平成14年度　学位論文

２次体の整数環について

兵庫教育大学大学院　学校教育研究科
教科・領域教育専攻　自然系コース
Ｍ０１１８２Ｊ　上　島　和　久

目 次

0章　序

本論文では 2 次体の整数環が一意分解性を持つかどうかについて考察する.

整数全体のなす環 $\mathbb{Z}$ において, 任意の整数 n $(\neq 0, \pm 1)$ は順序を除いて一意的に $n = \pm p_1 \cdots p_r$ と素数 $p_1, ..., p_r$ の積に分解できる. すなわち $\mathbb{Z}$ は一意分解整域をなす. 一方, 平方因子を含まない (素数の平方で割り切れない) 整数 m $(\neq 0, 1)$ と有理数体 $\mathbb{Q}$ に対して

$$\mathbb{Q}(\sqrt{m}) = \mathbb{Q} + \mathbb{Q}\sqrt{m} = \{r + s\sqrt{m} \mid r, s \in \mathbb{Q}\}$$

と表される集合を 2 次体という. 特に $m > 0$ のときは実 2 次体, $m < 0$ のときは虚 2 次体という. 2 次体 $\mathbb{Q}(\sqrt{m})$ にも代数的整数全体のなす整数環 O_m が定まる.

$$\begin{array}{ccc} \mathbb{Q} & \text{———} & \mathbb{Z} \\ \vdots & & \vdots \\ \mathbb{Q}(\sqrt{m}) & \text{———} & O_m \end{array}$$

虚 2 次体 $\mathbb{Q}(\sqrt{-1})$ の整数環 O_{-1} は Gauss の整数環として知られ, 一意分解整域である. 一方, 虚 2 次体 $\mathbb{Q}(\sqrt{-6})$ の整数は $r + s\sqrt{-6}$ $(r, s \in \mathbb{Z})$ と表される. ここで整数 55 は

$$55 = 5 \cdot 11 = (7 + \sqrt{-6})(7 - \sqrt{-6}) = (1 + 3\sqrt{-6})(1 - 3\sqrt{-6})$$

と分解不可能な因子の積として 3 通りに表されることから O_{-6} は一意分解整域ではない. このように 2 次体の整数環は必ずしも一意分解整域でない. 整数環 O_m が一意分解整域である 2 次体 $\mathbb{Q}(\sqrt{m})$ を単純体と呼ぶ. 同様に, 整数環が (ノルムに関して)Euclid 整域である 2 次体を Euclid 体という. Euclid 整域は一意分解整域であることから Euclid 体は単純体である. 2 次体 $\mathbb{Q}(\sqrt{m})$ が Euclid 体となる m は

$$m = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$$

の 21 個であることが 1950 年 Chatland と Davenport によって証明された (cf. [5]).

逆に単純体が Euclid 体であるとは限らない. 1967 年, Stark ([6]) は虚 2 次体 $\mathbb{Q}(\sqrt{m})$ で単純体となる m は次の 9 個に限ることを示した.

$$m = -1,\ -2,\ -3,\ -7,\ -11,\ -19,\ -43,\ -67,\ -163$$

これより $m = -19, -43, -67, -163$ のとき $\mathbb{Q}(\sqrt{m})$ は単純体であるが Euclid 体ではない. また「 実 2 次体 $\mathbb{Q}(\sqrt{m})$ が単純体となる m は無限に存在するであろう」という予想は現在でも未解決である. ちなみに, このような m は $2 \leq m < 100$ の範囲において

$$m = 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, 38, 41,$$

$$43, 46, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97$$

の 38 個であることが知られている.

２次体の整数環は一意分解整域とは限らないが, 0 でないイデアルは一意的に素イデアルの積として分解できる. すなわち 2 次体の整数環は Dedekind 整域である. さらに 0 でないイデアル全体のなす集合にある同値関係が導入され, この同値関係よる同値類全体は有限群をなす. この群をイデアル類群, その位数を類数という. また, 2 次体の整数環について, 一意分解整域であることと類数が 1 であることとが同値となる. これより 2 次体が単純体であるかどうかは類数を求めることにより判定できる.

与えられた 2 次体の類数を求めるためには $\mathbb{Z}$ の素数がどのように素イデアル分解されるかを知る必要が生じる. $\mathbb{Z}$ の素数の素イデアル分解は 3 つの型に分類され, Artin 記号により判定される. 本論文では, これらの結果を利用していくつかの 2 次体についてその類数を決定する.

なお「与えられた自然数 k を類数とする虚 2 次体 $\mathbb{Q}(\sqrt{m})$ は有限個であろう」という Gauss の類数問題は 1976 年の Goldfeld の仕事を経て, 1983 年に Zagier と Gross により証明された. 上に述べた Stark の結果は $k = 1$ のとき, このような m は $-1 \geq m \geq -163$ をみたすことを示している.

以下, 論文の概要を述べる.

１章では後章で必要となる整数論, 群・環・体, ベクトル空間, 整域とイデアルなどについての基本事項を説明する. §1.1 では整数論の基本概念と平方剰余の基本事項について, §1.2 では群・環・体の基本事項について, §1.3 ではベクトル空間の基本事項と体の拡大次数について説明する. §1.4 ではイデアル, 素イデアル, イデアルの積などの用語を定義する. §1.5 では整域における同伴, 既約元, 素元, 単項イデアル整域, 一意分解整域, Euclid 整域などの概念について説明し, 一意分解整域であることと素元分解整域であることとが同値で

あること, 単項イデアル整域が一意分解整域であること, Euclid 整域が単項イデアル整域であることなどを証明する.

