs^2 \end{aligned}$$

を得る. まず $A=a$ を示す.

$$A=ap^2+bpr+cr^2\geq ap^2-|bpr|+cr^2\geq a(p^2+r^2)-|bpr|\geq 2a|pr|-a|pr|=a|pr|$$

であるから, $a\geq A$ より $a\geq a|pr|$ となるので $|pr|\leq 1$ となる.
$|pr|=1$ ならば, $A\geq a$ より, $A=a$ となる.
$|pr|=0$ ならば, $p=r=0$ のとき, $1=ps-qr=0$ となり矛盾するから, $p=0$ または $r=0$ である.
$p=0$ のとき, $A=ap^2+bpr+cr^2=cr^2\geq ar^2\geq a$ より, $A=a$ である. $r=0$ のときも同様に示せる.

次に, $B=b, C=c$ を示す. $A=a$ より,

$$a=ap^2+bpr+cr^2=a\left(p+\frac{b}{2a}\right)^2+\frac{4ac-b^2}{4a}r^2\geq\frac{4ac-b^2}{4a}r^2.$$

よって, $4ac-b^2 \geq 4a^2-a^2=3a^2>0$ より,

$$r^2 \leq \frac{4a^2}{4ac-b^2} \leq \frac{4}{3}$$

となるから, $r=\pm 1, 0$ を得る. これらを場合分けしていく.

(i) $r=0$ のとき, $ap^2=a$ であるから $p=\pm 1$ であり, $ps-qr=1$ より, $(p,s)=(1,1),(-1,-1)$ となる. これから, $B=\pm 2aq+b$ となり, $|B|=|\pm 2aq+b| \leq A=a$ より, $2a|q| \leq a+|b| \leq 2a$ となるから, $|q| \leq 1$ となる.
$q=\pm 1$ ならば, $2a-|b| \leq a$ より $|b| \geq a$ であるから $|b|=a$ となるので, 簡約形式の定義より $b=a$ となる. よって, $B=\pm 2a+a=3a, -a$ となり, 矛盾する.
実際, $B=3a$ ならば $|B|=3a=3A>A, B=-a$ ならば $|B|=A$ となるので, 簡約形式の定義より $B>0$ となるため矛盾する.
したがって, $q=0$ より $B=b$ であるから命題 2.5 より $C=c$ となるので, $f=g$.

(ii) $r=\pm 1$ のとき, $|pr| \leq 1$ の値の場合分けで調べていく.

(a) $|pr|=1$ のとき, $p=\pm 1$ より, $A=a \pm b+c=a$ であるから $c=\pm b$ となる. よって, $|b| \leq a \leq c \leq |b|$ より, $|b|=a$ であるから, 簡約形式の定義より $(a,b,c)=(1,1,1)$ となる. これ以外の判別式 -3 の簡約形式はないから一致していなければならないので, $f=g$ を得る.

(b) $|pr|=0$ のとき, $p=0$ ならば $c=a$ である. また, $ps-qr=1$ より $(q,r)=(1,-1),(-1,1)$ となるから, $B=\pm 2cs-b$ であり, (i) と同じような議論をすれば $s=0$ となる.
したがって, $B=-b$ から $C=c=a=A$ より $B, b \geq 0$. したがって, $B=b=0$ より $f=g$ となる.

□

実は, この変数変換は意味がないように思われるが, 2 次方程式の解を一次分数変換させている. それが次の命題である :

命題 2.12 f, g を判別式 $D<0$ をもつ 2 次形式とし, α_1, α_2 をそれぞれ $f(x,1), g(x,1)$ の根で, 虚部が正の根とする. このとき, 以下は同値である :
(1) $f \sim g$;
(2) $\alpha_1=\frac{p\alpha_2+q}{r\alpha_2+s}$ かつ $ps-qr=1$ となる $p,q,r,s \in \mathbb{Z}$ が存在する.

証明. ($\Longrightarrow$) 定義において $y=1$ を代入すると,

$$f(x,1)=g(px+q, rx+s) \text{ かつ } ps-qr=1$$

となる $p,q,r,s \in \mathbb{Z}$ が存在する. $f(x,1), g(x,1)$ の根で, 虚部が正の根をそれぞれ α_1, α_2 とする.
一般に, $\alpha \in \mathbb{C}, p,q,r,s \in \mathbb{Z}$ に対し,

$$\mathrm{Im}\left(\frac{p\alpha+q}{r\alpha+s}\right)=\frac{(ps-qr)}{|r\alpha+s|^2}|\alpha|^2$$

が成り立つから根を比較すると,

$$\alpha_1 = \frac{p\alpha_2 + q}{r\alpha_2 + s}$$

となる.
($\Longleftarrow$) $f = (a, b, c), g = (A, B, C)$ と具体的にかくと α_1, α_2 は,

$$\alpha_1 = \frac{-b + \sqrt{D}}{2a}, \alpha_2 = \frac{-B + \sqrt{D}}{2A}$$

とかける. ここで,

$$\begin{aligned} A' &= ap^2 + bpr + cr^2, \\ B' &= 2apq + b(ps + qr) + 2crs, \\ C' &= aq^2 + bqs + cs^2 \end{aligned}$$

とおくと, $\alpha_2 = \frac{-B' + \sqrt{D}}{2A'}$ となる. これを変形すると $(A'B - AB') + (A - A')\sqrt{D} = 0$ であるから, $A = A', B = B', C = C'$ を得る. したがって, $f \sim (A', B', C') = g$ となる. □

つまり, 同値は一次分数変換により根を写していることを表していることがわかり, 簡約化するということは, 一次分数変換により根を基本領域に移動させているということである.

定理 2.11 により, $D < 0$ のとき $C_D/\sim$ の代表元を簡約形式でとることができる. 次の命題はその簡約形式の個数についてである :

命題 2.13 判別式 D をもつ正定値形式の簡約形式は有限個である.

証明. $f = (a, b, c)$ を判別式 D の簡約形式とすると, $b^2 - 4ac = D, |b| \leq a \leq c$ であるから, $-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2$ より $0 < a \leq \sqrt{-\frac{D}{3}}$.

よって, a のとりうる値は有限個となるので自動的に b, c も有限個になる. □

具体的に簡約形式を求める場合は, 定理 2.13 の証明にある計算をするだけで求めることができる. 実際に求めた結果は, 34 ページの表でまとめている.

2.2.2 不定形式の簡約形式

次に判別式が正かつ平方数でない場合を述べていく. この場合は, 負の場合に比べ非常に難しい. 簡約形式を求めても, その中で同値な簡約形式があることが正の場合の特徴である.

定義 2.14 $f = (a, b, c)$ を判別式 D をもつ不定形式とする.
$f = (a, b, c)$ が**簡約形式** $\overset{\text{def}}{\Longleftrightarrow} 0 < \sqrt{D} - b < 2|a| < \sqrt{D} + b.$

正定値形式の簡約形式と同様に, 次のように特徴づけすることができる :

命題 2.15 判別式 D をもつ不定形式 $f = (a, b, c)$ に対し, 以下は同値である :
(1) f は簡約形式 ;
(2) $f(x, 1) = 0$ の根をそれぞれ $\alpha_1 = \frac{-b+\sqrt{D}}{2a}, \alpha_2 = \frac{-b-\sqrt{D}}{2a}$ とすると, $0 < |-\alpha_1| < 1 < |-\alpha_2|$ である.

注意 2.16 不定形式に対して, 正定値形式と同じように根をどのように動かしているのかを疑問にもつと思われる. そのことについては, 後で述べる定理 2.55 の証明で述べる.

不定形式に対しても, 簡約形式に関する定理がある. 証明するために, 補題を用意する.

補題 2.17 判別式 D をもつ任意の不定形式 f に対して, f と同値な 2 次形式 $g = (A, B, C)$ の中で, $|B| \leq |A| \leq \sqrt{\frac{D}{3}}$ を満たすものが存在する.

証明. まず, $|A| \leq \sqrt{\frac{D}{3}}$ を示す.
$|A| > \sqrt{\frac{D}{3}}$ ならば, $f = (a, b, c)$ に対し, 変数変換 $(x, y) \mapsto (hx + y, -x)$ $(h \in \mathbb{Z})$ を行い, それで得た 2 次形式を (a_1, b_1, c_1) とする. (それぞれ計算すると $a_1 = ah^2 - bh + c, b_1 = 2ah - b, c_1 = a$ である)
特に, h を $|b_1| \leq |a|$ となる整数をとると

$$4a_1a = b_1^2 - D < b_1^2 \leq a^2$$

かつ

$$-4a_1a = D - b_1^2 \leq D < 3a^2$$

となる. よって, $|4a_1a| < 3a^2$ より $|a_1| < \frac{3}{4}|a|$ となる.
さらに, $|a_1| > \sqrt{\frac{D}{3}}$ ならば, 上記のアルゴリズムをもう一度行えば, f と同値な形式 (a_2, b_2, a_1) を得られ,

$$|a_2| < \frac{3}{4}|a_1| < \left(\frac{3}{4}\right)^2 |a|$$

を満たしている. これを繰り返していくと,

$$0 \leq \cdots < |a_{n+1}| < |a_n| < \cdots < |a_1| < |a|$$

となるが, $\sqrt{\frac{D}{3}}$ は定数より,

$$|a_i| \leq \sqrt{\frac{D}{3}}$$

となる i が存在する. 次に, $|B| \leq |A|$ となることを示す.
上のアルゴリズムで得た $f' = (a', b', c')$ に対し, 変数変換 $(x, y) \mapsto (x + ky, y)$ $(k \in \mathbb{Z})$ を行い, それで得た 2 次形式を (a', B', C') とする. このとき, x^2 の変数が動かないことに注意する. 特に k を $|B'| \leq |a'|$ となるようにとればよい. □

補題 2.17 により, 次の定理を証明する準備ができた.

定理 2.18 任意の不定形式 f に対して, $f \sim g$ となる簡約形式 g が存在する.

証明. f は判別式 D をもつと仮定する.
補題 2.17 より, $f = (a, b, c)$ は $b^2 \leq \sqrt{\frac{D}{3}}$ を満たしていると仮定してよい. このとき, $b^2 \neq D$ であるから $a \neq 0$ または $c \neq 0$ である.
このとき, $4|ac| = D - b^2 \leq D$ であるから, $2|a|, 2|c| < \sqrt{D}$ だから, 変数変換 $(x, y) \mapsto (y, -x)$ により, $a \neq 0$ と仮定してよい.
さらに, 変数変換 $(x, y) \mapsto (x - ky, y)$ $(k \in \mathbb{Z})$ により, 2 次形式 (a, b', c') を得たとする. k を $0 <$

$\sqrt{D}-2|a|<b'<\sqrt{D}$ となるようにとると, $0<\sqrt{D}-b'<2|a|<\sqrt{D}+b'$ となるから, (a,b',c') は簡約形式である. □

また, 不定形式の簡約形式に対しても, 簡約形式の個数の有限性がいえる.

命題 2.19 判別式 D をもつ不定形式の簡約形式は有限個である.

証明. $f=(a,b,c)$ を判別式 D の簡約形式とすると, $0<b<\sqrt{D}$ より b のとりうる値は有限個である.
よって, 定義から a のとりうる値も有限個であるから, 自動的に c も有限個である. □

このように, 不定形式のときは, 正定値形式のときよりも計算量が多くなることもあり, 求めることが非常に困難になっている.
さらに簡約形式と簡約形式が同値になる場合もあるため, 代表元を簡単に求めることができない. ここで簡約形式と同値な簡約形式の例を挙げておく.

例 2.20 $f=(2,3,-1), g=(-2,1,2)$ は判別式 17 をもつ簡約形式で

$$\begin{pmatrix} 2 & \frac{3}{2} \\ \frac{3}{2} & -1 \end{pmatrix} = {}^t\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}\begin{pmatrix} -2 & \frac{1}{2} \\ \frac{1}{2} & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

であるから, $f\sim g$ である.

実は, 簡約形式が同値であるかどうかを調べるために, 非常に有用な手法がある. $\mathbb{Q}$ 上の最小多項式が 2 次であるような無理数, いわゆる 2 次無理数の理論を使って調べていく. ここで, 定義しておくものがある.

定義 2.21 正の判別式をもつ 2 次形式 $f(x,y)$ において, $f(x,1)=0$ の解 α を f **に対応する 2 次無理数**といい, f を α **に対応する 2 次形式**という.

2.2.3 2 次無理数

この節では, 2 次形式の議論とは離れて, 初等整数論的な議論になる. まず, 簡約 2 次無理数について定義する. 2 次無理数 α に対し, $\overline{\alpha}$ は α の共役, つまり α を根にもつ 2 次多項式の α とは異なる根のことを表すことにする.

定義 2.22 2 次無理数 α は**簡約 2 次無理数** $\overset{\text{def}}{\iff}$ $\alpha>1$ かつ $-1<\overline{\alpha}<0$.

注意 2.23 判別式は正ではあるが平方数ではないと仮定しているので, 重根をもつ 2 次形式については考えていない.
さらに α が簡約 2 次無理数のとき, α の連分数展開の時に出てくる無理数, いわゆる中間連分数も簡約 2 次無理数になる.

簡約 2 次無理数の特徴づけを 2 次形式の係数を使って示す. 次の命題の証明は放物線のグラフを書けば明らかであるから, 証明は省略する.

命題 2.24 $f(x,y)=ax^2+bxy+cy^2$ を判別式 D をもつ 2 次形式とする. 以下は同値である :
(1) f が簡約 2 次無理数と対応する ;
(2) $a>0$, $b<0$, $c<0$, $a+b+c<0$, $a-b+c>0$;
(3) $f(1,0)>0$, $f(0,1)<0$, $f(1,1)<0$, $f(-1,1)>0$.

ここで連分数展開について, 新たな定義をする. これは 2 次無理数, 簡約 2 次無理数と非常に関係している連分数展開の種類である.

定義 2.25 $\alpha\in\mathbb{R}\backslash\mathbb{Q}$ の連分数展開を

$$\alpha=[a_0,\cdots,a_n,\cdots]$$

とする. このとき,

$$a_{n+km}=a_n\quad(k\in\mathbb{N})$$

となる $m\in\mathbb{N}$ が存在するとき, この連分数を**周期 m の循環連分数**という. 簡単に,

$$\alpha=[a_0,\cdots,a_l,\overline{b_1,\cdots b_m}]$$

と表す. また, この条件を満たす m の中で最小のものを**最小周期**という.
さらに,

$$\alpha=[\overline{b_1,\cdots b_m}]$$

と表せるとき, この連分数を**純循環連分数**という.

2 次無理数とこれらの連分数には次のような関係がある :

定理 2.26 $\alpha\in\mathbb{R}\backslash\mathbb{Q}$ とする.
(1) α は 2 次無理数 $\Longleftrightarrow$ α の連分数展開が循環連分数になる.
(2) α は簡約 2 次無理数 $\Longleftrightarrow$ α の連分数展開が純循環連分数になる.

証明. (1) ($\Longleftarrow$) α の連分数展開が循環連分数であることから,

$$\alpha=[a_0,\cdots,a_l,\overline{b_1,\cdots,b_m}]$$

となる $l,m\in\mathbb{N}$ が存在する. $\beta=[\overline{b_1,\cdots,b_m}]$ とおくと, 命題 1.7 より $\alpha\sim\beta$ である. また, $\beta=[b_1,\cdots,b_m,\beta]$ であるから,

$$\beta=\frac{p\beta+q}{r\beta+s}\ \text{かつ}\ ps-qr=\pm1$$

となる $p,q,r,s\in\mathbb{Z}$ が存在する. このとき,

$$r\beta^2+(s-p)\beta-q=0$$

となり, これは α が無理数であることから既約 2 次式である.
したがって, β は 2 次無理数であるから, α も 2 次無理数である.
($\Longrightarrow$) α を 2 次無理数とすると,

$$a\alpha^2+b\alpha+c=0$$

となる $a, b, c \in \mathbb{Z}$ が存在する. ただし $a \neq 0$ である. また, α の中間連分数 α_n を

$$\alpha = [a_0, \cdots, a_{n-1}, \alpha_n] = \frac{p_n \alpha_{n-1} + p_{n-1}}{q_n \alpha_{n-1} + q_{n-1}}$$

と表すと,

$$A_n {\alpha_n}^2 + B_n \alpha + C_n = 0.$$

ただし,

$$\begin{aligned} A_n &= a{p_n}^2 + b p_n q_n + c{q_n}^2, \\ B_n &= 2a p_n p_{n-1} + b(p_n q_{n-1} + p_{n-1} q_n) + 2c q_n q_{n-1}, \\ C_n &= a{p_{n-1}}^2 + b p_{n-1} q_{n-1} + c{q_{n-1}}^2. \end{aligned}$$

また, $|\alpha - \frac{p_n}{q_n}| < \frac{1}{{q_n}^2}$ であるから, $|\epsilon_n| < 1$ に対し, $p_n = \alpha q_n + \frac{\epsilon_n}{q_n}$ と表すことができるので, A_n, B_n, C_n の評価をすると,

$$\begin{aligned} |A_n| &< 2|a\alpha| + |b| + |a|, \\ {B_n}^2 &\leq 4(2|a\alpha| + |a| + |b|) + |b^2 - 4ac|, \\ |C_n| &< 2|a\alpha| + |b| + |a| \end{aligned}$$

となり, この 3 つの整数は有界になる. よって,

$$(A_l, B_l, C_l) = (A_m, B_m, C_m) = (A_n, B_n, C_n)$$

となる $l, m, n \in \mathbb{Z}_{\geq 0}$ が存在する. したがって, 3 つの中間連分数 $\alpha_l, \alpha_m, \alpha_n$ は同じ 2 次方程式の解であるから, このうち 2 つは一致しなければならない. それを α_l, α_m $(l > m)$ とすると α の連分数展開は,

$$\alpha = [a_0, \cdots, a_{l-1}, \alpha_l] = [a_0, \cdots, a_{l-1}, \cdots, a_{m-1}, \alpha_l]$$

となり, 循環連分数になっている.

(2) $(\Longrightarrow)$ α が循環連分数で表されているから, (1) より α は 2 次無理数であるので, 簡約性を示せばよい. さらに α が純循環連分数で表されているから,

$$\alpha = [a_0, \cdots, a_{n-1}, \alpha] = \frac{p_n \alpha + p_{n-1}}{q_n \alpha + q_{n-1}}$$

となる $n \in \mathbb{N}$ が存在する. 変形すると, $q_n \alpha^2 + (q_{n-1} - p_n)\alpha - p_{n-1} = 0$ となる.
$f(x) = q_n x^2 + (q_{n-1} - p_n)x - p_{n-1}$ とおく. すると, $f(1) < 0, f(0) < 0, f(-1) > 0$ がいえる. α は f の根であるから, 命題 2.24 より α は簡約 2 次無理数である.
$(\Longleftarrow)$ α の連分数展開を

$$\alpha = [a_0, \cdots, a_{n-1}, \alpha_n]$$

とする. α は 2 次無理数であるから (1) より, 循環連分数により表すことができるので,

$$\alpha_m = \alpha_n \text{ かつ } m > n$$

となる $m, n \in \mathbb{Z}_{\geq 0}$ が存在する. ここで, $n = 0$ であれば, α は純循環連分数で表すことができるので, $n \geq 1$ と仮定する.

$$\alpha_{m-1} = a_{m-1} + \frac{1}{\alpha_m}, \alpha_{n-1} = a_{n-1} + \frac{1}{\alpha_n}$$

が成り立つから, $\alpha_{m-1} - \alpha_{n-1} = a_{m-1} - a_{n-1} \in \mathbb{Z}$ である. 次に, この 2 つの元を具体的に,

$$\alpha_{m-1} = \frac{-b_{m-1} + \sqrt{D}}{2a_{m-1}}, \alpha_{n-1} = \frac{-b_{n-1} + \sqrt{D}}{2a_{n-1}}$$

とかく. すると, $\sqrt{D}$ の係数が 0 であることがわかる. このとき, これらの共役である $\overline{\alpha_{m-1}}, \overline{\alpha_{n-1}}$ を考え, 上と同じようにして引けば, $\overline{\alpha_{m-1}} - \overline{\alpha_{n-1}} \in \mathbb{Z}$ であることがわかる.

ここで, α が簡約 2 次無理数より, 注意 2.23 から, $\alpha_{m-1}, \alpha_{n-1}$ も簡約 2 次無理数であるから, $-1 < \overline{\alpha_{m-1}}, \overline{\alpha_{n-1}} < 0$ である. よって, $|\overline{\alpha_{m-1}} - \overline{\alpha_{n-1}}| < 1$ であるが, $\overline{\alpha_{m-1}} - \overline{\alpha_{n-1}} \in \mathbb{Z}$ より, $\overline{\alpha_{m-1}} = \overline{\alpha_{n-1}}$ を得る. したがって, $\alpha_{m-1} = \alpha_{n-1}$ となる.

以上により, $\alpha_m = \alpha_n$ ならば $\alpha_{m-1} = \alpha_{n-1}$ がいえたので, 上の議論を繰り返していけば, $\alpha_{m-n} = \alpha_0$ を得るので, α は純循環連分数により表される. □

この定理により無理数が与えられたとき, 連分数展開すれば 2 次無理数であるか, 簡約 2 次無理数であるかを判定することができる. 例えば, 例 1.4 で挙げた $\sqrt{2}$ は連分数展開すれば $\sqrt{2} = [1, \overline{2}]$ となるので, 循環連分数であるが純循環連分数はないので, 2 次無理数であるが簡約 2 次無理数でないことがわかる.

実は簡約 2 次無理数は 2 次無理数と関係しており, 次が成り立つ :

定理 2.27 α を 2 次無理数とすると, $\alpha \overset{+}{\sim} \beta$ となる簡約 2 次無理数 β が存在する.

証明. α の中間連分数を α_n とし, 連分数展開を

$$\alpha = [a_0, \cdots, a_{n-1}, \alpha_n]$$

とする. 定理 2.26 (1) より,

$$\alpha_m = \alpha_n \text{ かつ } m > n$$

となる $m, n \in \mathbb{Z}$ が存在する. このとき,

$$\alpha = [a_0, \cdots, a_{n-1}, \alpha_n] = [a_0, \cdots, a_{m-1}, \alpha_m] = [a_0, \cdots, a_{m-1}, \alpha_n]$$

であるから,

$$\alpha_n = [a_n, \cdots, a_{m-1}, \alpha_n]$$

となるので, α_n は循環連分数で展開されるから, 定理 2.26 (2) より, α_n は簡約 2 次無理数である.

ここで, n が奇数のときは, $n+1$ に変えても α_{n+1} も簡約 2 次無理数であるから, n は偶数としてよい. 以上により, 定理 1.5 から,

$$\alpha = \frac{p_n \alpha_n + p_{n-1}}{q_n \alpha_n + q_{n-1}}$$

かつ

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^n = 1$$

となるので, 命題 1.7 より, $\alpha \overset{+}{\sim} \alpha_n$ である. □

次に, 簡約 2 次無理数 α を連分数展開したとき, 中間連分数はすべて簡約 2 次無理数であるが, α と同値な簡約 2 次無理数がどのぐらいあるのかが気になると思われる. それについてまとめたものが次の定理である :

定理 2.28 α を簡約 2 次無理数とする. その中間連分数を α_n とし, $\alpha = [a_0, \cdots, a_{n-1}, \alpha_n]$ と連分数展開されたとする. また, この連分数展開の最小周期を m とする. このとき, 以下が成り立つ :
(1) α と同値な簡約 2 次無理数は, $\alpha_0 = \alpha, \alpha_1, \cdots, \alpha_{m-1}$ しかない ;
(2) m が奇数ならば, $\alpha_0 = \alpha, \alpha_1, \cdots, \alpha_{m-1}$ は互いに正に同値である ;
(3) m が偶数ならば, $\alpha_0 = \alpha, \alpha_2, \cdots, \alpha_{m-2}$ は互いに正に同値であり, $\alpha_1, \alpha_3, \cdots, \alpha_{m-1}$ は負に同値である. さらに, 任意の奇数 n に対し $\alpha \overset{+}{\not\sim} \alpha_n$ である.

証明する前に, 次のことに注意する :

注意 2.29 α の最小周期が m であるから, $\alpha_0 = \alpha, \alpha_1, \cdots, \alpha_{m-1}$ は相異なる.

定理 2.28 の証明. (1) β を α と同値な簡約 2 次無理数とする. その中間連分数を β_l とすると,

$$\beta = [b_0, \cdots, b_{l-1}, \beta_l]$$

と連分数展開される. 定理 1.8 (1) より,

$$\alpha_r = \beta_s$$

となる $r, s \in \mathbb{Z}_{\geq 0}$ が存在する. β は簡約 2 次無理数であるから, β_s の中間連分数が β になるが, $\alpha_r = \beta_s$ より, $\beta = \alpha, \cdots, \alpha_{m-1}$ のいずれかに一致することになるので, 結局, α と同値な簡約 2 次無理数は, $\alpha_0 = \alpha, \alpha_1, \cdots, \alpha_{m-1}$ しかない.

(2), (3) を証明する前に命題 1.7 より, $\alpha \overset{+}{\sim} \alpha_{2n}$ であることに注意する.

(2) m が奇数のとき, $\alpha_n = \alpha_{m+n}$ であるから n が奇数であっても $m+n$ が偶数である. 結局, $\alpha \overset{+}{\sim} \alpha_{m+n} = \alpha_n$ である.
したがって, $\alpha_0 = \alpha, \alpha_1, \cdots, \alpha_{m-1}$ は互いに正に同値である.
(3) m が偶数のとき, 命題 1.7 より,

$$\alpha \overset{+}{\sim} \alpha_2 \overset{+}{\sim} \cdots \overset{+}{\sim} \alpha_{m-2},$$
$$\alpha_1 \overset{-}{\sim} \alpha_3 \overset{-}{\sim} \cdots \overset{-}{\sim} \alpha_{m-1}$$

である. ここで, $\alpha \overset{+}{\sim} \alpha_n$ となる奇数 n が存在すると仮定すると, 定理 1.8 より,

$$\alpha_r = \alpha_{n+s} \text{ かつ } r+s \text{ が偶数}$$

となる $r, s \in \mathbb{Z}_{\geq 0}$ が存在する. このとき $n+s-r$ は奇数になるから, これは最小周期 m が偶数であることに矛盾するので, 任意の奇数 n に対し $\alpha \overset{+}{\not\sim} \alpha_n$ である. □

ここで, 話を 2 次形式に戻す. なぜ, 2 次無理数の理論を取り上げたかというと, 次のことが知られているからである :

定理 2.30 D を平方数ではない正の整数とする. 判別式 D をもつ 2 次形式 f, g に対して, α_f, α_g をそれぞれ f, g に対応する 2 次無理数で $\sqrt{D}$ の係数は正である根とする. このとき, 以下は同値である :
(1) $f \sim g$;
(2) $\alpha_f \overset{+}{\sim} \alpha_g$.

証明については, 定理 2.55 を証明するときに同時に証明する.

この定理により, 不定値形式の簡約形式を完全に判別することができる. 結局は簡約 2 次無理数に対応する 2 次形式を命題 2.24 によって求め, 同値な可能性があるのでそれを解消するために連分数展開し定理 2.28 を使って判別すればよい.

また, 簡約形式の数が無限個あるかもしれないと思われるが, そのようなことはない. 次にそれを証明する.

命題 2.31 簡約 2 次無理数に対応する 2 次形式の同値類は有限個しかない.

証明. $f=(a,b,c)$ を簡約 2 次無理数に対応する判別式 D の 2 次形式とし, 根をそれぞれ,

$$\alpha=\frac{-b+\sqrt{D}}{2a}, \overline{\alpha}=\frac{-b-\sqrt{D}}{2a}$$

とおくと, α が簡約 2 次無理数より, $D=|b^2|+4a|c|\geq b^2$ だから b は有限個しかない.

よって, $-4ac=D-b^2$ であるから, a,c も有限個しかない. □

実際に, 平方数でない正の整数 D が与えられたとき, 判別式 D をもつ簡約形式をどのように計算すべきかをまとめる.

Step 1. 命題 2.31 の証明と同じようにして, 3 つの整数の組 (a,b,c) を全て求める.
Step 2. Step 1 で求めた (a,b,c) に対し, 対応する簡約 2 次無理数をすべて求め. 連分数展開する.
Step 3. 定理 2.28 を利用して. 正に同値なものがあるかを調べる.

具体例を挙げておく. $D=b^2-4ac$ により, D と b の偶奇は一致していることに注意すれば, 余計な計算をしなくて済む.

例 2.32 (1) 判別式 5 のときを考える. このときの簡約 2 次無理数を解にもつ 2 次形式を求める. 命題 2.31 の証明により, $b^2\leq 5$ と命題 2.24 より $b<0$ であるから, $b=-1$ が得られる. よって, $-4ac=4$ となるから, 命題 2.24 より $a>0,c<0$ であるから $(a,c)=(1,-1)$ を得る.

実際, $f=(1,-1,-1)$ に対応する 2 次無理数は $\frac{1+\sqrt{5}}{2}$ であり, 連分数展開すると $\frac{1+\sqrt{5}}{2}=[\overline{1}]$ であるから, 簡約 2 次無理数である.

したがって, 判別式 5 の簡約形式は f の 1 つだけである.

(2) 判別式 60 のときを考える. (1) と同じような方法で, $b^2\leq 60$ より, $b=-2,-4,-6$ が得られる. 判別式が偶数より, $b=-1,-3,-5,-7$ は考えなくてもよい.

よって, $-4ac=56,44,24$ となる, 命題 2.24 より $a>0,c<0$ であるから

$$(a,b,c)=(1,-2,-14),(14,2,-1),(2,-2,-7),(7,-2,-2),(1,-4,-11),$$
$$(11,-4,-1),(2,-6,-3),(3,-6,-2),(1,-6,-6),(6,-6,1)$$

となる. 命題 2.24 より $a+b+c<0, a-b+c>0$ であるから, これらの中では,

$$(a,b,c)=(2,-6,-3),(3,-6,-2),(1,-6,-6),(6,-6,1)$$

のみが満たすことがわかる. $f_1 = (1, -6, -6), f_2 = (3, -6, -2), f_3 = (3, -6, -2), f_4 = (6, -6, 1)$ とおく. これらに対する 2 次無理数は,

$$\alpha_{f_1} = 3 + \sqrt{15} \quad , \quad \alpha_{f_2} = \frac{3 + \sqrt{15}}{2},$$
$$\alpha_{f_3} = \frac{3 + \sqrt{15}}{3} \quad , \quad \alpha_{f_4} = \frac{3 + \sqrt{15}}{6}$$

である. それぞれを連分数展開すると,

$$\alpha_{f_1} = [\overline{6, 1}], \alpha_{f_2} = [\overline{3, 2}], \alpha_{f_3} = [\overline{2, 3}], \alpha_{f_4} = [\overline{1, 6}]$$

となるから, 定理 2.26 (2) より, これらは全て簡約 2 次無理数である. 最小周期はすべて偶数であるから, 定理 2.28 (3) より, 正に同値なものは存在しない.

したがって, 判別式 60 の簡約形式は f_1, f_2, f_3, f_4 の 4 つである.

本によっては, 簡約 2 次無理数を解にもつような 2 次形式を簡約形式と定義する本もある. 結局, 簡約 2 次無理数を解にもつ 2 次形式を求めることになるので, 後で簡約形式をまとめている表を載せているが, 簡約 2 次無理数に対応する 2 次形式を挙げていることに注意する.

結局, 集合 C_D を同値関係で割った集合 $C_D/\sim$ は, 有限集合になることが分かり, 代表元として簡約形式をとればよいことが分かり, いくらか $C_D/\sim$ の構造がいくらかわかった.

次の節では, $C_D/\sim$ が群にするために, 演算を導入していく. この演算はとても重要な演算で, 2 次体イデアル類群の構造を知るためには欠かせないものである.

この節の最後に, 判別式 D が与えれられたときのいくつかの簡約形式を具体的に求めたものを表にまとめた. まず, 判別式 D が負のときの簡約形式について $-60 \leq D \leq -3$ までまとめる. h_D は判別式 D に対する簡約形式の個数である.

D	判別式 D の簡約形式	h_D
-3	x^2+xy+y^2	1
-4	x^2+y^2	1
-7	$x^2+xy+2y^2$	1
-8	x^2+2y^2	1
-11	$x^2+xy+3y^2$	1
-12	x^2+3y^2	1
-15	$x^2+xy+4y^2, 2x^2+xy+2y^2$	2
-16	x^2+4y^2	1
-19	$x^2+xy+5y^2$	1
-20	$x^2+5y^2, 2x^2+2xy+3y^2$	2
-23	$x^2+xy+6y^2, 2x^2 \pm xy+3y^2$	3
-24	$x^2+6y^2, 2x^2+3y^2$	2
-27	$x^2+xy+7y^2$	1
-28	x^2+7y^2	1
-31	$x^2+xy+8y^2, 2x^2 \pm xy+4y^2$	3
-32	$x^2+8y^2, 3x^2+2xy+3y^3$	2
-35	$x^2+xy+9y^2, 3x^2+xy+3y^2$	2
-36	$x^2+9y^2, 2x^2+2xy+5y^2$	2
-39	$x^2+xy+10y^2, 2x^2 \pm xy+5y^2, 3x^2+3xy+4y^2$	4
-40	$x^2+10y^2, 2x^2+5y^2$	2
-43	$x^2+xy+11y^2$	1
-44	$x^2+11y^2, 3x^2 \pm 2xy+4y^2$	3
-47	$x^2+xy+12y^2, 2x^2 \pm xy+6y^2, 3x^2 \pm xy+4y^2$	5
-48	$x^2+12y^2, 3x^2+4y^2$	2
-51	$x^2+xy+13y^2, 3x^2+3xy+5y^2$	2
-52	$x^2+13y^2, 2x^2+2xy+7y^2$	2
-55	$x^2+xy+14y^2, 2x^2 \pm xy+7y^2, 4x^2+3xy+4y^2$	4
-56	$x^2+14y^2, 2x^2+7y^2, 3x^2 \pm 2xy+5y^2$	4
-59	$x^2+xy+15y^2, 3x^2 \pm xy+5y^2$	3
-60	$x^2+15y^2, 3x^2+5y^2$	2

次に, 判別式 D が正かつ平方数でないときの簡約形式について $5 \leq D \leq 76$ までまとめる. h_D は判別式 D に対する簡約形式の個数である.

D	判別式 D の簡約形式	h_D
5	$x^2 - xy - y^2$	1
8	$x^2 - 2xy - y^2$	1
12	$x^2 - 2xy - 2y^2, 2x^2 - 2xy - y^2$	2
13	$x^2 - 3xy - y^2$	1
17	$x^2 - 3xy - 2y^2$	1
20	$x^2 - 4xy - y^2, 2x^2 - 2xy + 2y^2$	2
21	$x^2 - 3xy - 3y^2, 3x^2 - 3xy - y^2$	2
24	$x^2 - 4xy - 2y^2, 2x^2 - 4xy - y^2$	2
28	$x^2 - 4xy - 3y^2, 3x^2 - 2xy - 2y^2$	2
29	$x^2 - 5xy - y^2$	1
32	$x^2 - 4xy - 4y^2, 4x^2 - 4xy - y^2$	2
33	$x^2 - 5xy - 2y^2, 2x^2 - 5xy - y^2$	2
37	$x^2 - 5xy - 3y^2$	1
40	$x^2 - 6xy - y^2, 2x^2 - 4xy - 3y^2$	2
41	$x^2 - 5xy - 4y^2$	1
44	$x^2 - 6xy - 2y^2, 2x^2 - 6xy - y^2$	2
45	$x^2 - 5xy - 5y^2, 5x^2 - 5xy - y^2$	2
48	$x^2 - 6xy - 3y^2, 3x^2 - 6xy - y^2$	2
52	$x^2 - 6xy - 4y^2$	1
53	$x^2 - 7xy - y^2$	1
56	$x^2 - 6xy - 5y^2, 5x^2 - 4xy - 2y^2$	2
57	$x^2 - 7xy - 2y^2, 2x^2 - 7xy - y^2$	2
60	$x^2 - 6xy - 6y^2, 2x^2 - 6xy - 3y^2, 3x^2 - 6xy - 2y^2, 6x^2 - 6xy - y^2$	4
61	$x^2 - 7xy - 3y^2$	1
65	$x^2 - 7xy - 4y^2, 2x^2 - 5xy - 5y^2$	2
68	$x^2 - 8xy - y^2, 2x^2 - 6xy - 4y^2$	2
69	$x^2 - 7xy - 5y^2, 3x^2 - 3xy - 5y^2$	2
72	$x^2 - 8xy - 2y^2$	1
73	$x^2 - 7xy - 6y^2$	1
76	$x^2 - 8xy - 3y^2, 3x^2 - 8xy - y^2$	2

2.3　ディリクレ積と類群

この節では, 2 次形式の演算を導入し, 実際に $C_D/\sim$ が群になるかどうかを調べていく. また, 本論文の最後のほうに, この演算を拡張して, 2 元 3 次形式などさらに高次な形式に適用できる考えを第 5 章に紹介しているので, そちらも参照してほしい.