2 章では 2 次体の整数環に関する基本的定理について述べる. §2.1 では 2 次体が平方因子をもたない整数 $m \neq 0, 1$ により

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

と与えられること, および $\mathbb{Q}(\sqrt{m})$ に含まれる代数的整数全体 O_m が部分環をなすことを示す. さらに $m \equiv 1 \pmod 4$ の場合と $m \equiv 2, 3 \pmod 4$ の場合に分けて整数環 O_m の $\mathbb{Z}$ 基底を求める. §2.2 では $m \equiv 2, 3 \pmod 4$ かつ O_m が一意分解整域である場合について, 有理素数 p の素元分解が平方剰余 $\left(\frac{m}{p}\right)$ により定まることを示す. これは 4 章で証明する (p) の素イデアル分解法則のひな形とも目される. §2.3 では O_{-2}, O_3 が一意分解整域であることを示し, 有理素数 p の素元分解を例示する.

3 章では Euclid 体について考察する. §3.1 では Euclid 体, 単純体を定義し, 2 次体 $\mathbb{Q}(\sqrt{m})$ が虚 Euclid 体となるのは m が $-1, -2, -3, -7, -11$ の場合に限ることを証明する. §3.2 では $m \equiv 2, 3 \pmod 4$ となる実 Euclid 体 $\mathbb{Q}(\sqrt{m})$ が有限個であることを示し, Chatland と Davenport のリストにあるいくつかの m について $\mathbb{Q}(\sqrt{m})$ が Euclid 体であることを確かめる.

4 章では 2 次体のイデアル論について述べる. 2 次体 $\mathbb{Q}(\sqrt{m})$ の整数環 O_m において 0 でないイデアルが素イデアルの積として一意的に分解できること, 有理素数 p で生成される O_m の単項イデアル (p) の素イデアル分解が Artin 記号により判定できることなどを証明する. §4.1 では O_m の 0 でないイデアルに標準的基底が存在すること, および 0 でないイデアルが階数 2 の自由 $\mathbb{Z}$ 加群であることを示す. §4.2 では標準的基底からイデアルのノルムを求め, 単項イデアルのノルムが生成元のノルムの絶対値に一致することを示す. §4.3 では 0 でないイデアルが素イデアルの積として一意的に分解できること, すなわち O_m が Dedekind 整域であることを示す. また O_m が単項イデアル整域であることと一意分解整域であることとが同値であることを示す. §4.4 では有理素数 p で生成される O_m の単項イデアル (p) の素イデアル分解が 3 つの型に分類できること, Artin 記号により統一的に述べられることなどを示す. また (p) を割る素イデアルの標準的基底が明示されるが, これは 5 章での類数計算に用いられる.

5 章ではイデアル類の全体 CL_m が有限アーベル群をなすことを証明する. また類数 h が 1 であることと O_m が一意分解整域であることとが同値であることを示す. これより整数環 O_m が一意分解整域であるかどうかは類数を計算することにより判定できる. §5.1 ではイデアルの間に対等という同値関係を定義し, このときの同値類としてイデアル類を,

それらの個数として類数を定義する. また Minkowski の定数 κ を定義し, すべてのイデアル類にノルムが κ 以下のイデアルが存在することを示す. これより類数が有限であることが導かれる. さらにイデアル類全体のなす有限アーベル群として, イデアル類群を定義する. §5.2 では §5.1 の結果をふまえて, いくつかの 2 次体についてその類数を決定する.

1 章　準備

この章では後章で必要となる整数論, 群・環・体, ベクトル空間, 整域とイデアルなどについての基本事項を説明する. 一部を除き定理の証明を省略したが, 可能な限り参考文献を明示した.

§1.1 では整数論の基本概念と平方剰余の基本事項について, §1.2 では群・環・体の基本事項について, §1.3 ではベクトル空間の基本事項と体の拡大次数について説明する. §1.4 ではイデアル, 素イデアル, イデアルの積などの用語を定義する. §1.5 では整域における同伴, 既約元, 素元, 単項イデアル整域, 一意分解整域, Euclid 整域などの概念について説明し, 一意分解整域であることと素元分解整域であることとが同値であること, 単項イデアル整域が一意分解整域であること, Euclid 整域が単項イデアル整域であることなどを証明する.

以下, 論文を通して次の記号を用いる.

$\mathbb{N} = \{1, 2, 3, 4, ...\}$　自然数全体

$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, ...\}$　整数全体

$\mathbb{Q} = \left\{ \frac{b}{a} \;\middle|\; a, b \in \mathbb{Z},\ a \neq 0 \right\}$　有理数全体

$\mathbb{R} =$ 実数全体

$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$　複素数全体　(ただし　i　は　$i^2 = -1$　をみたす数　)

なお 2 次体の整数と区別するために $\mathbb{Z}$ の整数, 素数を有理整数, 有理素数と呼ぶ場合があるので注意されたい.

$A \implies B$　　(A ならば B が成り立つこと)

$A \iff B$　　(A と B が同値であること)

1.1　整数論の基本事項

定理 1.1 (除法の定理) 整数 a と自然数 b が与えられたとき $a = bq + r,\ 0 \leq r < b$ を満たす整数 q, r が一意に存在する.

除法の定理で定まる q を a を b で割った商, r を a を b で割った余りという.

$\mathbb{Z}$ の元 a, b, c が $a = bc$ をみたすとき「a は b の倍数である」,「b は a の約数である」,「b は a を割る」,「a は b で割り切れる」などといい $b \mid a$ と表す.