命題 2.33 $D \in \mathbb{Z}$ を $D \equiv 0, 1 \pmod 4$ かつ平方数ではない整数とする $a_1, b_1, c_1, a_2, b_2, c_2$ は

$$\begin{cases} b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2 = D, \\ \gcd(a_1, a_2, \frac{b_1+b_2}{2}) = 1 \end{cases}$$

を満たすと仮定すると, $j = 1, 2$ に対し,

$$\begin{aligned} &(1) \qquad b_3 \equiv b_j \pmod{2a_j}, \\ &(2) \qquad b_3^2 \equiv D \pmod{4a_1a_2} \end{aligned}$$

となる $b_3 \in \mathbb{Z}$ が $\bmod 2a_1a_2$ で一意に存在する.

注意 2.34 $i = 1, 2$ に対し, $b_i^2 \equiv D \pmod 4$ より, b_i と D の偶奇は同じである.

命題 2.33 の証明. 主張の連立合同式は, $i = 1, 2$ に対し,

$$\begin{aligned} &(1') \qquad a_ib_3 \equiv a_2b_i \pmod{2a_1a_2}, \\ &(2') \qquad \frac{b_1+b_2}{2}b_3 \equiv \frac{b_1b_2+D}{2} \pmod{2a_1a_2} \end{aligned}$$

といい換えられることを示す. まず, $((1), (2)$ ならば $(1'), (2'))$ を示す.
(1) より, $b_3^2 - (b_1+b_2)b_3 + b_1b_2 = (b_3 - b_1)(b_3 - b_2) \equiv 0 \pmod{4a_1a_2}$ であり
(2) より, $b_3^2 - (b_1+b_2)b_3 + b_1b_2 \equiv (b_1b_2 + D) - (b_1+b_2)b_3 \pmod{4a_1a_2}$ である.
ここで, 注意 2.34 より $2 \mid b_1 + b_2$ より, $2 \mid b_1(b_1+b_2) - 4a_1c_1 = b_1b_2 + D$ であるから, 両辺を 2 で割り

$$\frac{b_1+b_2}{2}b_3 \equiv \frac{b_1b_2+D}{2} \pmod{2a_1a_2}$$

を得るので, $(2')$ が示せた. $(1')$ については, (1) の両辺に a_i をかければよい.
次に, $((1'), (2')$ ならば $(1), (2))$ を示す. 判別式は正のときは平方数でないから, $a_1, a_2 \neq 0$ と仮定してよいので, (1) については両辺を a_i で割ればよい.
(2) については, (2') より $(b_1+b_2)b_3 \equiv b_1b_2 + D \pmod{4a_1a_2}$ であるから, 上と同様に, $b_3^2 + b_1b_2 \equiv (b_1+b_2)b_3 \pmod{4a_1a_2}$ を得る.
よって,

$$b_3^2 \equiv D \pmod{4a_1a_2}$$

である. これから, $(1'), (2')$ を満たす整数 b_3 が $\bmod 2a_1a_2$ で一意に存在することを示していく.
まず, 存在性について示していく. $\gcd(a_1, a_2, \frac{b_1+b_2}{2}) = 1$ より,

$$a_1n_1 + a_2n_2 + \frac{b_1+b_2}{2}n_3 = 1$$

となる $n_1, n_2, n_3 \in \mathbb{Z}$ が存在し, これらを固定する. $b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2 = D$ であるから,

$$a_1 D \equiv a_1 b_2^2 \pmod{2a_1a_2},$$
$$a_1 D \equiv a_1 b_2^2 \pmod{2a_1a_2}.$$

さらに, $b_1 \equiv b_2 \pmod 2$ であるから $a_1a_2b_1 \equiv a_1a_2b_2 \pmod{2a_1a_2}$ である. この 3 つのことに注意する. 具体的に,

$$b_3 \equiv a_1b_2n_1 + a_2b_1n_2 + \frac{b_1b_2 + D}{2}n_3 \pmod{2a_1a_2}$$

とすると, $(1')$, $(2')$ を満たすことがわかる.

次に一意性について示す. b_3, b_3' が $(1')$, $(2')$ を満たすと仮定すると

$$2a_1a_2 \mid a_1(b_3 - b_3'), a_2(b_3 - b_3'), \frac{b_1 + b_2}{2}(b_3 - b_3')$$

であり, $\gcd(a_1, a_2, \frac{b_1+b_2}{2}) = 1$ であるから, $2a_1a_2 \mid b_3 - b_3'$ より $b_3 \equiv b_3' \pmod{2a_1a_2}$ となり $\bmod 2a_1a_2$ で一意である. □

注意 2.35 上の定理は $\gcd(a_1, a_2, \frac{b_1+b_2}{2}) \neq 1$ のときでも, その最大公約数で割れば命題 2.33 の条件を満たす.

この結果により, 2 次形式の二項演算を定義できる.

定義 2.36 $D \in \mathbb{Z}$ を $D \equiv 0, 1 \pmod 4$ かつ平方数でない整数とする. $f = (a_1, b_1, c_1)$, $g = (a_2, b_2, c_2)$ を判別式 D をもつ 2 次形式で, $\gcd(a_1, a_2, \frac{b_1+b_2}{2}) = 1$ を満たすと仮定する.

このとき演算 $\circ$ を, 次のように定義する :

$f \circ g = (a_3, b_3, c_3)$
ただし, $a_3 = a_1a_2$, b_3 は命題 2.33 の連立合同式の根, $c_3 = \frac{b_3^2 - D}{4a_3}$.

この演算 $\circ$ を**ディリクレ積**という.

注意 2.37 $\gcd(a_1, a_2, \frac{b_1+b_2}{2}) \neq 1$ ではなくても, 前の注意により定義ができる.

この演算によりに 2 つの 2 次形式の合成を計算することができるが, 結果が一意でない可能性がある. 次にそれについて証明していく.

その前に 2 次形式の調和について定義する. 以降, この節では D は平方数でない $D \equiv 0, 1 \pmod 4$ を満たす整数と仮定する.

定義 2.38 $f = (a, b, c), g = (A, B, C)$ を判別式 D をもつ 2 次形式とする.
f と g は**調和している** $\overset{\text{def}}{\iff}$ 以下の 3 つを満たす :
(1) $aA \neq 0$;
(2) $b = B$;
(3) $a \mid C$ かつ $A \mid c$.

注意 2.39 定義 2.36 の演算は, 2 つの 2 次形式を調和している 2 つの 2 次形式に変換して合成している. 実際, $(a_1, b_1, c_1) \sim (a_1, b_3, a_2c_3), (a_2, b_2, c_2) \sim (a_2, b_3, a_1c_3)$ である.

演算の結果が一意であることを示すために, まずいくつか補題を用意する.

補題 2.40 $0 \neq M \in \mathbb{Z}$ とする. 原始形式 $f = (a, b, c)$ に対して, f は M と互いに素になる整数を原始的に表現する.

証明. f が原始的に表現する整数を割る素数は a, b, c のいずれかと互いに素であることに注意する. ここで,

$$\begin{aligned} S_a &:= \{p_a : \text{素数} \mid p_a \mid M \text{ かつ } p_a \nmid a\}, \\ S_c &:= \{p_c : \text{素数} \mid p_c \mid M \text{ かつ } p_a \nmid c \text{ かつ } p_c \mid a\}, \\ S_b &:= \{p_b : \text{素数} \mid p_b \mid M \text{ かつ } p_b \nmid b \text{ かつ 「} p_b \mid a \text{ または } p_b \mid c\text{」}\} \end{aligned}$$

とする. さらに,

$$X = \prod_{p \in S_c} p, Y = \prod_{p \in S_a} p$$

と定める. すると, $p \in S_a$ は $p \mid Y$ であり, $p \nmid X$ かつ $p \nmid a$ であるから, $p \nmid f(X, Y)$ である. 同様にして, $p \in S_c$ のときも $p \nmid f(X, Y)$ である.

さらに, $p \in S_b$ に対し, $p \mid a, p \mid c$ であるが $p \nmid X, Y$ または $p \nmid b$ であるから, $p \nmid f(X, Y)$ であるので, $f(X, Y)$ は M と互いに素である. □

補題 2.41 任意の D に対し, $C_1 \neq C_2$ となる $C_1, C_2 \in C_D/\sim$ をとる. $0 \neq M \in \mathbb{Z}$ をとったとき,

$$\gcd(a_1, a_2) = 1, \gcd(a_1 a_2, M) = 1$$

となる調和している 2 つの 2 次形式 $f_j = (a_j, b, *) \in C_j$ が存在する.

注意 2.42 補題 2.41 において, y^2 の係数は判別式の定義により x^2 の係数と xy の係数が分かれば求めることができるので, 省略するために $*$ を用いた.

補題 2.41 の証明. 任意の $f_1 \in C_1$ に対し, 補題 2.40 により $\gcd(p, q) = 1$ となる $(p, q) \in \mathbb{Z}^2$ を

$$0 \neq a_1 = f(p, q) \text{ かつ } \gcd(a_1, M) = 1$$

となるようにとることができる. さらに, $(r, s) \in \mathbb{Z}^2$ を

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

となるようにとる. その行列を f に作用させると, $F_1 = (a_1, b_1, *) \in C_1$ を得る. 同様にして, $F_2 = (a_2, b_2, *) \in C_2$ を $a_2 \neq 0$, $\gcd(a_2, a_1 M) = 1$ となるようにとれる.

また $\gcd(a_1, a_2) = 1$ であるから, $n_1, n_2 \in \mathbb{Z}$ を

$$b_1 + 2a_1 n_1 = b_2 + 2a_2 n_2$$

となるようにとれる. これを b とおく. ここで,

$$\begin{pmatrix} 1 & 0 \\ n_j & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

を F_i に作用させ, $f_i = (a_i, b, *)$ とする. これらは調和しており, 主張を満たしている. □

この補題により, 次が示せる：

命題 2.43 f_1, f_2, g_1, g_2 を判別式 D をもつ原始形式とする. このとき, $i = 1, 2$ に対し $f_i \sim g_i$ ならば, $f_1 \circ g_1 \sim f_2 \circ g_2$ である.

証明. $i = 1, 2$ に対し, $f_j = (a_j, b, c_j), g_j = (A_j, B, C_j)$ とおく. 注意 2.39 より f_1 と g_1, f_2 と g_2 はそれぞれ調和していると仮定してよい. この証明に対しては, いくつかの場合を用意してから, それを使って一般の場合に応用させていく.

(i) $f_1 = g_1$ かつ $\gcd(a_1, A_2) = 1$ のとき, f_1 は f_2, g_2 と調和しているから, $f_1 \circ f_2 \sim f_1 \circ g_2$ を示せばよい.

$$\gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

を, f_2 に作用させ g_2 となるような行列とすると,

$${}^t\gamma \begin{pmatrix} a_2 & \frac{b}{2} \\ \frac{b}{2} & c_2 \end{pmatrix} = \begin{pmatrix} A_2 & \frac{b}{2} \\ \frac{b}{2} & C_2 \end{pmatrix} \gamma^{-1}$$

であるから, $-A_2 q = c_2 r$ である. f_1 と f_2 が調和しているから $a_1 \mid c_2$ となるので, $\gcd(a_1, A_2) = 1$ より, $a_1 \mid q$ である. よって,

$$\gamma' = \begin{pmatrix} p & \frac{q}{a_1} \\ a_1 r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

とすると, この γ' を $f_1 \circ f_2$ に作用させると $f_1 \circ g_2$ となる.

(ii) $b = B$ かつ $\gcd(a_1, A_2) = 1$ のとき, f_1 と g_2 の判別式の関係からこれらは調和しているから, (i) により,

$$f_1 \circ f_2 \sim f_1 \circ g_2 \sim g_1 \circ g_2$$

となる.

(iii) $\gcd(a_1 a_1, A_1 A_2) = 1$ のとき, $n, n' \in \mathbb{Z}$ を

$$b + 2a_1 a_2 n = B + 2A_1 A_2 n'$$

となるように定め, これを B' とおく. ここで,

$$\gamma_i = \begin{pmatrix} 1 & 0 \\ a_i n & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

とおき, f_1 に γ_2, f_2 に γ_1 を作用させて得た 2 次形式を F_1, F_2 とおくと,

$$F_1 = (a_1, B', *),\ F_2 = (a_2, B', *)$$

となる. さらに, 行列

$$\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

を $f_1 \circ f_2$ に作用させて得た 2 次形式を H_1 とすると,

$$H_1 = (a_1 a_2, B, *)$$

である. 判別式の定義から,

$$a_1 a_2 \,\Big|\, \frac{B^2 - D}{4}$$

であるから F_1 と F_2 の判別式の関係により, これらは調和している.
同様にして, g_j に γ_j を作用させて得た 2 次形式 $G_j = (A_j, B', *)$ についても調和しており,

$$H_1 = (A_1 A_2, B, *) \sim g_1 \circ g_2$$

となる. よって (ii) により,

$$f_1 \circ f_2 \sim H_1 \sim H_2 \sim g_1 \circ g_2$$

となる.

(iv) 一般のとき, 補題 2.40 により,

$$\gcd(A_1' A_2', a_1 a_2 A_1 A_2) = 1$$

かつ, f_j と同値な $F_j = (A_j', B, *)$ が存在する. (iii) により, $f_1 \circ f_2 \sim F_1 \circ F_2 \sim g_1 \circ g_2$ となる.

□

命題 2.43 により, この演算の結果は同値関係を除いて一意に決まることがわかる. そして, 次の定理がいえる :

定理 2.44 $C_D/\sim$ は有限アーベル群になる.

証明. まず, 演算で閉じていることを背理法で示す. 任意の $f = (a_1, b_1, c_1), g = (a_2, b_2, c_2) \in C_D/\sim$ をとったときに, $f \circ g = (a_3, b_3, c_3)$ とする. このとき,

$$p \mid \gcd(a_3, b_3, c_3)$$

となる素数 p が存在すると仮定する. 注意 2.39 より $(a_1, b_1, c_1) \sim (a_1, b_3, a_2 c_3), (a_2, b_2, c_2) \sim (a_2, b_3, a_1 c_3)$ であることに注意する. 背理法の仮定より, $p \mid a_1 a_2$, $p \mid b_3$, $p \mid c_3$ であるから, $p \mid a_1$ ならば $p \mid \gcd(a_1, b_3, a_2 c_3)$ となる. これは, 命題 2.7 より, (a_1, b_1, c_1) が原始形式であることに矛盾するので, (a_3, b_3, c_3) は原始形式である. また, $f \circ g$ の判別式が D であることは, 演算の定義より明らかである.
結合法則, 可換性については演算の定義より明らかであり, 有限性については簡約形式の有限性により明らかである.

単位元は

$$e = \begin{cases} (1, 0, -\frac{D}{4}) & (D \equiv 0 \pmod 4), \\ (1, 1, \frac{1-D}{4}) & (D \equiv 1 \pmod 4) \end{cases}$$

である. 実際に, $D \equiv 0 \pmod 4$ のとき, $(a, b, c) \circ (1, 0, -\frac{D}{4})$ を計算していく. 命題 2.33 (1), (2) の連立合同式に当てはめると, $(a_3, b_3, c_3) \sim (a, b, c)$ であるから,

$$(a, b, c) \circ (1, 0, -\tfrac{D}{4}) = (a, b, c)$$

となる. $D \equiv 1 \pmod 4$ のときも同様にして示すことができる.

逆元については, $f = (a, b, c)$ に対して, $f^{-1} = (a, -b, c) \sim (c, b, a)$ である. 実際, $D \equiv 0 \pmod 4$ のとき, $(a, b, c) \circ (c, b, a)$ を計算してみると, 単位元のときと同じようにして, $(a_3, b_3, c_3) \sim (ac, b, 1)$ となるので,

$$(a, b, c) \circ (c, b, a) = (ac, b, 1)$$

となる. ここで b が偶数であることに注意して,

$$\begin{pmatrix} ac & \frac{b}{2} \\ \frac{b}{2} & 1 \end{pmatrix} = {}^t\begin{pmatrix} \frac{b}{2} & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -\frac{D}{4} \end{pmatrix} \begin{pmatrix} \frac{b}{2} & 1 \\ -1 & 0 \end{pmatrix}$$

であるから, $(ac, b, 1) \sim (1, 0, -\frac{D}{4})$ となるので,

$$(a, b, c) \circ (c, b, a) = (1, 0, -\tfrac{D}{4})$$

である. $D \equiv 1 \pmod 4$ のときも同様に示すことができる.

以上のことから, $C_D/\sim$ は有限アーベル群であることが示された. □

定理 2.44 をうけて, 次のことを定義する :

定義 2.45 (1) 任意の D に対し, 有限アーベル群 $C_D/\sim$ を判別式 D の 2 次形式に対する**類群**という.
(2) $h_D := |C_D/\sim| < \infty$ を判別式 D に対する**類数**という.
(3) 判別式 D の 2 次形式に対する類群の単位元

$$e = \begin{cases} (1, 0, -\frac{D}{4}) & (D \equiv 0 \pmod 4), \\ (1, 1, \frac{1-D}{4}) & (D \equiv 1 \pmod 4) \end{cases}$$

を判別式 D の**基本形式**という.

簡約形式と類数の表は 34 ページから 35 ページに載せている.

以上により, 2 次形式の類数を定義することができた. 次の節では 2 次体について述べていく. そして, 2 次形式と 2 次体が対応することを示していく.

2.4　2 次体のイデアル類群と 2 次形式との対応

この節では, まず 2 次体に関するイデアル類群について述べていく. その後, 2 次形式との対応を示していく.
一般に, $\mathbb{Q}$ 上の 2 次体は $\mathbb{Q}(\sqrt{D})$ (D は平方因子をもたない) という形になっている. 実際, 2 次体 F の生成元を α とし, α の $\mathbb{Q}$ 上の最小多項式を x^2+bx+c $(b,c\in\mathbb{Q})$ とすると, これの根は

$$\alpha=\frac{-b\pm\sqrt{b^2-4c}}{2}$$

であるから, 2 次体 F は

$$F=\mathbb{Q}(\alpha)=\mathbb{Q}(\tfrac{-b\pm\sqrt{b^2-4c}}{2})=\mathbb{Q}(\sqrt{b^2-4c})=\mathbb{Q}(\sqrt{D})$$

である. 一般に $D>0$ のとき F を**実 2 次体**といい, $D<0$ のとき F を**虚 2 次体**という.
次に, 2 次体の整数環について述べていく. 証明については省略する.

定理 2.46 2 次体 F を $F=\mathbb{Q}(\sqrt{D})$ とするとき, F の整数環 $\mathfrak{O}_F$ は以下のようにかける :

$$\mathfrak{O}_F=\begin{cases}\mathbb{Z}[\frac{1+\sqrt{D}}{2}] & (D\equiv 1\ (\mathrm{mod}\ 4)),\\ \mathbb{Z}[\sqrt{D}] & (D\not\equiv 1\ (\mathrm{mod}\ 4)).\end{cases}$$

定理 2.46 により, 2 次体の判別式を求めることができる.

命題 2.47 2 次体 F に対し, $F=\mathbb{Q}(\sqrt{D})$ とかけるとき, F の判別式 Δ_F は以下のようにかける :

$$\Delta_F=\begin{cases}D & (D\equiv 1\ (\mathrm{mod}\ 4)),\\ 4D & (D\not\equiv 1\ (\mathrm{mod}\ 4)).\end{cases}$$

注意 2.48 判別式の表し方により, 2 次体 F は $F=\mathbb{Q}(\sqrt{\Delta_F})$ とかけることになる.

2 次体 $F=\mathbb{Q}(\sqrt{D})$ の整数環 $\mathfrak{O}_F$ がどのような形をしているかわかったので, それからノルムも定式的に求めることができる. つまり, $\alpha\in\mathfrak{O}_F$ に対して,

$$N_F(\alpha)=\begin{cases}x^2+xy+\dfrac{1-D}{4}y^2 & (D\equiv 1\ (\mathrm{mod}\ 4)),\\ x^2-Dy^2 & (D\not\equiv 1\ (\mathrm{mod}\ 4))\end{cases}$$

という形になっている. ただし, $x,y\in\mathbb{Z}$ である.
次に, 2 次体と 2 次形式を関連させていく. 実際には 2 次体 F に対して, 判別式 Δ_F をもつ 2 次形式の類群 $C_{\Delta_F}/\sim$ を対応させていく.

注意 2.49 逆はできない. 例えば判別式 32 の 2 次体は存在しない.

その前に, 狭義イデアル類群を定義する. これはイデアル類群を定義した際に F の整数環 $\mathfrak{O}_F$ の分数イデアルのなすアーベル群 I_F を単項分数イデアルのなすアーベル群 P_F で割って定義したが, 狭義イデアル類群は P_F の部分群で I_F を割る群のことである.

定義 2.50 F を代数体とする. $P_F^+ := \{(\alpha) \in P_F \mid N_F(\alpha) > 0\}$ とするとき, $Cl_F^+ := I_F/P_F^+$ を F の**狭義イデアル類群**という. また, $|Cl_F^+|$ を**狭義類数**といい, h_F^+ とかく.

注意 2.51 狭義イデアル類群についても同値関係を導入して定義することができる.
代数体 F の整数環 $\mathfrak{O}_F$ の分数イデアル I, J に対し, 次のような同値関係を導入する :

$$I \overset{+}{\sim} J \overset{\text{def}}{\Longleftrightarrow} (\alpha)I = (\beta)J, N_F(\alpha\beta) > 0 \text{ となる } \alpha, \beta \in \mathfrak{O}_F \text{ が存在する.}$$

この同値関係により I_F を割った群を狭義イデアル類群ともみることができ, 上の定義と同じである.

2 次体においては狭義イデアル類群と普通のイデアル類群の位数の差は以下の場合によって異なってくる.

命題 2.52 2 次体 F の狭義類数 h_F^+ と類数 h_F の関係は, 次のように与えられる :

$$h_F^+ = \begin{cases} h_F & (\Delta_F < 0 \text{ のとき}), \\ h_F & (\Delta_F > 0 \text{ かつ } N_F(u) = -1 \text{ となる } u \in {\mathfrak{O}_F}^\times \text{が存在するとき}), \\ 2h_F & (\text{その他}). \end{cases}$$

証明. それぞれについて, 場合分けして考える.

(i) $\Delta_F < 0$ のときは, すべての元のノルムは正より $P_F^+ = P_F$ であるから $Cl_F^+ = Cl_F$ である.

(ii) $\Delta_F > 0$ かつ $N_F(u) = -1$ となる $u \in {\mathfrak{O}_F}^\times$ が存在するときは, $N_F(\alpha) < 0$ となる $(\alpha) \in P_F$ に対し, $(\alpha) = (u\alpha) \in P_F^+$ より $P_F^+ = P_F$ であるから $Cl_F^+ = Cl_F$ である.

(iii) それ以外のとき, 写像 ϕ を次のように定義する :

$$\begin{array}{rccc} \phi \ : & P_F & \longrightarrow & \{\pm 1\} \\ & \cup & & \cup \\ & (\alpha) & \longmapsto & \operatorname{sgn}(N_F(\alpha)) \end{array}$$

すると, この写像は全射準同型写像であり, $\operatorname{Ker}(\phi) = P_F^+$ である.
したがって準同型定理より, $h_F^+ = 2h_F$ である.

□

まずは 2 次形式と虚 2 次体を関連づける. その前にいくつか補題を用意する.

補題 2.53 F を 2 次体とする. $I = [\alpha_1, \alpha_2]$ を整数環 $\mathfrak{O}_F$ の分数イデアルとしたとき,

$$f_I = \frac{N_F(\alpha_1 x + \alpha_2 y)}{N^F(I)}$$

は判別式 Δ_F の 2 次形式である.

証明. f_I を実際に計算すると, σ を F から $\mathbb{C}$ への埋め込みで恒等でないものとすると,

$$f_I = \frac{N_F(\alpha_1)x^2 + T_F(\alpha_1\alpha_2{}^\sigma)xy + N_F(\alpha_2)y^2}{N^F(I)}$$

となるから判別式は, 定理 1.48 より,

$$\begin{aligned}\Delta_{f_I} &= \frac{T_F(\alpha_1\alpha_2{}^\sigma) - 4N_F(\alpha_1)N_F(\alpha_2)}{N^F(I)^2} \\ &= \frac{(\alpha_1\alpha_2{}^\sigma - \alpha_1{}^\sigma\alpha_2)^2}{N^F(I)^2} \\ &= \Delta_F\end{aligned}$$

となる. □

補題 2.54 判別式 Δ_F をもつ 2 次体 F に対し, 判別式 Δ_F となる原始形式 $f = (a, b, c) \in C_{\Delta_F}$ をとると,

$$I = \left(a, \frac{-b + \sqrt{\Delta_F}}{2}\right)$$

は F の整数環 $\mathfrak{O}_F$ のイデアルである.

証明. $\omega = \frac{\Delta_F + \sqrt{\Delta_F}}{2}$ とおくと, $\mathfrak{O}_F = \mathbb{Z}[1, \omega]$ であるから,

$$\omega I \subset I$$

を示せばよいので, $a\omega, \frac{-b+\sqrt{\Delta_F}}{2} \cdot \omega \in I$ を示せばよい.

まず, $\Delta_F = b^2 - 4ac \equiv b^2 \equiv b \equiv -b \pmod 2$ であるから,

$$\mathbb{Z}[1, \omega] = \mathbb{Z}[1, \tfrac{-b+\sqrt{\Delta_F}}{2}]$$

より, $a\omega \in I$ である.

また, $\Delta_F = b^2 - 4ac \equiv b^2 \pmod{4a}$ であるから,

$$\begin{aligned}\frac{-b + \sqrt{\Delta_F}}{2} \cdot \omega &= \frac{\Delta_F}{2} \cdot \frac{-b + \sqrt{\Delta_F}}{2} + \frac{\sqrt{\Delta_F}}{2} \cdot \frac{-b + \sqrt{\Delta_F}}{2} \\ &= \frac{\Delta_F}{2} \cdot \frac{-b + \sqrt{\Delta_F}}{2} + \frac{-b\sqrt{\Delta_F} + \Delta_F}{4} \\ &\equiv \frac{\Delta_F}{2} \cdot \frac{-b + \sqrt{\Delta_F}}{2} - \frac{b}{2} \cdot \frac{-b + \sqrt{\Delta_F}}{2} \pmod a \\ &\equiv \frac{\Delta_F - b}{2} \cdot \frac{-b + \sqrt{\Delta_F}}{2} \pmod a\end{aligned}$$

となるから, $\frac{-b+\sqrt{\Delta_F}}{2} \cdot \omega \in I$ である. □

補題 2.53, 補題 2.54 を使って, 次の定理を示す :

定理 2.55 (虚 2 次体の整数環のイデアルと 2 次形式との対応) 判別式 Δ_F をもつ虚 2 次体 F に対し,

$$Cl_F = Cl_F^+ \simeq C_{\Delta_F}/\sim$$

が成り立つ. 特に, $h_F = h_{\Delta_F}$ である.

証明. 写像 ϕ を

$$\begin{array}{rccc} \phi \ : & C_{\Delta_F} & \longrightarrow & Cl_F \\ & \cup & & \cup \\ & f=(a,b,c) & \longmapsto & [a, \frac{-b+\sqrt{\Delta_F}}{2}] \end{array}$$

と定義する. この写像は補題 2.54 により定義できる.

まず, $f \sim g$ ならば $\phi(f) \sim \phi(g)$ を示す. $f(x,1)=0$ と $g(x,1)=0$ の虚部が正の根をそれぞれ α_1, α_2 とすると命題 2.12 により,

$$\alpha_1 = \frac{p\alpha_2+q}{r\alpha_2+s} \text{ かつ } ps-qr=1$$

となる $p,q,r,s \in \mathbb{Z}$ が存在する. また, $[a, \frac{-b+\sqrt{\Delta_F}}{2}] = a[1, \frac{-b+\sqrt{\Delta_F}}{2a}]$ とであるから,

$$\begin{aligned} \phi(f) &= a[1, \tfrac{-b+\sqrt{\Delta_F}}{2a}] = a[1,\alpha_1] \\ &= a[1, \tfrac{p\alpha_2+q}{r\alpha_2+s}] \\ &\sim [r\alpha_2+s, p\alpha_2+q] \\ &= [1,\alpha_2] \sim \phi(g) \end{aligned}$$

となっている. 次に, ϕ が全単射であることを示す.

単射については,

$$\phi(f) \sim \phi(g) \text{ ならば } f \sim g$$

を示せばよい. $f(x,1)=0$ と $g(x,1)=0$ の虚部が正の根をそれぞれ α_1, α_2 とすると, $\phi(f) \sim \phi(g)$ より,

$$\lambda[1,\alpha_1] = [1,\alpha_2]$$

となる $\lambda \in F^\times$ が存在する. これを $\mathbb{Z}$ 上の加群として基底変換しているというように見れば,

$$\lambda \begin{pmatrix} \alpha_1 \\ 1 \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} \alpha_2 \\ 1 \end{pmatrix}$$

となる

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$$

が存在する. これを変形すると,

$$\alpha_1 = \frac{p\alpha_2+q}{r\alpha_2+s}$$

となるが, α_1, α_2 の決め方と命題 2.12 により, $ps-qr=1$ かつ $f(x,1)$ と $g(px+q, rx+s)$ の虚部が正の根は一致することになるから, $f \sim g$ である.

全射については, $I=[\alpha,\beta] \in I_F$ をとり, $\tau = \frac{\beta}{\alpha}$ とおく. ($N_F(\alpha)>0$ であることに注意する.)
すると, $I=[\alpha,\beta]=\alpha[1,\tau] \sim [1,\tau]$ であるので, $I=[1,\tau]$ と仮定してよい. I に対応する 2 次形式を

$$f_I = \frac{N_F(x+\tau y)}{N^F(I)}$$

とすると, 補題 2.53 により f_I の判別式は Δ_F である. τ の $\mathbb{Q}$ 上の最小多項式を ax^2+bx+c とする. ただし, $a,b,c\in\mathbb{Z}$, $a>0, \gcd(a,b,c)=1$ である. $f_I=(a,b,c)$ であるから ϕ は全射である.

最後に ϕ が準同型写像であることを示す. $\gcd(a,a',\frac{b+b'}{2})=1$ を満たす $f=(a,b,c), g=(a',b',c')\in C_{\Delta_F}$ に対して, 定義 2.36 により

$$f\circ g=(aa', B, \tfrac{B^2-\Delta_F}{4aa'})$$

とかける. ただし, B は,

$$\begin{cases} B\equiv b & (\mathrm{mod}\ 2a),\\ B\equiv b' & (\mathrm{mod}\ 2a'),\\ B^2\equiv \Delta_F & (\mathrm{mod}\ 4aa') \end{cases}$$

を満たす. よって,

$$\phi(f)=[a,\tfrac{-b+\sqrt{\Delta_F}}{2}], \phi(g)=[a',\tfrac{-b'+\sqrt{\Delta_F}}{2}], \phi(f\circ g)=[aa',\tfrac{-B+\sqrt{\Delta_F}}{2}]$$

となる. 簡単のために $\Delta=\frac{-B+\sqrt{\Delta_F}}{2}$ とおくと, これら 3 つのイデアルは,

$$\phi(f)=[a,\Delta], \phi(g)=[a',\Delta], \phi(f\circ g)=[aa',\Delta]$$

とかけるから, 結局は $[a,\Delta]\cdot[a',\Delta]=[aa',\Delta]$ となることを示せばよい.
実際, $\Delta^2\equiv -B\Delta\ (\mathrm{mod}\ aa')$ であるから,

$$[a,\Delta]\cdot[a',\Delta]=[aa',a\Delta,a'\Delta,\Delta^2]=[aa',a\Delta,a'\Delta,-B\Delta].$$

しかし, $\gcd(a,a',B)=1$ より, $[a,\Delta]\cdot[a',\Delta]=[aa',\Delta]$ となるから, $\phi(f\circ g)=\phi(f)\cdot\phi(g)$ である. □

次に, 実 2 次体について議論する. 実 2 次体に注意すべきことはノルムが常に正になるとは限らないということである. 大まかな方針は虚 2 次体の証明とほぼ同じであるが, それにもう少しだけ追加させて議論していく. その前に, この証明で必要になる写像を 1 つ定義する. 写像 π を

$$\begin{array}{rccc} \pi\ :\ F & \longrightarrow & \mathbb{Q}\\ \cup & & \cup\\ \tau & \longmapsto & \frac{\tau-\overline{\tau}}{\sqrt{\Delta_F}} \end{array}$$

と定義する. この写像の意味としては $\sqrt{\Delta_F}$ の係数の符号を表している.

定理 2.56 (実 2 次体の整数環のイデアルと 2 次形式との対応) 判別式 Δ_F をもつ実 2 次体 F に対し,

$$Cl_F^+\simeq C_{\Delta_F}/\sim$$

が成り立つ. 特に, $h_F^+=h_{\Delta_F}$ である.

証明. 写像 ϕ を

$$\begin{array}{rccc} \phi\ :\ C_{\Delta_F} & \longrightarrow & Cl_F\\ \cup & & \cup\\ f=(a,b,c) & \longmapsto & [a,\frac{-b+\sqrt{\Delta_F}}{2}]\ (a>0\ \text{のとき}) \end{array}$$

$$\begin{array}{rccc} \phi\ : & C_{\Delta_F} & \longrightarrow & Cl_F \\ & \cup & & \cup \\ & f=(a,b,c) & \longmapsto & (\sqrt{\Delta_F})[a, \frac{-b+\sqrt{\Delta_F}}{2}]\ (a<0 \text{ のとき}) \end{array}$$

と定義する. この写像は補題 2.54 により定義できる.

まず, $f \sim g$ ならば $\phi(f) \overset{+}{\sim} \phi(g)$ を示す. $f=(a,b,c), g=(A,B,C)$ とすると,

$$f(x,y) = g(px+qy, rx+sy) \text{ かつ } ps-qr=1$$

となる $p,q,r,s \in \mathbb{Z}$ が存在する. ここで, α_1 を $f(x,1)=0$ の根で $\pi(\alpha_1)$ の符号が a の符号と同じになるもので, α_2 を $g(x,1)=0$ の根で $\pi(\alpha_2)$ の符号が A の符号と同じになるものとする. 一般性を失うことなく $a>0$ と仮定できる. このときに α_1 と α_2 の関係がどのようになっているのかを見ていく.

$$0 = f(\alpha_1,1) = g(p\alpha_1+q, r\alpha_1+s) = (r\alpha_1+s)^2 g\Big(\frac{p\alpha_1+q}{r\alpha_1+s}, 1\Big)$$

となっており,

$$\pi\Big(\frac{p\alpha_1+q}{r\alpha_1+s}\Big) = \frac{\pi(\alpha_1)}{N_F(r\alpha_1+s)}$$

と計算することができる. $N_F(r\alpha_1+s) = r^2 - \frac{b}{a}rs + \frac{c}{a} = \frac{A}{a}$ であるから, 次の 2 つの場合に分けて考える :

(i) $N_F(r\alpha_1+s)>0$ のとき, a と A の符号は同じであるから,

$$\alpha_2 = \frac{p\alpha_1+q}{r\alpha_1+s}$$

である. $\lambda = r\alpha+s$ とおくと, $N_F(\lambda)>0$ であり, $\lambda[1,\alpha_2]=[1,\alpha_1]$ となる.
よって,

$$\phi(g) \overset{+}{\sim} [1,\alpha_2] \overset{+}{\sim} [1,\alpha_1] \overset{+}{\sim} \phi(f)$$

となる.

(ii) $N_F(r\alpha_1+s)<0$ のとき, a と A の符号は異なるから,

$$\alpha_2 = \frac{p\alpha_1+q}{r\alpha_1+s}$$

である. $\lambda = r\alpha_1+s$ とおくと, $N_F(\lambda)<0$ であり, $\lambda[1,\alpha_2]=[1,\alpha_1]$ となるから, $\lambda(\sqrt{\Delta_F})[1,\alpha_2] = (\sqrt{\Delta_F})[1,\alpha_1]$ であり, $N_F(\lambda\sqrt{\Delta_F})>0$ に注意すると, $(\sqrt{\Delta_F})[1,\alpha_2] \overset{+}{\sim} [1,\alpha_1]$ である.
よって, この場合は

$$\phi(g) \overset{+}{\sim} (\sqrt{\Delta_F})[1,\alpha_2] \overset{+}{\sim} [1,\alpha_1] \overset{+}{\sim} \phi(f)$$

となる.

以上によりどちらの場合でも, $\phi(f) \overset{+}{\sim} \phi(g)$ である.