$a \mid b$ かつ $a \mid c$ のとき a を b, c の公約数, $a \mid c$ かつ $b \mid c$ のとき c を a, b の公倍数という.

a, b のいずれか一方が 0 でないとき a, b の公約数の中に最大のものが存在する. それを a, b の最大公約数といい (a, b) と表す. ただし $(0, 0) = 0$ と定める. $(a, b) = 1$ のとき a と b は互いに素であるという.

2 以上の自然数 n で, 約数が ± 1 と $\pm n$ のみであるようなものを素数という. 素数でない 2 以上の自然数を合成数という. 素数 p と整数 n に対して $(p, n) = 1$ か $p \mid n$ のいずれかが成り立つことを注意しておく.

定理 1.2 ([1, 1 章 定理 1.8]) a, b が整数, p が素数のとき次が成り立つ.

$$p \mid ab \quad \Longrightarrow \quad p \mid a \quad \text{または} \quad p \mid b$$

n は自然数とする. 整数 a, b が $n \mid a - b$ をみたすとき $a \equiv b \pmod{n}$ と表し, n を法として a は b に合同であるという. 合同関係 $\equiv$ は $\mathbb{Z}$ 上の同値関係であり, このときの同値類を剰余類または合同類という. また整数 a を含む剰余類を $\overline{a}$ と表す.

定義 1.3 (平方剰余記号) p を奇素数, a を p と互いに素な整数とする. 合同方程式 $x^2 \equiv a \pmod{p}$ が解をもつとき, a は法 p で平方剰余であるといい $\left(\frac{a}{p}\right) = 1$ と表す. 解をもたないとき, 法 p で平方非剰余であるといい $\left(\frac{a}{p}\right) = -1$ と表す. また $p \mid a$ のときは $\left(\frac{a}{p}\right) = 0$ と定める.

上で定めた記号 $\left(\frac{a}{p}\right)$ を 平方剰余記号, または Legendre 記号という. 平方剰余記号について $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ が成り立つ (cf. [1, 1 章 定理 1.30]).

定理 1.4 (Euler の規準, [1, 1 章 定理 1.32]) a が奇素数 p の倍数でないとき次がなり立つ.

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

定理 1.5 (第１補充法則, [1, 1 章 定理 1.33])

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

定理 1.6 (第２補充法則, [1, 1 章 定理 1.33])

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv 1, 7 \pmod 8 \\ -1, & p \equiv 3, 5 \pmod 8 \end{cases}$$

定理 1.7 (平方剰余の相互法則, [1, 1 章 定理 1.33]) p, q が相異なる奇素数のとき次がなり立つ.

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

1.2 群・環・体の基本事項

定義 1.8 (群) 集合 G に 2 項演算 $\cdot$ が定義され, 次の条件をみたすとき G を群という.

(1) 結合律が成り立つ. すなわち任意の $a, b, c \in G$ に対して $(ab)c = a(bc)$ が成り立つ.

(2) ある元 $1 \in G$ が存在して, 任意の $a \in G$ に対して $a1 = 1a = a$ が成り立つ.

(3) 任意の $a \in G$ に対して $ab = ba = 1$ をみたす $b \in G$ が存在する.

上の条件 (2) をみたす 1 は一意に定まる. 1 を G の単位元という. G の元 a に対して条件 (3) をみたす b は一意に定まる. b を a の逆元といい, a^{-1} と表す.

任意の $a, b \in G$ に対して $ab = ba$ が成り立つ群 G をアーベル群または可換群という. G がアーベル群のとき演算を加法 $+$ で表し, 加法群ということがある. 加法群 G の単位元は零元と呼ばれ 0 と表される. また a の逆元は $-a$ と表される.

定義 1.9 (部分群) 群 G の空でない部分集合 H が次の条件をみたすとき G の部分群であるといい $H \leq G$ と表す.

(1) 任意の $a, b \in H$ に対して $ab \in H$ である.

(2) $a \in H$ ならば $a^{-1} \in H$ である.

部分群 H は G の演算に関してそれ自身群となる.

群 G が有限集合であるとき G を有限群という. 有限群 G の元の個数を G の位数という.

群 G の元 a と整数 n にたいして a のべき a^n を次のように定義する.

$$a^n = \begin{cases} \overbrace{aa\cdots a}^{n\text{ 個}} & n > 0 \text{ のとき} \\ 1 & n = 0 \text{ のとき} \\ \underbrace{a^{-1}a^{-1}\cdots a^{-1}}_{-n\text{ 個}} & n < 0 \text{ のとき} \end{cases}$$

群 G の元 a に対して $a^n = 1$ をみたす自然数が存在するとき, そのようなものの中で最小の n を a の位数という. そのような自然数が存在しないとき a の位数は無限であるという.

群 G の元 a に対して a のべき全体の成す集合を $< a >$ と表す.

$$< a >= \{\, a^n \mid n \in \mathbb{Z} \,\}$$

$< a >$ は G の部分群である. $< a >$ が有限群であるとき, 群 $< a >$ の位数と元 a の位数は一致する.

定理 1.10 (Lagrange の定理, [2, 2 章 定理 8.4, 系 8.5]) 位数 g の有限群 G において次が成り立つ.

(1) 部分群 H の位数 h は g の約数である.

(2) G の元 a の位数は g の約数である. 特に $a^g = 1$ が成り立つ.