次に, ϕ が全単射であることを示す. 単射については, まず α_1 を $f(x,1)=0$ の根で $\pi(\alpha_1)$ の符号が a の符号と同じになるもので, α_2 を $g(x,1)=0$ の根で $\pi(\alpha_2)$ の符号が A の符号と同じになるものとする.

$$\lambda[1, \alpha_2] = [1, \alpha_1]$$

となる $N_F(\lambda) > 0$ を満たす $\lambda \in F^\times$ が存在すると仮定できるので,

$$\lambda \begin{pmatrix} \alpha_2 \\ 1 \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} \alpha_1 \\ 1 \end{pmatrix}$$

となる

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$$

が存在する. これを変形すると,

$$\alpha_2 = \frac{p\alpha_1 + q}{r\alpha_1 + s}, \lambda = r\alpha_1 + s$$

となる. ここで,

$$\frac{\pi(\alpha_1)}{\pi(\alpha_2)} N_F(\lambda) = ps - qr$$

であり, $N_F(\lambda) > 0$ であるから, (i) の証明中の計算により, $\pi(\alpha_1)$ と $\pi(\alpha_2)$ の符号が同じになる. よって, $ps - qr = 1$ になるから, 命題 2.12 を同じような方法で $f \sim g$ であることがわかる.

全射, 準同型については, 虚 2 次体のときと同じように証明できる. □

注意 2.57 実は, 2 次形式の判別式が体の判別式でなくても対応させることができる. 例えば注意 2.49 において, 判別式 32 の 2 次体は存在しないが, 判別式 32 となる基底をもつ整域は存在する. (実際は $\mathbb{Z}[2\sqrt{2}]$ がそうである)

このような整域は整環と呼ばれ, 一般にはデデキント整域にはならない. (詳しくは, [11] を参照)

以上により, 狭義イデアル類群の元は同じ判別式をもつ 2 次形式に対応することができるため, 非常に簡単にきれいな形で代表元を求めることができる. さらに, 次も同時に証明されたことになる.

系 2.58 2 次体 F に対し, F の類数 h_F は有限である. つまり, F のイデアル類群 Cl_F は有限アーベル群である.

第 1 章で述べたように, 一般には数の幾何と呼ばれる概念を使って証明するが, 2 次体の場合には類数の有限性は 2 次形式を使って証明されたことになる.

注意すべき点としては実 2 次体のときはノルムが -1 の単数をもつかどうかで変わってしまうことである. それについては第 5 章で述べるペル方程式で今後の課題として述べる.

第3章　クロネッカー·ウェーバーの定理

この章では, アーベル拡大に関する重要な定理であるクロネッカー · ウェーバーの定理について述べ, 実際に証明していく. 証明には, 第 1 章で述べたガロア理論や分解群, 惰性群, 高次分岐群などさまざまな概念を総動員する. この章は, 第 1 節で, 証明の方針を 3 つ述べ, 最初の 1 つを示している. 第 2 節, 第 3 節では, 残りの 2 つを順に示し, 証明を完了させている.

参考文献において, [1], [2], [3](下), [5], [6] を参考にした.

3.1　証明の方針

まず, クロネッカー · ウェーバーの定理がどのようなものかを述べておく. 次のクロネッカー · ウェーバーの定理は, すべてのアーベル体が必ず円分体に含まれることを表している.

定理 3.1 (クロネッカー · ウェーバーの定理) $\mathbb{Q}$ 上アーベル拡大となる代数体 F は円分体に含まれる.

この定理の有用なところとしては, 円分体に含まれることにより, より広い視点でアーベル体を見ることができる. 例えば, 定理 1.43 (1) によりどのような円分体に含まれるかが分かれば, 判別式の素因子を見つけることができる.

証明するにあたって, 次のような方針に沿って示していく :

Step 1. 拡大次数が素数べきのときに定理 3.1 が成り立てば, 一般の拡大次数に対しても定理 3.1 は成り立つ.
Step 2. 拡大次数と判別式が素数べきのときに定理 3.1 は成り立つ.
Step 3. 拡大次数と判別式がどちらも素数べきのときに定理 3.1 が成り立てば, 拡大次数が素数べきかつ判別式が一般のとき, 定理 3.1 は成り立つ.

この節では, Step 1 を示していく. それ以降はかなり準備が必要なので次節で示していく. Step 1 については群論の有限アーベル群の基本定理が必要となる.

命題 3.2 (Step 1) 定理 3.1 が拡大次数が素数べきのときに成り立てば, 一般の拡大次数にも定理 3.1 は成り立つ.

証明. この定理の証明に対しては, 有限アーベル群の基本定理を使う. つまり, 有限位数のアーベル群は巡回群の直積で表せるという定理である.

$F/\mathbb{Q}$ をアーベル拡大とすると p_j を相異なる素数, $a_j \in \mathbb{N}$ としたときに,

$$\mathrm{Gal}(F/\mathbb{Q}) = \prod_{i=1}^{n} G_j, G_j \simeq C_{{p_j}^{a_j}}$$

というようになる. $H_i = \prod_{j\neq i} G_j$ とおき, $F_i = F^{H_i}$ とすると, 定理 1.60 (2) より $|F:\mathbb{Q}| = p_i^{a_i}$ であるから, $|\prod_{i=1}^n F_i : \mathbb{Q}| = |F:\mathbb{Q}|$ となる.

よって,

$$F = \prod_{i=1}^{n} F_i$$

となる. 仮定より, 素数べきの次数のときに成り立っているから,

$$F_i \subset \mathbb{Q}(\zeta_{m_i})$$

となる $m_i \in \mathbb{N}$ が存在する. $l = \mathrm{lcm}(m_1, \cdots, m_n)$ とすれば,

$$F = \prod_{i=1}^{n} F_i \subset \mathbb{Q}(\zeta_{n_1}, \cdots, \zeta_{m_n}) \subset \mathbb{Q}(\zeta_l)$$

となる. □

3.2 拡大次数と判別式がともに素数べきのときについて

前節の命題により, 拡大次数が素数べきのときに成り立つことを証明できれば一般の場合も成り立つことがわかった. この節では, Step 2 である拡大次数と判別式がともに素数べきのときに成り立つことを示していく. これは 2 べきのときはそこまで難しくないが, 奇素数べきの場合がとても難しい.

命題 3.3 (Step 2) 拡大次数 $|F:\mathbb{Q}|$ と判別式 Δ_F がどちらも素数べきであるアーベル体 F は円分体に含まれる.

まず素数が 2 のときについて, この命題を示していく. まず次の補題が必要である :

補題 3.4 (Step 2-1) 拡大次数 $|F:\mathbb{Q}|$ と判別式 Δ_F がどちらも 2 のべきかつ実数体 $\mathbb{R}$ に含まれるアーベル体 F は円分体に含まれる.

証明. $|F:\mathbb{Q}| = 2^m$ とおき, $K = \mathbb{Q}(\zeta_{2^{m+2}})$, $K' = \mathbb{Q}(\zeta_{2^{m+2}} + \zeta_{2^{m+2}}^{-1})$ とする. ($K' = K \cap \mathbb{R}$ である.)
$L = FK'$ とすると, $L/\mathbb{Q}$ は巡回拡大である. 実際, 巡回拡大でなければ定理 1.62 (3) により. $L/\mathbb{Q}$ はアーベル拡大であるから, 2 次の部分体を 2 つもたなければならない.

しかし, Δ_L は 2 べきかつ $L \subset \mathbb{R}$ より, 判別式が 2 べきの実 2 次体は $\mathbb{Q}(\sqrt{2})$ のみだけであるから矛盾するので, $L/\mathbb{Q}$ は巡回拡大である.

よって, 定理 1.60 (2) により, ただ 1 つの次数 2^m の部分体として, $F = K'$ となるから, $F \subset K$ となる. □

補題 3.4 により, 実数体 $\mathbb{R}$ に含まれない場合も示すことができる.

命題 3.5 (Step 2-2) 拡大次数 $|F:\mathbb{Q}|$ と判別式 Δ_F がどちらも 2 のべきで, 実数体 $\mathbb{R}$ に含まれないアーベル体 F は円分体に含まれる.

証明. $F/\mathbb{Q}, \mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ はともにアーベル拡大であるから, 定理 1.62 (3) により, $F(\sqrt{-1})/\mathbb{Q}$ はアーベル拡大であり, $|F(\sqrt{-1}):\mathbb{Q}|$, $\Delta_{F(\sqrt{-1})}$ はともに 2 べきである. $K = F(\sqrt{-1}) \cap \mathbb{R}$ とおくと, 補題 3.4 により,

$$K \subset \mathbb{Q}(\zeta_n)$$

となる $n \in \mathbb{N}$ が存在する. $a, b \in \mathbb{R}$ に対し $F(\sqrt{-1}) = K(a + b\sqrt{-1})$ とおくと $a - b\sqrt{-1} \in F(\sqrt{-1})$ であるから, $a, b^2 \in K$ である. つまり, $a + b\sqrt{-1}$ の K 上の最小多項式は $X^2 - 2aX + (a^2 + b^2)$ となるので, $|F(\sqrt{-1}) : K| = 2$ である.

したがって, $n' = \mathrm{lcm}(n, 4)$ とおくと,

$$F \subset F(\sqrt{-1}) = K(\sqrt{-1}) \subset \mathbb{Q}(\zeta_n, \sqrt{-1}) \subset \mathbb{Q}(\zeta_{n'})$$

となる. □

補題 3.5 により, 命題 3.3 の拡大次数と判別式がともに 2 べきのときは示すことができた. 次に奇素数べきに対して成り立つのかを示していく. 考え方は基本的に 2 べきのときと同様である. つまり, 次の命題が重要になってくる :

命題 3.6 拡大次数 $|F : \mathbb{Q}|$ と判別式 Δ_F がともに奇素数べきとなるアーベル拡大 $F/\mathbb{Q}$ は巡回拡大である.

命題 3.6 を示すためには, 整数環を広げたものを用いて証明する必要があるので, まずその環について定義する. その後, 第 1 章で定義した共役差積の素イデアルの指数を高次分岐群の位数を使って表すことができるヒルベルトの公式を証明する.

3.2.1 ヒルベルトの公式

定義 3.7 F を代数体, I を F の整数環 $\mathfrak{O}_F$ のイデアルとする.

$$\mathfrak{O}_{F,I} := \left\{ \frac{\alpha}{\beta} \;\middle|\; \alpha, \beta \in \mathfrak{O}_F, (\beta, I) = 1 \right\}$$

を F の I 整数環という. これは整域であり, 商体は F である.

これからは $\mathfrak{O}_F$ を少し広げて考えた整域 $\mathfrak{O}_{F,I}$ について考えていく. 環論の用語を使うと, 局所化したようなものである.
本論文では I 整数環の性質については簡単に述べるが, 証明については省略する. (詳しくは [1](下), [3](II) を参照)

まず, 環論的立場からの性質を述べる.

補題 3.8 代数体 F の整数環 $\mathfrak{O}_F$ のイデアル I をとったときに, I の素イデアル分解を,

$$I = \prod_{i=1}^{s} \mathfrak{p}_j{}^{e_j}$$

とすると, $\mathfrak{O}_{F,I}$ の素イデアルは $i = 1, \cdots, n$ に対し, $\mathfrak{p}_i' = \mathfrak{p}_i \mathfrak{O}_{F,I}$ の有限個であり, それ以外は全て $\mathfrak{O}_{F,I}$ になる.

この補題により, 次の命題が示される :

補題 3.9 代数体 F に対し, F の整数環 $\mathfrak{O}_F$ のイデアル I をとると, $\mathfrak{O}_{F,I}$ は PID である.

よって, この 2 つの補題から, PID はデデキント整域であるから $\mathfrak{O}_{F,I}$ のイデアルは素イデアル分解可能で, さらにその素イデアルは有限個しかない.

次に, 第 1 章で行った相対拡大について考えていく. 相対拡大 K/F に対し, I を $\mathfrak{O}_F$ のイデアルとすると, 2 つの I 整数環 $\mathfrak{O}_{K,I}$ と $\mathfrak{O}_{F,I}$ を考えることができる. これら 2 つの差は次の命題によりわかる :

補題 3.10 K/F を代数体の相対拡大とする. F の整数環 $\mathfrak{O}_F$ のイデアル I に対し,

$$\mathfrak{O}_{K,I} = \mathfrak{O}_K \mathfrak{O}_{F,I}.$$

次に, 相対拡大 K/F と $\mathfrak{O}_F$ のイデアル I に対し, 共役差積 $(\mathfrak{O}_{K,I}^*)^{-1}$ を考える. $\mathfrak{O}_{K,I}^*$ の定義を確認すると,

$$\mathfrak{O}_{K,I}^* := \left\{ \alpha \in K \mid T_{K/F}(\alpha \mathfrak{O}_{K,I}) \subset \mathfrak{O}_{F,I} \right\}$$

である. これに対しては, 次のことがいえる :

補題 3.11 K/F を代数体の相対拡大とする. F の整数環 $\mathfrak{O}_F$ のイデアル I に対し,

$$(\mathfrak{O}_{K,I}^*)^{-1} = D_{K/F} \mathfrak{O}_{K,I}.$$

補題 3.11 において, イデアル I を $\mathfrak{O}_F$ の素イデアル $\mathfrak{p}$ として考え. これを $\mathfrak{O}_K$ に上げて分解したとき,

$$\mathfrak{p}\mathfrak{O}_K = \prod_{j=1}^{g} \mathfrak{P}_j{}^{e_j}$$

と分解されたとすると, $\mathfrak{O}_{K,\mathfrak{p}}$ の素イデアルは $1 \leq i \leq g$ に対し $\mathfrak{P}_i' = \mathfrak{P}_i \mathfrak{O}_{K,\mathfrak{p}}$ である.
今, K/F の共役差積 $D_{K/F}$ の素イデアル分解を,

$$D_{K/F} = \prod_{\mathfrak{P}} \mathfrak{P}^{d(\mathfrak{P})}$$

とすると, 命題 3.8 により,

$$D_{K/F} \mathfrak{O}_{K,\mathfrak{p}} = \prod_{i=1}^{g} \mathfrak{P}_i'{}^{d(\mathfrak{P}_i)}$$

というように分解される. したがって, 次のことがいえる :

命題 3.12 相対拡大 K/F に対し, $\mathfrak{O}_F$ の素イデアル $\mathfrak{p}$ をとり, $\mathfrak{P}$ を $\mathfrak{O}_K$ の素イデアルで $\mathfrak{P} \mid \mathfrak{p}$ となるものとする.

このとき, K/F の共役差積 $D_{K/F}$ の $\mathfrak{P}$ 指数と $(\mathfrak{O}_{K,\mathfrak{p}}^*)^{-1}$ の $\mathfrak{P}' = \mathfrak{P}\mathfrak{O}_{K,\mathfrak{p}}$ の指数は一致する.

命題 3.12 を使って, ヒルベルトの公式を示していく. その前に, 1 つ補題を用意する.

補題 3.13 ガロア拡大 K/F に対し, $\mathfrak{P}$ を K の整数環 $\mathfrak{O}_K$ の素イデアルとし, T を $\mathfrak{P}$ の惰性体 $T_{\mathfrak{P}}(K/F)$ とする. さらに, $\pi \in \mathfrak{O}_K$ で, $\pi \in \mathfrak{P} \backslash \mathfrak{P}^2$ となるものをとると,

$$\mathfrak{O}_{K,\mathfrak{P}} = \mathfrak{O}_{K,\mathfrak{p}} = \mathfrak{O}_{T,\mathfrak{p}_T} + \mathfrak{O}_{T,\mathfrak{p}_T}\pi + \cdots + \mathfrak{O}_{T,\mathfrak{p}_T}\pi^{e-1}$$

である. ただし, $e = e_{K/F}(\mathfrak{P})$, $\mathfrak{p}_T = \mathfrak{P} \cap \mathfrak{O}_T$ である.

次の定理がヒルベルトの公式である. この証明は整数環そのままだと証明するのが難しいため, この節で定義した少し広げた整数環を導入する.

定理 3.14 (ヒルベルトの公式) K/F をガロア拡大とする. K の整数環 $\mathfrak{O}_K$ の素イデアル $\mathfrak{P}$ に対し, この $\mathfrak{P}$ に関する高次分岐群の降鎖を

$$v_0 \supsetneq v_1 \supsetneq \cdots \supsetneq v_m \supsetneq v_{m+1} = \{1\}$$

とする. このとき, K/F の共役差積 $D_{K/F}$ の $\mathfrak{P}$ 指数 s は,

$$s = \sum_{i=0}^{m} |v_i| - 1$$

となる.

証明. 命題 1.76 (2) と命題 1.86 (3) により, K/T に関してだけ考えればよい.
命題3.12により, $D_{K/T}$ の $\mathfrak{P}$ 指数と $(\mathfrak{O}^*_{K,\mathfrak{p}})^{-1}$ の $\mathfrak{P}' = \mathfrak{P}\mathfrak{O}_{K,\mathfrak{P}}$ の指数は一致するから, $(\mathfrak{O}^*_{K,\mathfrak{p}})^{-1}$=$D_{K/T}\mathfrak{O}_{K,\mathfrak{P}}$ の $\mathfrak{P}'$ 指数が

$$\sum_{i=0}^{m} |v_i| - 1$$

と等しくなることを示していく. 簡単のために, $v_{\mathfrak{P}}(I)$ を I の $\mathfrak{P}$ 指数とかくことにする.
補題 3.13 から, $\pi \in \mathfrak{P}\backslash\mathfrak{P}^2$ となるものをとると,

$$\mathfrak{O}_{K,\mathfrak{P}} = \mathfrak{O}_{K,\mathfrak{p}} = \mathfrak{O}_{T,\mathfrak{p}_T} + \mathfrak{O}_{T,\mathfrak{p}_T}\pi + \cdots + \mathfrak{O}_{T,\mathfrak{p}_T}\pi^{e-1} \text{ である.}$$

とかくことができる. ただし, $e = e_{K/F}(\mathfrak{P})$, $\mathfrak{p}_T = \mathfrak{P} \cap \mathfrak{O}_T$ である. 命題 1.73 から, $f(X)$ を π の T 上の最小多項式とすると

$$\mathfrak{O}^*_{K,\mathfrak{p}} = \frac{\mathfrak{O}_{K,\mathfrak{P}}}{f'(\pi)}$$

となるから,

$$(\mathfrak{O}^*_{K,\mathfrak{p}})^{-1} = D_{K/F}\mathfrak{O}_{K,\mathfrak{P}} = f'(\pi)\mathfrak{O}_{K,\mathfrak{P}}.$$

よって, 命題 3.12 より,

$$v_{\mathfrak{P}}(D_{K/T}) = v_{\mathfrak{P}'}(D_{K/T}\mathfrak{O}_{K,\mathfrak{P}}) = v_{\mathfrak{P}'}(f'(\pi)\mathfrak{O}_{K,\mathfrak{P}}) = v_{\mathfrak{P}}(f'(\pi))$$

となるから, $v_{\mathfrak{P}}(f'(\pi))$ についてみていく.

$$f'(\pi) = \prod_{\tau \in v_0\backslash\{1\}} (\pi - \pi^\tau)$$

とかける. これをさらに細かく分けていくと,

$$f'(\pi) = \prod_{\tau \in v_0\backslash v_1} (\pi - \pi^\tau) \prod_{\tau \in v_1\backslash v_2} (\pi - \pi^\tau) \cdots \prod_{\tau \in v_m\backslash v_{m+1}} (\pi - \pi^\tau)$$

となる.

ここで, 命題 1.92 より, $\tau \in v_n \backslash v_{n+1} \iff v_{\mathfrak{P}}(\pi - \pi^\tau) = n+1$ であるから,

$$\begin{aligned} v_{\mathfrak{P}}\left(\prod_{\tau \in v_0 \backslash v_1} (\pi - \pi^\tau)\right) &= |v_0| - |v_1|, \\ v_{\mathfrak{P}}\left(\prod_{\tau \in v_1 \backslash v_2} (\pi - \pi^\tau)\right) &= 2(|v_1| - |v_2|), \\ &\vdots \\ v_{\mathfrak{P}}\left(\prod_{\tau \in v_m \backslash v_{m+1}} (\pi - \pi^\tau)\right) &= (m+1)(|v_m| - |v_{m+1}|) \end{aligned}$$

と計算できるので, 結局, $v_{m+1} = \{1\}$ に注意すると

$$v_{\mathfrak{P}}(f'(\pi)) = (|v_0| - |v_1|) + 2(|v_1| - |v_2|) + \cdots + (m+1)(|v_m| - |v_{m+1}|) = \sum_{i=0}^{m} |v_i| - 1$$

となる. □

ヒルベルトの公式を示せたので, 次では本格的に命題 3.6 を示していく.

3.2.2 拡大次数と判別式がともに奇素数べきのときについて

この節ではまず, 命題 3.6 を示す. この命題を示せれば拡大次数と判別式がとも奇素数べきのときに定理 3.1 が成り立つことも示すことができる.

そのために, 2 つ補題を用意する.

補題 3.15 p を奇素数とする. 代数体の拡大 $F/\mathbb{Q}$ を判別式 Δ_F が p べきである p 次巡回拡大と仮定し, $\mathrm{Gal}(F/\mathbb{Q}) = \langle\sigma\rangle$ とする. また, F の整数環 $\mathfrak{O}_F$ の素イデアル $\mathfrak{P}$ は $\mathfrak{P} \mid p$ を満たすとする.

このとき, $\pi \in \mathfrak{P} \backslash \mathfrak{P}^2$ となる元をとると, $\pi^\sigma - \pi$ を割る $\mathfrak{P}$ の指数は 2 である.

証明. $\pi^\sigma - \pi$ を割る $\mathfrak{P}$ の指数を簡単のために v_σ とおく.
定理 1.80, 命題 1.86 (3), 命題 1.91 (3) より, $\mathrm{Gal}(F/\mathbb{Q}) = I_{\mathfrak{P}}(F/\mathbb{Q}) = v_1$ である. よって命題 1.92 より, $v_\sigma \geq 2$ であるから, $v_\sigma \leq 2$ を示していく.

命題 1.86 (5) より, $F = \mathbb{Q}(\pi)$ とかける. $f(X)$ を π の $\mathbb{Q}$ 上の最小多項式とすると, $F/\mathbb{Q}$ が p 次巡回拡大より,

$$f(X) = X^p + a_1 X^{p-1} + \cdots + a_p = \prod_{i=0}^{p-1} (X - \pi^{\sigma^i})$$

とかける. $f(X) \in \mathbb{Z}[X]$ であり, 惰性群は分解群の部分群より $\pi^{\sigma^i} \in \mathfrak{P}^{\sigma^i} = \mathfrak{P}$ であるから, $a_i \in \mathfrak{P} \cap \mathbb{Z} = (p)$ である.

ここで,

$$f'(X) = \prod_{i=1}^{p-1} (\pi - \pi^{\sigma^i})$$

を考える. $a \in \mathbb{Z}$ に対し, $\pi^\sigma - \pi \in \mathfrak{P}^a$ より任意の j に対し, $\pi^{\sigma^{j+1}} - \pi^{\sigma^j} \in \mathfrak{P}^a$ であるから, $\pi^{\sigma^j} - \pi \in \mathfrak{P}^a$ となる.

$1 \leq j \leq p-1$ に対し σ^j も $\mathrm{Gal}(F/\mathbb{Q})$ の生成元であるから逆も成り立つので, 任意の j に対し $v_\sigma = v_{\sigma^j}$ であるから $\mathfrak{P}^{v_\sigma(p-1)} \parallel$ [5] $f'(\pi)$ となる.

一方,

$$f'(\pi) = p\pi^{p-1} + (p-1)a_1\pi^{p-2} + \cdots + a_{p-1}$$

とかけ, 任意の i に対し $\mathfrak{P}^p \mid a_i$ より各項の $\mathfrak{P}$ 指数は $\bmod p$ でそれぞれ, $p-1, p-2, \cdots, 0$ に等しいため, それぞれ異なっていることになる. したがって, $f'(\pi)$ の $\mathfrak{P}$ 指数はこの中の最小値に等しい. 特に第 1 項目を考えると, $p + (p-1) \geq v_\sigma(p-1)$ より $2p-1 \geq v_\sigma(p-1)$ を得る. もし $v_\sigma > 2$ ならば,

$$p \leq \frac{v_\sigma - 1}{v_\sigma - 2} = 1 + \frac{1}{v_\sigma - 2} \leq 2$$

となり, p が奇素数であることに矛盾するから $v_\sigma \leq 2$ となるので, $v_\sigma = 2$ になる. □

この補題を用いて, 次の補題を示す :

補題 3.16 p を奇素数とする. 代数体の拡大 $F/\mathbb{Q}$ が p^2 次アーベル拡大かつ F の判別式 Δ_F が p べきならば, 巡回拡大である.

証明. 仮定より, p は F で完全分解することがわかる. $G = \mathrm{Gal}(F/\mathbb{Q})$ が巡回拡大でないと仮定すると, $G \simeq C_p \times C_p$ であるから, 任意の $\sigma \in \mathrm{Gal}(F/\mathbb{Q})\backslash\{\mathrm{id}\}$ に対して,

$$H = \langle\sigma\rangle \text{ かつ } |G : H| = p$$

となる G の部分群 H をとることができる. $K = F^H$ とおく. $\mathfrak{P}$ を $\mathfrak{O}_F$ の素イデアルで $\mathfrak{P} \mid p$ を満たすとする.

ここで, $\pi \in \mathfrak{O}_F$ を $\pi \in \mathfrak{P}\backslash\mathfrak{P}^2$ となるような元をとる. $\pi - \pi^\sigma$ の $\mathfrak{P}$ 指数を v_σ とおくと, 定理 3.14 により,

$$D_{F/K} = \mathfrak{P}^{v_\sigma(p-1)}$$

とかける. また $K/\mathbb{Q}$ については, 定理 3.14 と補題 3.15 により,

$$D_{K/\mathbb{Q}} = \mathfrak{P}^{2p(p-1)}$$

とかける. したがって命題 1.76 (2) より,

$$D_{F/\mathbb{Q}} = D_{F/K}D_{K/\mathbb{Q}} = \mathfrak{P}^{(v_\sigma - 2p)(p-1)}$$

となるが, これは一定のイデアルとなるので v_σ は一定の値 n をとることになる.

しかし, 命題 1.92 により, $v_{n-1} = G, v_n = \{1\}$ となるが, 命題 1.91 (4) と p は F で完全分解することから,

$$p^2 = |v_{n-1}/v_n| \leq N^F(\mathfrak{P}) = p$$

に矛盾するから, $F/\mathbb{Q}$ は巡回拡大である. □

[5] $b \parallel a$ とは, b が a をきっちり割ることである, つまり, a の b 指数を v とすると, $b^v \mid a$ だが, $b^{v+1} \nmid a$ となることである.

後はこの議論を拡大次数が $p^3, p^4, \cdots$ と繰り返していけば, 次の命題 3.6 が示せたことになる.

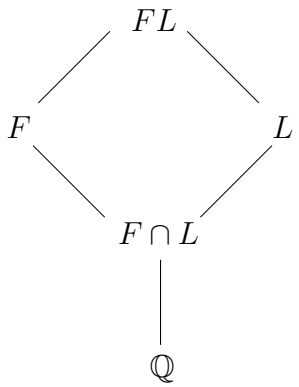
話を戻してクロネッカー · ウェーバーの定理の証明に戻る. 命題 3.3 を完全に示していくために, 次の補題を示す :

命題 3.17 (Step 2-3) 拡大次数 $|F : \mathbb{Q}|$ と判別式 Δ_F がともに奇素数べきであるアーベル体 F は円分体に含まれる.

証明. p を奇素数とする. $|F : \mathbb{Q}| = p^m, K = \mathbb{Q}(\zeta_{p^{m+1}})$ とおく.

$$\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/p^{m+1}\mathbb{Z})^\times \simeq C_{p^m(p-1)}$$

であるから, $|H| = p - 1$ となる $\mathrm{Gal}(K/\mathbb{Q})$ の部分群 H がとれるので, $L = K^H$ とおくと, 以下のハッセ図より $|FL : \mathbb{Q}|, \Delta_{FL}$ はともに p べきになる.



命題 3.6 により, $\mathrm{Gal}(FL/\mathbb{Q})$ は巡回群になる. $|L : \mathbb{Q}| = |F : \mathbb{Q}| = p^m$ であるから, 定理 1.60 (2) により $F = L$ を得るので, $F = L \subset K$ となる. □

この命題により命題 3.3 が完全に証明でき, Step 2 が完了した. 次節から Step 3 に入っていく.

3.3 クロネッカー · ウェーバーの定理の証明の完結

この節では Step 3 に入っていく. Step 3 が完了すればクロネッカー · ウェーバーの定理を完全に証明できたことになる. そのためには, 次の補題が必要になる :

補題 3.18 $F/\mathbb{Q}$ を n 次アーベル拡大とする. $p \mid \Delta_F$ かつ $p \nmid n$ となる任意の素数 p に対して, 以下の (1) から (4) を満たす $\mathbb{Q}$ 上アーベル拡大 K が存在する :
(1) $|K : \mathbb{Q}| \mid n$;
(2) $F \subseteq K(\zeta_p)$;
(3) $p \nmid \Delta_K$;
(4) $\Delta_K \mid \Delta_F$.

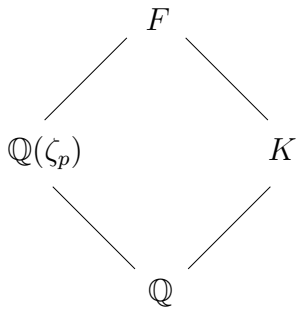
証明. この命題の証明は F を 2 つの場合にわけて考えていく. $\mathfrak{p}$ を p を割る $\mathfrak{O}_F$ の素イデアルとする.

(i) $\zeta_p \in F$ のとき, まず, この場合に起こることを確認する.
命題 1.91 (5) より $|F : V_{\mathfrak{p}}^{(1)}(F/\mathbb{Q})|$ は p べきになるが, $|F : V_p^{(1)}(F/\mathbb{Q})| \mid n$ であることと $p \nmid n$ より, $F = V_{\mathfrak{p}}^{(1)}(F/\mathbb{Q})$ となる. つまり, $v_1 = \{1\}$ である.
命題 1.91 (6) より, $e_{F/\mathbb{Q}}(\mathfrak{p}) = |I_{\mathfrak{p}}(F/\mathbb{Q})| \mid (p-1)$ であるが命題 1.67 より, $\mathfrak{p}' = \mathfrak{p} \cap \mathfrak{O}_{\mathbb{Q}(\zeta_p)}$ とおくと,

$$e_{F/\mathbb{Q}}(\mathfrak{p}) = e_{F/\mathbb{Q}(\zeta_p)}(\mathfrak{p}) e_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\mathfrak{p}')$$

であり, $e_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\mathfrak{p}') = p-1$ であるから, $e_{F/\mathbb{Q}(\zeta_p)}(\mathfrak{p}) = 1$ となる. これに注意して $K = T_{\mathfrak{p}}(F/\mathbb{Q})$ が (1) から (4) の条件を満たすことを示していく.

この場合のハッセ図は以下のようである.

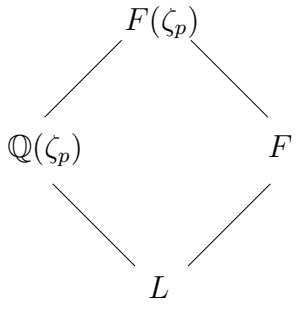


K は F の部分体より, $K/\mathbb{Q}$ はアーベル拡大で $|K : \mathbb{Q}| \mid n$, $\Delta_K \mid \Delta_F$ である. また,

$$I_{\mathfrak{p}}(F/\mathbb{Q}(\zeta_p)) = I_{\mathfrak{p}}(F/\mathbb{Q}) \cap \mathrm{Gal}(F/\mathbb{Q}(\zeta_p))$$

であるから, この群による不変体は $K(\zeta_p)$ であり, $e_{F/\mathbb{Q}(\zeta_p)}(\mathfrak{p}) = 1$ より $F = K(\zeta_p)$ である.
さらに, 命題 1.86 (3) より $p \nmid \Delta_K$ である.

(ii) $\zeta_p \notin F$ のとき, まず $F(\zeta_p)$ に対し $p \mid \Delta_{F(\zeta_p)}, p \nmid |F(\zeta_p) : \mathbb{Q}|$ を満たすことを示す.
$F(\zeta_p)$ は F の拡大体であるから定理 1.43 (1) より, $p \mid \Delta_F$ より $p \mid \Delta_{F(\zeta_p)}$ である.
$L = F \cap \mathbb{Q}(\zeta_p)$ とし, ハッセ図をかくと以下のようになる.



$F(\zeta_p) = F \cdot \mathbb{Q}(\zeta_p)$ であるから, 定理 1.62 (2) より,

$$|F(\zeta_p) : \mathbb{Q}| = |F(\zeta_p) : L| \cdot |L : \mathbb{Q}| = |F : L| \cdot |\mathbb{Q}(\zeta_p) : L| \cdot |L : \mathbb{Q}|$$

となるので,

$$\begin{cases} |F(\zeta_p):\mathbb{Q}| = |F:L|\cdot(p-1), \\ |F(\zeta_p):\mathbb{Q}| = |\mathbb{Q}(\zeta_p):L|\cdot n \end{cases}$$

となる. よって,

$$|F(\zeta_p):\mathbb{Q}|^2 = |F:L|\cdot(p-1)\cdot|\mathbb{Q}(\zeta_p):L|\cdot n$$

を得る. 定理 1.62 (1) より,

$$|F(\zeta_p):F| = |\mathbb{Q}(\zeta_p):L|$$

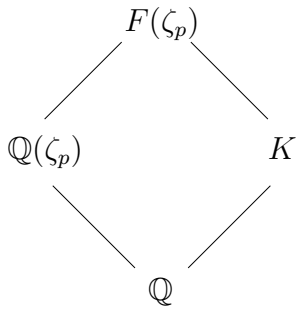
であるから,

$$|F(\zeta_p):\mathbb{Q}| \,\Big|\, (p-1)\cdot n$$

となる. $p \nmid n$ より, $|F(\zeta_p):\mathbb{Q}| \nmid n$ である.

このことから, (i) の結果を適用できる. $K = T_{\mathfrak{p}}(F(\zeta_p)/\mathbb{Q})$ とする. このとき F の部分体ではないことに注意する.

ハッセ図をかくと以下のようになる. 定理 1.43 (1), (3) と命題 1.86 (3) より, $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$ である.



まず, $F \subset F(\zeta_p) = K(\zeta_p)$ である. $|F(\zeta_p):\mathbb{Q}| \neq n$ であるから, 拡大次数については少し議論が必要になる. 定理 1.62 (1) より,

$$|F(\zeta_p):K| = |\mathbb{Q}(\zeta_p):\mathbb{Q}| = p-1$$

であるから,

$$|F(\zeta_p):\mathbb{Q}| = |F(\zeta_p):K|\cdot|K:\mathbb{Q}| = (p-1)\cdot|K:\mathbb{Q}|.$$

よって, $|K:\mathbb{Q}| \,\Big|\, n$ であり, K の定義より, 命題 1.86 (3) から $p \nmid \Delta_K$ である.

最後に $q \neq p$ となる素数 q に対し, 定理 1.80 により, $q \mid \Delta_K$ より, q は K で分岐するが, $K = F\cdot\mathbb{Q}(\zeta_p)$ であるから, q は F で分岐するしかないので $q \mid \Delta_F$ である.

□

この命題は文章だけでは何もわからないが, 実は F の判別式 Δ_F を p べきにするために, Δ_F とは等しくはないが, 割るような数を判別式としてもつ代数体 K をとれるというものである. さらにこの代数体 K の判別式 Δ_K が p べきでない場合はもう一度同じことを行う.

この議論を繰り返し行えば最終的に判別式が p べきの代数体が取れることになる. よって, 次の命題が示される :

命題 3.19 (Step 3) アーベル体の拡大次数と判別式がともに奇素数べきのときに定理 3.1 が成り立てば, 拡大次数が素数べきかつ一般の判別式で定理 3.1 が成り立つ.

以上, Step 1, Step 2, Step 3 により, クロネッカー · ウェーバーの定理が完全に証明されたことになる. 第 4 章ではこの定理と第 3 章で説明した 2 次体の整数論を展開してその中で自分が考えたことを述べていく. その前に, 簡単な例を述べておく.

例 3.20 p を奇素数とする. $F = \mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}}p})$ のとき, $F \subset \mathbb{Q}(\zeta_p)$ である.

このことについては, ガウス和と呼ばれる概念や, 例 1.44 で挙げた, 特に p 分体 $\mathbb{Q}(\zeta_p)$ の判別式が平方数でないことから示すことができる.

このことを使って, すべての 2 次体がどのような円分体に含まれるのか具体的に計算することができる. 例えば, $F = \mathbb{Q}(\sqrt{-5})$ に対しては, 上の式からでは求めることができないが,

$$F \subset \mathbb{Q}(\sqrt{5}, \sqrt{-1}) \subset \mathbb{Q}(\zeta_{20}, \zeta_4) = \mathbb{Q}(\zeta_{20})$$

と計算できる.