定義 1.11 (環) 集合 R に加法 $+$ と乗法 $\cdot$ の 2 つの演算が定義され, 次の条件をみたすとき R を環という.

(1) R は加法についてアーベル群をなす.

(2) R の任意の元 a, b, c に対して $(ab)c = a(bc)$ が成り立つ.

(3) R の元 1 で, R の任意の元 a に対して $a1 = 1a = a$ をみたすものが存在する.

(4) R の任意の元 a, b, c に対して $a(b + c) = ab + ac$, $(a + b)c = ac = bc$ が成り立つ.

任意の $a, b \in R$ に対して $ab = ba$ が成り立つとき R を可換環という. 可換環 R の元 a に

対して $ab = ba = 1$ となる $b \in R$ が存在するとき a は可逆であるという. 可逆な元 a を単数, または単元という. R の単数全体の集合は乗法に関して群をなす. この群を R の単数群, または単元群といい $R^\times$ と表す.

定義 1.12 (部分環) 環 R の部分集合 R' が R の単位元を含み, R の加法, 乗法についてそれ自身環をなすとき R' を R の部分環という.

定義 1.13 (体) 可換環 R の 0 以外の元がすべて可逆であるとき R を体という.

自然数 n に対して $\mathbb{Z}$ の法 n による剰余類全体を $\mathbb{Z}/n\mathbb{Z}$ または $\mathbb{Z}/(n)$ と表す.

定理 1.14 (剰余環, [3, 3 章 §3.1]) $\mathbb{Z}/n\mathbb{Z}$ は可換環となる. $\mathbb{Z}/n\mathbb{Z}$ を n を法とする剰余環という.

定義 1.15 (零因子, 整域) 可換環 R の元 a $(\neq 0)$ に対し, 条件 $ab = 0$ をみたす 0 でない元 $b \in R$ が存在するとき a を零因子という. R が零因子を持たないとき, 整域であるという.

定理 1.16 ([3, 3 章 命題 3.4]) 剰余環 $\mathbb{Z}/n\mathbb{Z}$ $(n > 1)$ において次の 2 条件は同値である.

(1) $\mathbb{Z}/n\mathbb{Z}$ は整域である.

(2) n は素数である..

体の 0 でない元はすべて可逆であるから零因子になり得ない. ゆえに次の定理を得る.

定理 1.17 ([3, 3 章 §3.1]) 体は整域である.

多項式環

R を可換環とする. 次の形の式を X を変数とする R 係数多項式という.

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0, \qquad a_i \in R$$

可換環 R の元を係数とし, X を変数とする多項式の全体を $R[X]$ と表す. $R[X]$ は通常の和と積について可換環となる. $R[X]$ を R 上の多項式環という (cf. [3, 3 章 §3.3]).

$R[X]$ の多項式 $f(X)$ が

$$f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0, \quad a_n \neq 0$$

をみたすとき f の次数は n であるといい, $\deg(f) = n$ と表す. ただし $\deg(0) = -\infty$ とする. 次数が 0 以下の多項式は R の元と同一視でき, 定数と呼ばれる. また最高次係数が 1 である多項式はモニック多項式と呼ばれる.

定理 1.18 ([2, 1 章 §6]) R が整域のとき $R[X]$ も整域である.

定理 1.19 (除法の定理, [2, 1 章 定理 6.1]) K を体, $K[X] \ni f, g,\ g \neq 0$ とする. このとき $f = gq + r,\ \deg(r) < \deg(g)$ をみたす $q, r \in K[X]$ が一意に定まる.

q, r をそれぞれ f を g で割った商, 余りという. 余りが 0 のとき f は g で割り切れるといい $g \mid f$ と表す.

多項式 f が定数でない多項式 g, h により $f = gh$ と表されるとき f は可約であるという. 次数が 1 以上で可約でない多項式は既約であるという.

定義 1.20 (原始多項式) $\mathbb{Z}[X] \ni f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ の係数 $a_0, a_1, \ldots, a_n$ の最大公約数が 1 であるとき $f(X)$ を原始多項式という.

定理 1.21 ([2, 3 章 補題 26.9]) $\mathbb{Z}[X] \ni g, h$ が原始多項式のとき, その積 gh も原始多項式である.

多項式 $f(X)$ に対して $f(a) = 0$ をみたす a を f の根という.

定義 1.22 (代数的数と代数的整数) 有理数を係数とする 0 でない多項式の根である複素数を代数的数という. 整数係数モニック多項式の根である複素数を代数的整数という.

定理 1.23 (最小多項式, [4, 7 章 pp.224-225]) α が代数的数であるとき $f(\alpha) = 0$ をみたす 0 でない多項式 $f(X) \in \mathbb{Q}(X)$ のうち最小次数でモニックなものを α の ($\mathbb{Q}$ 上の) 最小多項式という. α の最小多項式は一意的に定まる. α の最小多項式を $p(X)$ とすると次が成り立つ.

(1) $\mathbb{Q}(X) \ni f(X)$ が α を根にもつならば $p(X) \mid f(X)$ が成り立つ.

(2) $p(X)$ は $\mathbb{Q}$ 上既約である.

最小多項式の次数が 1であることと $\alpha \in \mathbb{Q}$ であることとが同値であるのは明らかであろう.

補題 $\mathbb{Z}$ 係数多項式の等式

$$a_n x^n + \cdots + a_1 x + a_0 = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0)$$

において, すべての a_i が素数 p の倍数であれば, すべての b_i が p の倍数であるか, すべての c_i が p の倍数である.

Proof 背理法で示す. ある b_i, c_j が p の倍数でないと仮定し, このような i, j を最小に選ぶ. このとき $b_{i-1}, ..., b_1, b_0$, $c_{j-1}, ..., c_1, c_0$ が p の倍数であるから, 右辺の $i+j$ 次の係数

$$b_{i+j}c_0 + \cdots + b_{i+1}c_{j-1} + b_i c_j + b_{i-1}c_{j+1} + \cdots + b_0 c_{i+j}$$

は $b_i c_j$ 以外の項が p の倍数で $b_i c_j$ が p の倍数でないので, p の倍数でない. これはすべての a_i が素数 p の倍数であることに矛盾する. ∎

次の定理は 2 章 §2.1 で必要になる.

定理 1.24 $\mathbb{Q}$ 係数の多項式の等式

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = (x^r + b_{r-1}x^{r-1} + \cdots + b_0)(x^s + c_{s-1}x^{s-1} + \cdots + c_0)$$

において, すべての a_i が整数であれば, すべての b_i, c_j は実は整数である.

Proof $b_i = \dfrac{\beta_i}{\alpha_i}$, $c_j = \dfrac{\delta_j}{\gamma_j}$ を既約分数表示とし, $\alpha_{r-1}, ..., \alpha_0$ の最小公倍数を ℓ, $\gamma_{s-1}, ..., \gamma_0$ の最小公倍数を m とする. $|\ell m| = 1$ を示せばよいので, $|\ell m| \neq 1$ と仮定して矛盾を導く. 右辺をそれぞれ ℓ, m 倍すると次の等式を得る.

$$\ell m(x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) = (\ell x^r + \lambda_{r-1}x^{r-1} + \cdots + \lambda_0)(m x^s + \mu_{s-1}x^{s-1} + \cdots + \mu_0)$$

ここで λ_i, μ_j は整数である. ℓm の素因数の 1 つを p とすると前の補題よりすべての λ_i と ℓ が p の倍数であるか, すべての μ_i と m が p の倍数であるか, のいずれかが成り立つ. 今, すべての λ_i と ℓ が p の倍数であると仮定する. $\ell = p^t \ell'$ とおく. ただし ℓ' は p と互いに素であるとする. ℓ は $\alpha_{r-1}, ..., \alpha_0$ の最小公倍数であるから, ある α_k は p^t で割り切れる. このとき $\lambda_k = \ell \dfrac{\beta_k}{\alpha_k}$ は p で割りきれないので矛盾が生じる. すべての μ_i と m が p の倍数としても同様に矛盾を得る. ∎

1.3 ベクトル空間

M を加法群, R を可換環とする. $R \times M \ni (a, m)$ に対して M の元 am が定まり, 任意の $a, b \in R$ と任意の $x, y \in M$ に対して次が成り立つとき M を (左) R 加群という.

(1) $(ab)x = a(bx)$

(2) $a(x + y) = ax + ay$

(3) $(a + b)x = ax + bx$

(4) R の単位元 1 に対して $1x = x$

R が体であるとき, M は R 上のベクトル空間と呼ばれ, M の元はベクトルと呼ばれる.

M を R 加群, N を加法群 M の部分群とする. 任意の $a \in R$ と任意の $x \in N$ に対して $ax \in N$ が成り立つとき N を M の部分加群という. 部分加群はそれ自身 R 加群である.

R 加群 M の部分集合 S に対して S の有限個の元の 1 次結合として表される元全体, すなわち

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \qquad (a_i \in R, x_j \in S)$$

の形の元全体の集合は M の部分加群となる. この部分加群を S で生成される部分加群という. 特に M が有限集合 S で生成されるとき M を有限生成 R 加群という. 以下特に断らない限り R 加群はすべて有限生成であるとする.

R 加群 M の部分集合 B が

$$\sum_{i=1}^{n} a_ix_i = 0 \quad (a_i \in R,\ x_i \in B) \quad \Longrightarrow \quad a_1 = \cdots = a_n = 0$$

をみたすとき B は R 上 1 次独立であるという. R 上 1 次独立でないとき R 上 1 次従属であるという.

M を生成する 1 次独立な部分集合を M の (R) 基底という. B が M の基底であることと, M の任意の元 x が一意的に

$$x = c_1x_1 + \cdots + c_nx_n \qquad (c_i \in R,\ x_i \in B)$$

と B の有限個の元の 1 次結合として表されることとは同値である.

基底を持つ R 加群を自由 R 加群という.

定理 1.25 ([2, 3 章 例題 27.9]) 体 F 上のベクトル空間 V は自由 F 加群である．V の F 基底に含まれる元の個数は基底の選び方によらない．これをベクトル空間 V の F 上の次元といい $\dim V$ と表す．

以下, 有限生成 F 加群 V を有限次元ベクトル空間という．また有限生成でない F 加群 を無限次元ベクトル空間という．

定理 1.26 ([2, 3 章 定理 30.1]) R は可換環とする．このとき自由 R 加群 M の基底に含まれる元の個数は基底の選び方によらない．これを M の階数といい $rank\ M$ と表す．

定義 1.27 (体の拡大) 体 E の部分環 F が E の演算に関して体をなすとき，F を E の部分体, E を F の拡大体という．また E が F の拡大体であることを E/F と表し, 体の拡大という．

定義 1.28 (有限次拡大体) 体 E は部分体 F 上のベクトル空間と見なすことができる．E が F 上有限次元ベクトル空間であるとき E を F の有限次拡大 (体), 無限次元ベクトル空間であるとき, 無限次拡大 (体) という．また E の F 上のベクトル空間としての次元を拡大次数といい $[E : F]$ と表す．