第4章　考察と具体例

この章では, 第2章, 第3章を踏まえて, 著者が考察したことを紹介する. 2次形式が表現する奇素数と2次体との対応についての問題である. この問題は類体論により証明が完了しているが, それの具体例を述べている. 第1節では, 類数が1の虚2次体では2次形式はどのような素数を表現し, さらに虚2次体の上ではそのような働きを行うのかをまとめた. 第2節では, 類数2の虚2次体について, 第1節と同じ問題について考察した. この場合は, 簡約形式が2つあるが, 特に, 基本形式が表現する素数について考え, ヒルベルト類体との対応について考えた.

この章で, 重要になるものが次の定理である：

定理 4.1 2次体 $F=\mathbb{Q}(\sqrt{D})$ と奇素数 p に対し,

$$p\mathfrak{O}_F=\begin{cases}\mathfrak{p}_1\mathfrak{p}_2 & (\left(\frac{D}{p}\right)=1 \text{ のとき}),\\ \mathfrak{p}^2 & (\left(\frac{D}{p}\right)=0 \text{ のとき}),\\ \mathfrak{p} & (\left(\frac{D}{p}\right)=-1 \text{ のとき}).\end{cases}$$

この定理と2次体の判別式の表し方から次がわかる：

系 4.2 2次体 F と素数 p において, 以下は同値である：
(1) p は F で完全分解；
(2) $(\frac{\Delta_F}{p})=1$.

この系により, 2次体において完全分解する素数はルジャンドル記号を計算すればよいということがわかる. 例えば, $\mathbb{Q}(\sqrt{-1})$ で完全分解する素数は定理1.2 (4) より, $p\equiv 1 \pmod 4$ である. もう1つ少し複雑になるが別の例を挙げておく.

例 4.3 $F=\mathbb{Q}(\sqrt{-5})$ で完全分解する素数を求める. $\Delta_F=-20$ であるから系4.2により,

$$\left(\frac{-20}{p}\right)=1$$

となる素数 p を求めればよい. $(\frac{-20}{p})=(\frac{-1}{p})(\frac{5}{p})$ であるから,

$$\left(\frac{-1}{p}\right)=\left(\frac{5}{p}\right)=1,$$

または

$$\left(\frac{-1}{p}\right)=\left(\frac{5}{p}\right)=-1$$

となる.

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & (p \equiv 1 \pmod 4), \\ -1 & (p \equiv 3 \pmod 4), \end{cases}$$

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & (p \equiv 1, 4 \pmod 5), \\ -1 & (p \equiv 2, 3 \pmod 5) \end{cases}$$

となるから, 連立合同式により F で完全分解する素数は $p \equiv 1, 3, 7, 9 \pmod{20}$ である.

4.1 類数 1 の虚 2 次体に対応する 2 次形式が表現する素数について

ここで, 次の問題を提起する :

2 元 2 次形式で表現される奇素数はどのような奇素数か. また, その奇素数はどのような意味があるのか.

この問題に対し, 特に次の問題が有名である :

定理 4.4 整数の 2 つの平方和で表現される奇素数は 4 で割って 1 余る素数で, 逆も成り立つ.

証明については $\mathbb{Q}(\sqrt{-1})$ の整数環 $\mathbb{Z}[\sqrt{-1}]$ が PID であることを使って証明していく. 環論を用いてイデアルによる証明や素元と既約元による証明で示される. 実際, 前章までで見たように $\mathbb{Q}(\sqrt{-1})$ の類数は 1 である. ここで注目してほしいことは, それのイデアル類群に対応する簡約形式である. この場合は $x^2 + y^2$ だけである. 素数 p が簡約形式で表現できるとき, そのようなことが起きているのだろうか.

この節では 2 次形式で表現される素数の性質について述べていく.

命題 4.5 $D \equiv 0, 1 \pmod 4$, $n \in \mathbb{Z}$ を D と互いに素とする.
(1) n が判別式 D の原始形式で原始的に表現されるならば, D は $\bmod |n|$ で平方剰余である.
(2) n が偶数かつ D が $\bmod |n|$ で平方剰余または, n が奇数かつ D が $\bmod 4|n|$ で平方剰余ならば, n は判別式 D の原始形式で原始的に表現される.

この命題により, 次の系が示される :

系 4.6 $n \in \mathbb{Z}$, 奇素数 p に対し, 以下は同値である :
(1) p が判別式 $-4n$ の原始形式で表現される ;
(2) $(\frac{-n}{p}) = 1$.

ここで, $(\frac{-n}{p}) = (\frac{-4n}{p})$ であることと, 2 次形式はある簡約形式に同値であることに注意すると, 特定の 2 次体で完全分解する奇素数は 2 次形式で次にように特徴づけできる.

定理 4.7 $4 \mid \Delta_F$ となる 2 次体 F と, 奇素数 p に対して, 以下は同値である :
(1) p が F で完全分解する ;
(2) p は判別式 Δ_F の簡約形式で原始的に表現される.

ここで重要になってくるものは類数が 1 であることである. 類数が 1 であれば, 簡約形式の個数は 1 個しかないので, 完全分解する素数が決まればそれにより表現される簡約形式は簡単に求まってしまう. 他にも判別式が 4 で割れるときの虚 2 次体で類数が 1 の判別式は次のようになる. 証明については 2 次形式を使って簡単に証明できる.

定理 4.8 $4 \mid \Delta_F$ となる虚 2 次体 F に対し, $h_F = 1 \Longleftrightarrow F = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2})$.

また, 類数 1 の虚 2 次体は次のものしかないことが知られている :

定理 4.9 (H. M. Stark, 1964) 虚 2 次体 F に対し,
$h_F = 1 \Longleftrightarrow F = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-11}), \mathbb{Q}(\sqrt{-19}), \mathbb{Q}(\sqrt{-43}), \mathbb{Q}(\sqrt{-67}), \mathbb{Q}(\sqrt{-163})$.

判別式が 4 で割って 1 余るときの証明については現在考察中である.

では, 虚 2 次体の類数が 2 以上の場合はどのようになるのであろうか. この場合は簡約形式の個数が 2 以上になり, どの簡約形式がどの素数を表現するのか簡単に判別できない. 例えば, 例 4.3 で挙げた $F = \mathbb{Q}(\sqrt{-5})$ のときを考えると, 完全分解する素数は $p \equiv 1, 3, 7, 9 \pmod{20}$ であることを示している. また, $\Delta_F = -20$ であるから, 判別式が -20 の簡約形式は $x^2 + 5y^2, 2x^2 + 2xy + 3y^2$ であることがわかっているが, この 2 次形式がどの素数を表現するかという問題は判別式が -4 のときよりも難しい. 次節では, 特に類数が 2 である判別式に関する考察を行っていく.

4.2 類数 2 の虚 2 次体に対応する基本形式が表現する素数について

私が, クンマーによるフェルマーの最終定理[6] の証明を勉強している中で, 次の定理が鍵になった :

定理 4.10 [アルティンの相互法則] 代数体 F に対し, K を F のヒルベルト類体とすると

$$\mathrm{Gal}(K/F) \simeq Cl_F$$

が成り立つ.

注意 4.11 アルティンの相互法則は, より一般のイデアル類群において証明されている. 定理 4.10 の主張はその中でも最も簡単なものである. (詳しくは, [13], [14], [17] を参照)

この定理の証明は, 第 1 章で定義したアルティン写像を使って証明するが, 現在学んでいる. ヒルベルト類体とは, 代数体 F を基礎体としたとき, 最大不分岐アーベル拡大となる F の拡大体のことであると特徴づけできる. 簡単な例を挙げておく.

例 4.12 (1) $\mathbb{Q}(\sqrt{-1})$ のヒルベルト類体は自分自身である.
(2) $\mathbb{Q}(\sqrt{-5})$ のヒルベルト類体は $\mathbb{Q}(\sqrt{-5}, \sqrt{-1})$ である.
(3) $\mathbb{Q}(\sqrt{-6})$ のヒルベルト類体は $\mathbb{Q}(\sqrt{-6}, \sqrt{2})$ である.

[6] $p \nmid h_{\mathbb{Q}(\zeta_p)}$ となる奇素数 p に対して, $x^p + y^p = z^p$ となる自明でない $x, y, z \in \mathbb{Z}$ は存在しないことを証明した. この証明に対しては, クンマー拡大や円分体の理論などを使う.

実際不分岐拡大となっているかについては, 命題 1.79, 定理 1.80 を使って確かめることができる. 例えば, (2) については, $K=\mathbb{Q}(\sqrt{-5},\sqrt{-1}), F=\mathbb{Q}(\sqrt{-5})$ とおくと, $\Delta_K=400, \Delta_F=-20$ であるから, (Δ_K については, 行列のクロネッカー積を用いれば求められる.) 命題 1.79 より,

$$\begin{aligned}\Delta_{K/\mathbb{Q}} &= \Delta_{F/\mathbb{Q}}^{|K:F|} N^{F/\mathbb{Q}}(\Delta_{K/F}),\\ 400 &= 20^2 N^{F/\mathbb{Q}}(\Delta_{K/F}),\\ \Delta_{K/F} &= \mathfrak{O}_F\end{aligned}$$

となる. したがって定理 1.80 より, K で分岐する $\mathfrak{O}_F$ の素イデアルは存在しないことになるので, K/F は不分岐拡大である. 同じようにして (3) も不分岐拡大であることが確かめることができる. さらに, ヒルベルト類体は類体論を使えば, 次の性質が成り立つことがわかる :

命題 4.13 代数体 F に対し, K を F のヒルベルト類体とすると, 以下は同値である :
(1) F の整数環 $\mathfrak{O}_F$ の素イデアル $\mathfrak{p}$ が K で完全分解 ;
(2) $\mathfrak{p}$ は単項イデアルである.

では, 例 4.12 (2) のとき, ガロア理論を用いてヒルベルト類体について見ていく. $K=\mathbb{Q}(\sqrt{-5},\sqrt{-1}), F=\mathbb{Q}(\sqrt{-5})$ とおく. このとき,

$$\mathrm{Gal}(K/\mathbb{Q}) \simeq V_4 \simeq C_2 \times C_2$$

であるから, アーベル拡大である. V_4 はクラインの四元群と呼ばれる群である. よって, クロネッカー · ウェーバーの定理により, K は円分体に含まれることになる. 実際, $K \subset \mathbb{Q}(\zeta_{20})$ である.

また,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{20})/\mathbb{Q}) \simeq (\mathbb{Z}/20\mathbb{Z})^\times = \{1,3,7,9,11,13,17,19\}$$

であるから, ガロア対応をかくと以下のようになる.

$$\begin{array}{ccc} \mathbb{Q}(\zeta_{20}) & & \{1\} \\ | & & | \\ \mathbb{Q}(\sqrt{-5},\sqrt{-1}) & & \{1,\ 9\} \\ | & & | \\ \mathbb{Q}(\sqrt{-5}) & & \{1,\ 3,\ 7,\ 9\} \\ | & & | \\ \mathbb{Q} & & (\mathbb{Z}/20\mathbb{Z})^\times \end{array}$$

つまり, この $\{1, 9\}$ というものがどのような特徴をもっているのかを見ればよい. まず簡単にわかるものとして, $(\mathbb{Z}/20\mathbb{Z})^\times$ の位数 2 の唯一の部分群となっていることである. 実際, $(\mathbb{Z}/20\mathbb{Z})^\times$ の部分群 $\{1, 3, 7, 9\}$ をみると, $\{1, 3, 7, 9\}$ は F で完全分解する素数を表していて, $\{1,3,7,9\} \simeq C_4$ であるから, この群の自明でない部分群は $\{1, 9\}$ しかないことがわかる. この性質が後で重要になってくる. では, 他の例でも適用できるかというとそうではない. 例えば, 例 4.12 (3) を同じようにガロア対応を考えると,

$$\begin{array}{ccc} \mathbb{Q}(\zeta_{24}) & & \{1\} \\ | & & | \\ \mathbb{Q}(\sqrt{-6},\sqrt{2}) & & \{1,\ 7\} \\ | & & | \\ \mathbb{Q}(\sqrt{-6}) & & \{1,\ 5,\ 7,\ 11\} \\ | & & | \\ \mathbb{Q} & & (\mathbb{Z}/24\mathbb{Z})^{\times} \end{array}$$

となる. しかし $\{1,5,7,11\} \simeq V_4$ であるから, 自明でない部分群としては $\{1,\ 5\}$, $\{1,\ 7\}$, $\{1,\ 11\}$ の 3 つがあるので, 必ず唯一になっているとは限らないことに注意する.

そこで重要になってくるものが, 定理 4.10 のイデアル類群と同型であるということである. 現在は虚 2 次体の場合であるから, 狭義イデアル類群はイデアル類群と同じであるから完全に 2 次形式の形にいい直すことができる. 著者は, このガロア対応と 2 次形式の表現する奇素数は対応すると考えた.

まず, 判別式が -20 の場合をみていく. $p \equiv 1,3,7,9 \pmod{20}$ と仮定する. このとき, 命題 4.5 (2) により, 判別式 -20 の簡約形式により表現される.

判別式 -20 の簡約形式は $x^2+5y^2, 2x^2+2xy+3y^2$ であるから, それぞれの 2 次形式がその素数を表現するのかを決めていく.

$x^2+5y^2=p$ となる $x,y \in \mathbb{Z}$ が存在するならば, $x^2 \equiv p \pmod{5}$ であるから,

$$\left(\frac{p}{5}\right) = 1$$

となる. よって, $p \equiv 1,3,7,9 \pmod{20}$ の中では, $p \equiv 1,9 \pmod{20}$ である.

また, $2x^2+2xy+3y^2=p$ となる $x,y \in \mathbb{Z}$ が存在するならば, $(2x+y)^2 \equiv 2p \pmod{5}$ であるから,

$$\left(\frac{p}{5}\right) = -1$$

となる. よって, $p \equiv 1,3,7,9 \pmod{20}$ の中では, $p \equiv 3,7 \pmod{20}$ である.

また, 同じ方法を判別式 -24 に対しては適用できない. なぜならば, ルジャンドル記号を適用できないからである.

そのために, 2 次形式論の種の定理を用いる. 現在, 学んでいる途中であり, この理論を学ぶことは今後の課題の 1 つである.

命題 4.14 $D \equiv 0,1 \pmod{4}$ とする. D を割らない素数 p に対し,

$$\begin{array}{rccc} \chi\ :\ (\mathbb{Z}/D\mathbb{Z})^{\times} & \longrightarrow & \{\pm 1\} \\ \cup & & \cup \\ \overline{p} & \longmapsto & \left(\dfrac{D}{p}\right) \end{array}$$

さらに, $\chi(1)=1$, $\chi(-1)=-1$ となる準同型写像が一意に存在する.

注意 4.15 この記号はルジャンドル記号を拡張させたヤコビ記号と呼ばれるものである. つまり, ルジャンドル記号では分母の部分が奇素数であったが, それを拡張させ一般の合成数の場合にしたものである.

この写像を使って, 基本形式が表現する素数を求めることができる.

命題 4.16 $D \equiv 0, 1 \pmod 4$, f を判別式 D の 2 次形式とする. このとき, 以下が成り立つ :
(1) D を割らない奇素数 p に対して, $\overline{p} \in \mathrm{Ker}(\chi)$ ならば, p は判別式 D の簡約形式で表現される ;
(2) 基本形式で表現される $(\mathbb{Z}/D\mathbb{Z})^\times$ の値の集合 H は $\mathrm{Ker}(\chi)$ の部分群である ;
(3) 判別式 D の 2 次形式 f より表現される $(\mathbb{Z}/D\mathbb{Z})^\times$ の値は $\mathrm{Ker}(\chi)$ における H の剰余類をなす.

この命題により, 判別式が -20 のときを完全に示せる. 写像 χ を

$$\begin{array}{ccccc} \chi & : & (\mathbb{Z}/20\mathbb{Z})^\times & \longrightarrow & \{\pm 1\} \\ & & \cup & & \cup \\ & & \overline{p} & \longmapsto & \left(\dfrac{-20}{p}\right) \end{array}$$

となる準同型写像とすると,

$$\mathrm{Ker}(\chi) = \{p \mid p \equiv 1, 3, 7, 9 \pmod{20}\}$$

であることがわかる. $\mathrm{Ker}(\chi)$ の部分群は $\{1, 9\}$ のみであるから, 命題 4.16 により, $x^2 + 5y^2$ が表現する奇素数は $p \equiv 1, 9 \pmod{20}$ である. したがって,

$$x^2 + 5y^2 = p \Longleftrightarrow p \equiv 1, 9 \pmod{20}$$

が示された.

判別式 -24 の場合は, χ を

$$\begin{array}{ccccc} \chi & : & (\mathbb{Z}/24\mathbb{Z})^\times & \longrightarrow & \{\pm 1\} \\ & & \cup & & \cup \\ & & \overline{p} & \longmapsto & \left(\dfrac{-24}{p}\right) \end{array}$$

となる準同型写像とすると,

$$\mathrm{Ker}(\chi) = \{p \mid p \equiv 1, 5, 7, 11 \pmod{24}\}$$

であることがわかる.
また, 判別式が -24 の簡約形式は $x^2 + 6y^2, 2x^2 + 3y^2$ の 2 つであり, $x^2 + 6y^2$ が表現する奇素数は, $p \equiv 1, 7 \pmod{24}$ である. 必要十分条件であることを示すために, もう少し考えなければならない. 2 次形式の種を定義する.

定義 4.17 $D \equiv 0, 1 \pmod 4$, $H \subset \mathrm{Ker}(\chi)$ を定理 4.16 の通りとし, H' を $\mathrm{Ker}(\chi)$ における H の剰余類とする.

このとき, mod D で H' を表現する, 判別式 D の 2 次形式全ての集合を H' の種という.

2 次形式の種を定義したとき, 次の定理を証明することができる :

定理 4.18 $D \equiv 0, 1 \pmod 4$ に対し, H と H' を定義 4.17 と同じ集合, p を D を割らない奇素数とする. このとき, 以下は同値である :
(1) p が H' の種にある簡約形式で表現される ;
(2) $\overline{p} \in H'$.

この定理を使えば, 判別式 -24 の場合がわかってくる. 判別式が -24 の簡約形式は $x^2+6y^2, 2x^2+3y^2$ の 2 つであり, x^2+6y^2 が表現する奇素数は, $p \equiv 1, 7 \pmod{24}$ である. $H = \{1, 7\}$ とおくと, これは $\mathrm{Ker}(\chi)$ の部分群である.
一方, $2x^2+3y^2$ が表現する奇素数は $p \equiv 5, 11 \pmod{24}$ であるから, $2x^2+3y^2$ は H の種にはなりえない. 実際, 定理 4.18 により, H の種は x^2+6y^2 と同値な 2 次形式だけであり, $2x^2+3y^2$ とは同値でないからである.