定義 1.29 (2 次体) 複素数体 $\mathbb{C}$ の部分体で, 有理数体 $\mathbb{Q}$ の有限次元拡大である体 E を代数体という．代数体 E の $\mathbb{Q}$ 上の拡大次数が n のとき E を n 次代数体という．また 2 次代数体を単に 2 次体という．

1.4 イデアル

定義 1.30 (イデアル) 可換環 R の空でない部分集合 I が次の条件をみたすとき R のイデアルという．

(1) $\alpha, \beta \in I \implies \alpha + \beta \in I$

(2) $\gamma \in R,\ \alpha \in I \implies \gamma\alpha \in I$

可換環 R の元 $\alpha_1, \ldots, \alpha_r \in R$ に対して

$$I = \{\ \gamma_1\alpha_1 + \cdots + \gamma_r\alpha_r \ \mid\ \gamma_i \in R\ \}$$

とおけば, I は R のイデアルとなる. このとき I を $\alpha_1, \ldots, \alpha_r$ によって生成されるイデアルといい $I = (\alpha_1, \cdots, \alpha_r)$ と表す. I は $\alpha_1, \cdots, \alpha_r$ を含む最小のイデアルである. なぜならば I' を $\alpha_1, \ldots, \alpha_r$ を含む R のイデアルとすると I' は $\gamma_1\alpha_1 + \cdots + \gamma_r\alpha_r \in I'$ より $I \subseteq I'$ となるからである. 特に 1 つの元 α から生成されるイデアル (α) を単項イデアルという. なお, 以下において可換環はすべてのイデアルが有限生成であるような環であるとする (このような環はネーター環と呼ばれる).

定理 1.31 可換環 R のイデアル $A = (\alpha_1, \ldots, \alpha_r),\ B = (\beta_1, \ldots, \beta_s)$ に対し次の 2 条件は同値である.

(1) $A = B$

(2) $\alpha_i = \sum_{j=1}^{s} \gamma_{ij}\beta_j\ ,\quad \beta_j = \sum_{i=1}^{r} \delta_{ji}\alpha_i \quad (\gamma_{ij}, \delta_{ji} \in R\ )$ と表される.

Proof (1) が成り立つとする. A の元 α_i は B の元でもあるから

$$\alpha_i = \sum_{j=1}^{s} \gamma_{ij}\beta_j\ , \quad (\gamma_{ij} \in R)$$

と表される. B の元 β_j についても同様である. よって (2) が成り立つ.

逆に (2) が成り立つとする. このとき $\alpha_1, ..., \alpha_r \in B$ となることから

$$A = \{\ \gamma_1\alpha_1 + \cdots + \gamma_r\alpha_r\ \mid\ \gamma_i \in R\ \} \subseteq B$$

となる. 同様に $\beta_1, ..., \beta_s \in A$ より $B \subseteq A$ が導かれる. ゆえに $A = B$ である. ∎

2 つのイデアル $A = (\alpha_1, \ldots, \alpha_r),\ B = (\beta_1, \ldots, \beta_s)$ の積を

$$AB = (\alpha_1\beta_1, \ldots, \alpha_1\beta_s, \ldots\ldots \alpha_r\beta_1, \ldots, \alpha_r\beta_s)$$

と定める. 特に $A = (\alpha)$, $B = (\beta)$ のとき $AB = (\alpha)(\beta) = (\alpha\beta)$ である. まずこの積が well-defined であることを示そう.

定理 1.32 可換環 R のイデアル A, B の積 AB は生成元のとり方によらない.

Proof $A = (a_1, \ldots, a_r) = (\alpha_1, \ldots, \alpha_t),\ B = (b_1, \ldots, b_s) = (\beta_1, \ldots, \beta_u)$ とする.

$$(a_1b_1, \ldots\ldots, a_rb_s) = (\alpha_1\beta_1, \ldots\ldots, \alpha_t\beta_u)$$

を示せばよい. ここで a_i は α_j の 1 次結合であり, b_k は β_ℓ の 1 次結合であるから a_ib_k は $\alpha_j\beta_\ell$ の 1 次結合である. 同様にして $\alpha_j\beta_\ell$ は a_ib_k の 1 次結合である. 従って定理 1.31 により

$$(a_1b_1, \ldots\ldots, a_rb_s) = (\alpha_1\beta_1, \ldots\ldots, \alpha_t\beta_u)$$

を得る. ∎

可換環 R の乗法は交換可能であり, 結合律もみたすから次の定理が成り立つ (証明略).

定理 1.33 可換環 R のイデアル A, B, C について $AB = BA$, $A(BC) = (AB)C$ が成り立つ.

可換環 R のイデアル I と $a, b \in R$ に対して $a - b \in I$ であるとき $a \equiv b \pmod{I}$ と表し, I を法として a は b に合同であるという. 合同関係は R 上の同値関係であり, 各同値類を I を法とする剰余類という. I を法とする剰余類全体を R/I とおく. R の元 a を含む剰余類を $\overline{a}$ と表すことにし, R/I における加法と乗法を $\overline{a} + \overline{b} = \overline{a+b}$, $\overline{a}\overline{b} = \overline{ab}$ と定義すれば, これは well-defined であり, この演算により R/I は可換環をなす (cf. [2, 3 章 pp.84-85]). R/I を R の I による剰余環という.

定義 1.34 (素イデアル) 整域 R のイデアル I に対し剰余環 R/I が整域であるとき, I を素イデアルという.

剰余環の定義より, 次の 4 つは同値である. ただし, $\alpha, \beta \in R$ とする.

(1) I は R の素イデアル.

(2) R/I は整域である.

(3) $\alpha\beta \equiv 0 \pmod{I} \implies \alpha \equiv 0$ または $\beta \equiv 0 \pmod{I}$

(4) $\alpha\beta \in I \implies \alpha \in I$ または $\beta \in I$

定理 1.35 P を整域 R の素イデアル, S を R の部分環とするとき, $P \cap S$ は S の素イデアルである.

Proof $P \cap S$ が S のイデアルであることは明らかである. $a, b \in S$, $ab \in P \cap S$ とすると $ab \in P$ となるが, P は素イデアルだから $a \in P$ または $b \in P$ が成り立つ. すなわち $a \in P \cap S$ または $b \in P \cap S$ となる. ゆえに $P \cap S$ は S の素イデアルである. ∎

1.5 一意分解整域

R を整域, $\alpha, \beta, \gamma \in R$ とする. $\mathbb{Z}$ の場合と同様に $\alpha = \beta\gamma$ が成り立つとき 「α を β の倍数」,「 β を α の約数」,「β は α を割る」,「α は β で割り切れる」などといい, $\beta \mid \alpha$ と表す.

定義 1.36 (同伴) 整域 R の 2元 α, β に対し $\alpha = u\beta$ をみたす単数 $u \in R$ が存在するとき α と β は同伴であるという.

同伴という関係は R 上の同値関係である.

定理 1.37 整域の 2 元 α, β に対し次は同値である.

(1) $(\alpha) = (\beta)$

(2) α と β は同伴である.

Proof α と β が同伴であると仮定すると $\alpha = u\,\beta$ をみたす単数 u が存在する. このとき $\beta = u^{-1}\alpha$ となる. 従って定理 1.31 より $(\alpha) = (\beta)$ が得られる. 逆に $(\alpha) = (\beta)$ であるとすれば $\alpha = \gamma\beta$, $\beta = \delta\alpha$ をみたす γ, δ が存在する. ここで $\alpha = \gamma\delta\alpha$ となるが R は整域であるから $\gamma\delta = 1$ となる. 従って γ, δ は単数である. よって α と β は同伴である. ∎

系 1.38 整域 R において α が単数であることと $(\alpha) = (1)$ が成り立つことは同値である.

定義 1.39 (単項イデアル整域) 任意のイデアルが単項イデアルである整域 R を単項イデアル整域という.

補題 1.40 単項イデアル整域 R の 0 でない元の列 $\alpha_1, \alpha_2, \ldots$ が $\alpha_{i+1} \mid \alpha_i$ をみたしているとする. このとき, ある $n_0 \in \mathbb{N}$ が存在して, 任意の $n \geq n_0$ に対して α_n と α_{n_0} が同伴となる.

Proof R のイデアル (α_i) $(i = 1, 2, \cdots)$ 全ての和集合を I とする. まず I が R のイデアルであることを示す. $x, y \in I$ とすると $\alpha_i \mid x$, $\alpha_j \mid y$ をみたす i, j が存在する. $i \geq j$ の場合も同様であるから $i \leq j$ の場合について考える. $\alpha_j \mid \alpha_i$, $\alpha_j \mid x$ より $x, y \in (\alpha_j)$ となる. 従って $x + y \in (\alpha_j) \subseteq I$ が成り立つ. 次に $x \in I, \gamma \in R$ に対して $x \in (\alpha_i)$ をみたす i が存在するので $\gamma\, x \in (\alpha_i) \subseteq I$ も成り立つ. よって I は R のイデアルである.

さて R は単項イデアル整域だから $I=(\beta)$ と表される. これより任意の i に対し $\beta \mid \alpha_i$ が成り立つ. 一方 $\beta \in I$ より $\beta \in (\alpha_{n_0})$ となる n_0 が存在する. 従って $n \geq n_0$ ならば $\alpha_n \mid \alpha_{n_0}$ が成り立つが, $\alpha_{n_0} \mid \beta$ と $\beta \mid \alpha_n$ より $\alpha_{n_0} \mid \alpha_n$ も成り立つ. ゆえに α_{n_0} と α_n は同伴である. ∎

定義 1.41 (既約元) 整域 R の 0 でも単数でもない元 α が次の条件をみたすとき, α は既約であるという.

$$\alpha=\beta\gamma \text{ ならば } \beta \text{ または } \gamma \text{ が単数である.}$$

定義 1.42 (素元) 整域 R の 0 でも単数でもない元 π が次の性質をもつとき π を素元という.

$$\pi \mid \alpha\beta \quad (\alpha,\beta \in R) \quad \Longrightarrow \quad \pi \mid \alpha \text{ または } \pi \mid \beta$$

有理素数 p は $\mathbb{Z}$ の素元である.

定理 1.43 整域 R の元 π について, π が R の素元であることと (π) が R の素イデアルであることとは同値である.

Proof　次の同値変形より導かれる. ただし $\alpha,\beta \in R$ である.

$$\begin{aligned}
\pi \text{ は } R \text{ の素元} &\iff \pi \mid \alpha\beta \text{ ならば } \pi \mid \alpha \text{ または } \pi \mid \beta \\
&\iff \alpha\beta \text{ が } \pi \text{ の倍数ならば } \alpha \text{ または } \beta \text{ が } \pi \text{ の倍数} \\
&\iff \alpha\beta \in (\pi) \text{ ならば } \alpha \in (\pi) \text{ または } \beta \in (\pi) \\
&\iff (\pi) \text{ は素イデアル}
\end{aligned}$$

∎

定理 1.44 整域 R において素元は既約元である.