したがって,

$$p \equiv 1, 7 \pmod{24} \Longleftrightarrow p = x^2 + 6y^2$$

となる. つまり, 例 4.12 (3) の場合でも, 基本形式によりヒルベルト類体が構成されることがわかる. このことを他の類数 2 の虚 2 次体に対して行えば, 次のことを考えた :

> 類数 2 の虚 2 次体 F に対し, $\mathbb{Q}$ 上アーベル拡大である F のヒルベルト類体は具体的に構成可能で, 基本形式を使って構成できる.

また, 類数 2 の虚 2 次体は, 次のものしかないことが示されている :

定理 4.19 (A. Baker, H. M. Stark, 1971) 虚 2 次体 F に対し,
$h_F = 2 \Longleftrightarrow F = \mathbb{Q}(\sqrt{-5}), \mathbb{Q}(\sqrt{-6}), \mathbb{Q}(\sqrt{-10}), \mathbb{Q}(\sqrt{-13}), \mathbb{Q}(\sqrt{-15}), \mathbb{Q}(\sqrt{-22}), \mathbb{Q}(\sqrt{-35}), \mathbb{Q}(\sqrt{-37}),$
$\mathbb{Q}(\sqrt{-51}), \mathbb{Q}(\sqrt{-58}), \mathbb{Q}(\sqrt{-91}), \mathbb{Q}(\sqrt{-115}), \mathbb{Q}(\sqrt{-123}), \mathbb{Q}(\sqrt{-187}), \mathbb{Q}(\sqrt{-235}),$
$\mathbb{Q}(\sqrt{-267}), \mathbb{Q}(\sqrt{-403}), \mathbb{Q}(\sqrt{-427}).$

これらすべてのヒルベルト類体を, 次のページで表にしてまとめている.

ここまでで, 類数が 2 の場合を調べてきた. その次に類数が 3 の場合を考えたが, この方法は使えない. なぜなら, $\mathbb{Q}$ 上アーベルでないヒルベルト類体が存在するからである.

例 4.20 $\mathbb{Q}(\sqrt{-23})$ のヒルベルト類体は $\mathbb{Q}(\sqrt{-23}, \alpha)$ である. ただし, α は $X^3 - X + 1 = 0$ の根である. 実際, $\mathrm{Gal}(K/\mathbb{Q}) = S_3$ で S_3 はアーベル群ではない.

つまり, どの円分体にも含まれていないことになるので, 同じような議論をすることができない.

また, 実 2 次体については基本単数を考える必要があるので, 虚 2 次体よりさらに難しくなる.

以下の表は, 類数 2 の虚 2 次体に対するヒルベルト類体である.

虚 2 次体	ヒルベルト類体	ヒルベルト類体の判別式
$\mathbb{Q}(\sqrt{-5})$	$\mathbb{Q}(\sqrt{-1},\sqrt{5})$	400
$\mathbb{Q}(\sqrt{-6})$	$\mathbb{Q}(\sqrt{-3},\sqrt{2})$	576
$\mathbb{Q}(\sqrt{-10})$	$\mathbb{Q}(\sqrt{-2},\sqrt{5})$	1600
$\mathbb{Q}(\sqrt{-13})$	$\mathbb{Q}(\sqrt{-1},\sqrt{13})$	2704
$\mathbb{Q}(\sqrt{-15})$	$\mathbb{Q}(\sqrt{-3},\sqrt{5})$	225
$\mathbb{Q}(\sqrt{-22})$	$\mathbb{Q}(\sqrt{-11},\sqrt{2})$	7744
$\mathbb{Q}(\sqrt{-35})$	$\mathbb{Q}(\sqrt{-7},\sqrt{5})$	1225
$\mathbb{Q}(\sqrt{-37})$	$\mathbb{Q}(\sqrt{-1},\sqrt{37})$	21904
$\mathbb{Q}(\sqrt{-51})$	$\mathbb{Q}(\sqrt{-3},\sqrt{17})$	2601
$\mathbb{Q}(\sqrt{-58})$	$\mathbb{Q}(\sqrt{-2},\sqrt{29})$	53824
$\mathbb{Q}(\sqrt{-91})$	$\mathbb{Q}(\sqrt{-7},\sqrt{13})$	8281
$\mathbb{Q}(\sqrt{-115})$	$\mathbb{Q}(\sqrt{-23},\sqrt{5})$	13225
$\mathbb{Q}(\sqrt{-123})$	$\mathbb{Q}(\sqrt{-3},\sqrt{41})$	15129
$\mathbb{Q}(\sqrt{-187})$	$\mathbb{Q}(\sqrt{-11},\sqrt{17})$	34969
$\mathbb{Q}(\sqrt{-235})$	$\mathbb{Q}(\sqrt{-47},\sqrt{5})$	55225
$\mathbb{Q}(\sqrt{-267})$	$\mathbb{Q}(\sqrt{-3},\sqrt{89})$	71289
$\mathbb{Q}(\sqrt{-403})$	$\mathbb{Q}(\sqrt{-31},\sqrt{13})$	162409
$\mathbb{Q}(\sqrt{-427})$	$\mathbb{Q}(\sqrt{-7},\sqrt{61})$	182329

第5章　今後の研究について

この章では, 著者が今後の研究の対象をいくつか述べていく. 第1節では実2次体と関わりのあるペル方程式について述べている. 第4章で虚2次体について議論したが, 実2次体ではこのペル方程式の議論も必要になる. そのペル方程式が解ける必要十分条件や, 実2次体の類数問題について述べている. 第2節では, 第2章で定義した, 2元2次形式の演算であるディリクレ積を2元3次形式に拡張させる方法について紹介している.

5.1　実2次体の類数とペル方程式について

次にペル方程式について述べる. ペル方程式は実2次体の基本単数を求めることに使われる. $m \in \mathbb{Z}$ を平方数でない整数としたとき, ペル方程式は

$$X^2 - mY^2 = \pm 1, \pm 4$$

という形の方程式である. 解の構造は命題1.40により実2次体 F の単数群の構造と同じであるから, 定理1.54により,

$$\mathfrak{O}_F^{\times} \simeq \mathbb{Z} \times \langle \pm 1 \rangle \simeq \langle u_1 \rangle \times \langle \pm 1 \rangle$$

という構造をもっているので, この u_1 を具体的に求めることが重要になっている.

著者が非常に関心をもっているのは

$$X^2 - mY^2 = -1, -4$$

が整数解をもっているかどうかである. これは, 命題2.52の狭義類数と一般的な類数との差が2倍異なるか, 全く同じかをいうために必要なことである. [KW86] の $X^2 - mY^2 = -1$ が解をもつために必要十分条件を紹介する.

2次無理数 α に対して, $l(\alpha)$ を α を連分数展開したときの循環節の長さを表すことにする.

定理 5.1 以下は同値である：
(1) ペル方程式 $X^2 - mY^2 = -1$ が整数解 (X, Y) をもつ ;
(2) $l(\sqrt{m})$ は奇数である.

著者はペル方程式について詳しく勉強していないため, 現在は証明できていないが, 有用な定理である.

問題になってくるものが $X^2 - mY^2 = -4$ が整数解をもつ必要十分条件である. まだ論文を詳しく読んでいないが, 次のことを論文内でいっている：

定理 5.2 (P. Kaplan and K. S. Williams, [KW86], THEOREM 1) $X^2 - mY^2 = -1$ が整数解 (X, Y) をもつと仮定する. このとき, 以下は同値である :
(1) $X^2 - mY^2 = -4$ が整数解 (X, Y) をもつ ;
(2) $l(\sqrt{m}) \equiv l(\frac{1+\sqrt{m}}{2}) \pmod 4$.

つまり, 条件を付け足すことにより $X^2 - mY^2 = -4$ が整数解をもつ必要十分条件を与えることができている. しかし, 私はこの条件がなくても整数解をもつ条件を特徴づけできると考えているので, 今後頑張っていきたい.

また, 実 2 次体では次の問題が未解決である :

予想 5.3 (ガウスの予想) 実 2 次体 F に対し, 類数 h_F が 1 になる F は無限個存在する.

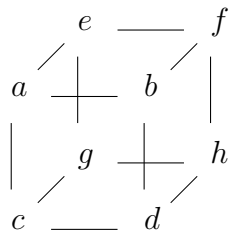
この問題は, ノルムが -1 の単数をもつかもたないかにより, 類数と狭義類数が異なるため, まずはノルムが -1 の単数をもつ実 2 次体の必要十分条件を与えてから解析していきたい.

5.2 高次合成則

この節で紹介する結果は, 2014 年にフィールズ賞を受賞したマンジュル · バルガヴァ氏の結果である. 論文は, [Bha04I], [Bha04II], [Bha04III], [Bha08IV] であり 200 年もの間知られていなかった, 2 次形式の高次合成則を発見した.

本論文では, [Bha04I] の結果の一部を紹介する. まず, [Bha04I] で学んだことを紹介する.

$A = (a, b, c, d, e, f, g, h) \in \mathbb{Z}^8$ に対し, それらからなる立方体 C^A を



とし, この立方体に対する 3 つの行列 [7],

$$M_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad , \quad N_1 = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$
$$M_2 = \begin{pmatrix} a & c \\ e & g \end{pmatrix} \quad , \quad N_2 = \begin{pmatrix} b & d \\ f & h \end{pmatrix}$$
$$M_3 = \begin{pmatrix} a & e \\ b & f \end{pmatrix} \quad , \quad N_3 = \begin{pmatrix} c & g \\ d & h \end{pmatrix}$$

に対して 3 つの 2 次形式を

$$Q_i^A(x, y) = -\det(M_i x - N_i y)$$

と定義する. 簡単のために, $Q_i = Q_i^A$とかく.

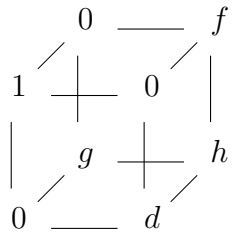
これら 3 つの 2 次形式は, 第 3 章で述べたように $\mathrm{SL}_2(\mathbb{Z})$ で同値関係を導入していたので, この立方体に対しては $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ に対して同値関係 $\sim'$ を導入することができる. この立方体を定義して分かることを述べておく.

定理 5.4 Q_1, Q_2, Q_3 の判別式は全て等しい.

この判別式を立方体の判別式という. さらに, Q_1, Q_2, Q_3 がすべて原始形式になるような立方体を原始立方体という. 2 次形式と同じ理由により, 各係数が互いに素であるときに, 原始立方体の集合を同値関係 $\sim$ で割った集合の構造を見ていく. すると, 次の結果が分かる :

定理 5.5 $A = (a, b, c, d, e, f, g, h) \in \mathbb{Z}^8$ に対し, C^A が判別式 D の原始立方体のとき, $\overline{Q_1} \circ \overline{Q_2} \circ \overline{Q_3}$ は判別式 D の基本形式になる.

定理 5.5 を簡単に見ていく. 判別式 D の原始立方体は,



と同値になることが示される. この立方体に対する 3 つの 2 次形式は,

$$Q_1(x, y) = -dx^2 + hxy - fgy^2, Q_2(x, y) = -gx^2 + hxy - dfy^2, Q_3(x, y) = -fx^2 + hxy + dgy^2$$

である. よって, Q_1 が原始形式より $\gcd(d, h, fg) = 1$ であるから $\gcd(d, h, g) = 1$ であるので, 定義 2.36 より,

$$Q_1 \circ Q_2 = dgx^2 + hxy - fy^2$$

である. 変数変換 $(x, y) \mapsto (y, -x)$ により,

$$Q_1 \circ Q_2 \sim -fx^2 - hxy + dgy^2 = {Q_3}^{-1}$$

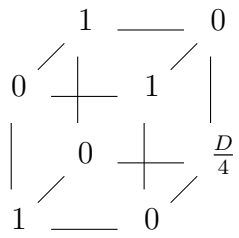
であるから, $Q_1 \circ Q_2 \circ Q_3$ は判別式 D の基本形式になる.

ここから, [Bha04I] の結果を紹介する. 判別式 D の原始立方体の集合を Cb_D とかく.

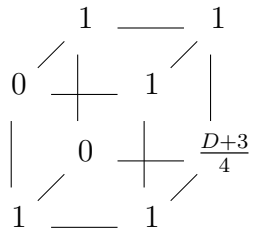
定理 5.6 (バルガヴァ, [Bha04I], THEOREM 1) $D \equiv 0, 1 \pmod 4$ となる整数 D をとる.
$Q_1^{A_0} = Q_2^{A_0} = Q_3^{A_0} = Q_{\mathrm{id},D}$ を満たす立方体 A_0 が存在すると仮定し, その原始形式を $Q_{id,D}$ とおく.
このとき, $C_D/\sim$ に対し, 以下の 2 つを満たすような群の演算が一意に存在する :
(1) $\overline{Q_{\mathrm{id},D}}$ は, 単位元である ;
(2) Q_1^A, Q_2^A, Q_3^A がすべて原始形式となる任意の判別式 D の立方体に対し, $\overline{Q_1^A} \circ \overline{Q_2^A} \circ \overline{Q_3^A} = \overline{Q_{\mathrm{id},D}}$ となる ;
(3) $\overline{Q_1} \circ \overline{Q_2} \circ \overline{Q_3} = \overline{Q_{\mathrm{id},D}}$ となる, Q_1, Q_2, Q_3 に対し, $Q_1^A = Q_1, Q_2^A = Q_2, Q_3^A = Q_3$ となる判別式 D の立方体 A が同値関係 $\sim'$ を除いて一意に存在する.

[7] それぞれ立方体を回転させて正面, 左, 真上から見たときの前後の行列のことである.

この定理において, $Q_{\mathrm{id},D}$ を定義 2.45 で定義した基本形式とする. すると, これは, 定理の条件を満たしている. 実際, $D \equiv 0 \pmod 4$ のとき,



さらに, $D \equiv 1 \pmod 4$ のとき,



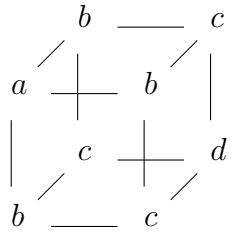
とすれば, この立方体に対応する 3 つの 2 次形式は, すべて判別式 D の基本形式である. この立方体を基本立方体という. このような立方体をとれば, 定義 2.36 の演算が定理 5.6 の条件をすべて満たしていることが示される. この定理は, 2 次形式の演算を立方体の中で考えるということをいっている.

次に, 立方体に対する演算の結果を紹介する.

定理 5.7 (バルガヴァ, [Bha04I], THEOREM 2) $D \equiv 0, 1 \pmod 4$ となる整数 D をとる.
$A_{\mathrm{id},D}$ を判別式 D の基本立方体とする. このとき, $Cb_D/\sim'$ に対し, 以下の 2 つを満たすような群の演算が一意に存在する :
(1) $\overline{A_{\mathrm{id},D}}$ は単位元である ;
(2) $i = 1, 2, 3$ に対し, $\overline{A} \mapsto \overline{Q_i^A}$ という写像は, $C_D/\sim$ への群準同型写像である.

この定理は, 2 次形式の演算により, 立方体の演算を定義できることをいっている.

この主張の後に, 2 元 3 次形式に対する演算を定義できると論文にある. 立方体を,



に対して考えていく. 詳しくは学んでいる途中である.

2 次形式の議論により 2 次体のイデアル類群の位数や構造を見ることができるが, 3 次体のイデアル類群の位数や構造に関しては PARI-GP などのパソコンのソフトを使えば求めることができるが, 実際に計算で求めることは現在できない. 私は, 2 次体と同じように 3 次体のイデアルを 2 元 3 次形式と対応させることにより求めることができると考えている. それから, 3 次体のイデアル類群やヒルベルト類体などを考えていきたい.

参考文献

[1] 藤崎源二郎, 代数的整数論 (上)(下), 裳華房, 2012.

[2] 石田信, 代数的整数論, 森北出版, 1974.

[3] 河田敬義, 数論 (I)(II), 岩波書店, 1978.

[4] 小野孝, 数論序説, 裳華房, 1987.

[5] P. Ribenboim, Algebraic Numbers, Wiley-Interscience, 1972.

[6] R. A. Mollin, Algebraic Number Theory, CRC Press, 2011.

[7] 足立恒雄, ガロア理論講義, 日本評論社, 2010.

[8] 桂利之, 代数学 III 体とガロア理論, 東京大学出版, 2010.

[9] D. A. Buell, Binary Quadratic Forms, Springer, 1989.

[10] D. E. Flath, Introduction to Number Theory, Wiley-Interscience, 1989.

[11] D. A. Cox, Primes of the forms $x^2 + ny^2$, Wiley-Interscience, 1989.

[12] 倉田礼次郎, ガウス 2 次形式論 (2), 河合文化教育研究所, 1988.

[13] 足立恒雄, 三宅克哉, 類体論講義, 日本評論社, 1998.

[14] 高木貞治, 代数的整数論, 岩波書店, 1996.

[15] F. Bouyer, Composition and Bhargava's Cube. `https://www2.warwick.ac.uk/fac/sci/maths/people/staff/bouyer/gauss_composition.pdf`

[16] J. S. Milne, Algebraic Number Theory. `http://www.jmilne.org/math/CourseNotes/ANT.pdf`

[17] J. S. Milne, Class Field Theory. `http://www.jmilne.org/math/CourseNotes/CFT.pdf`

[18] 吉田輝義, GL_n の大域 · 局所 Langlands 対応, `http://www.math.okayama-u.ac.jp/~yoshino/pdffiles/YoshidaTeruyoshi.pdf`

[Bha04I] M. Bhargava, *Higher composition laws I: A new view on Gauss composition, and quadratic generations*, Ann. of Math. (2) **159** (2004), 217–250.

[Bha04II] M. Bhargava, *Higher composition laws II: On cubic analogues of Gauss composition*, Ann. of Math. (2) **159** (2004), 865–886.

[Bha04III] M. Bhargava, *Higher composition laws III: The parametrization of quartic rings*, Ann. of Math. (2) **159** (2004), 1329–1360.

[Bha08IV] M. Bhargava, *Higher composition laws IV: The parametrization of quintic rings*, Ann. of Math. (2) **167** (2008), 53–94.

[KW86] P. Kaplan and K. S. Williams, *Pell's equations* $X^2 - mY^2 = -1, -4$ *and continued fractions*, J. Number Theory **23** (1986), 169–182.