Proof　素元 π が $\pi=\alpha\beta$ と分解されたとする. このとき $\pi \mid \alpha\beta$ より $\pi \mid \alpha$ または $\pi \mid \beta$ が成り立つ. 今 $\pi \mid \alpha$ と仮定すると $\alpha=\pi\gamma$ と表されることから $\pi=\alpha\beta=\pi\gamma\beta$ となるが $\pi \neq 0$ より $1=\gamma\beta$ を得る. ゆえに β は R の単数となる. $\pi \mid \beta$ と仮定しても同様にして α が単数であることが導かれる. ゆえに α または β が単数となる. よって π は既約元である. ∎

定義 1.45 整域 R の 0 でも単数でもない任意の元 α が有限個の既約元の積として表され, かつ $\alpha = \pi_1 \cdots \pi_r = \rho_1 \cdots \rho_s$ と 2 通りに既約元の積として表されるときは $r = s$ であり, 番号を適当に付け直すと π_i と ρ_i が同伴になるようにできるとき, R を一意分解整域という.

一意分解整域を UFD と略記することがある.

定義 1.46 0 でも単数でもない元はすべて有限個の素元の積として表されるような整域を素元分解整域という.

定理 1.47 一意分解整域 R において既約元と素元は一致する.

Proof　定理 1.44 より素元は既約元である. 従って一意分解整域において既約元が素元であることを示せばよい. 今 ρ を既約元とし, $\rho \mid \alpha\beta$ と仮定する. このとき $\alpha\beta = \rho\gamma$ と表されるが R は一意分解整域だから ρ と同伴な既約元 π が α または β の既約分解に現れる. よって $\rho \mid \alpha$ または $\rho \mid \beta$ が成り立つ. ゆえに ρ は素元である. ∎

系 1.48 一意分解整域は素元分解整域である.

Proof　一意分解整域において 0 でも単数でもない元は既約元の積として表される. 一方, 定理 1.47 より, 一意分解整域において既約元は素元である. ゆえに一意分解整域においては 0 でも単数でもない元は素元の積として表される. よって一意分解整域は素元分解整域である. ∎

定理 1.49 (素元分解の一意性) 素元分解整域において素元分解は一意的である. また素元分解整域は一意分解整域である.

Proof　素元分解整域 R の元 α が

$$\alpha = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

と 2 通りに素元分解されたとする. このとき $r = s$ であり, 適当に番号を付け直すことにより p_1 と q_1, p_2 と q_2, …, p_r と q_r がそれぞれ同伴となることを r に関する帰納法により証明する.

$r = 1$ のとき p_1 は既約元でその約数は単数と p_1 と同伴な元のみであるから $s = 1$ で q_1 と p_1 は同伴である.

次に $r > 1$ とし $r-1$ までは成立しているものとする． $q_1 q_2 \cdots q_s \in (p_1)$ であり (p_1) は素イデアルだから， $q_1, q_2, \ldots, q_s$ のうちのいずれか, 例えば q_1 が $q_1 \in (p_1)$ をみたす. このとき $p_1 \mid q_1$ で, q_1 が既約元であるから p_1 と q_1 は同伴となる. 従って適当な単数 u により $q_1 = up_1$ とおくことができ

$$p_2 \cdots p_r = (uq_2)q_3 \cdots q_s$$

が成り立つ. ここで uq_2 も素元であるから帰納法の仮定により $r-1 = s-1$ で, 適当に番号を付け直すことで p_2 と q_2 ,..., p_r と q_r がそれぞれ同伴となる. よって r の場合も証明された.

以上で素元分解整域においては素元分解の一意性が成り立つことが示された.

次に β を R の既約元として， $\beta = p_1 \cdots p_\ell$, ($p_i$は素元) と素元分解されたとする. β の約数は β と同伴な元か単数のみであるから $\ell = 1$ で $p_1 = \beta$ が成り立つ. 従って β は素元である. ゆえに素元分解整域において既約元と素元は一致する. 素元分解が一意であるから既約分解も一意である. よって素元分解整域は一意分解整域である. ∎

系 1.48 と定理 1.49 より次の定理が得られる.

定理 1.50 整域 R について一意分解整域であることと素元分解整域であることとは同値である.

定理 1.51 単項イデアル整域は素元分解整域である.

Proof　背理法で示す. 単項イデアル整域で素元分解整域でないものが存在したとしてそれを R とする． R には 0 でも単数でもない元 α_1 で素元の積として表されないものが存在する． α_1 は素元でないから $\alpha_1 \mid \beta\gamma$ かつ $\alpha_1 \nmid \beta$, $\alpha_1 \nmid \gamma$ をみたす β, γ が存在する. $(\alpha_1, \beta) = R$ とすると $1 = \alpha_1 x + \beta y$ と表されることから $\gamma = \alpha_1\gamma x + \beta\gamma y$ より $\alpha_1 \mid \gamma$ となり矛盾が生じる. 従って $(\alpha_1, \beta) = (\lambda) \subsetneq R$ である. $\alpha_1 = \lambda\delta$ とおく. δ が単数ならば $\alpha_1 \mid \lambda$, $\lambda \mid \beta$ より矛盾が生じるので δ は単数でない. よって λ, δ は 0 でも単数でもない. また λ, δ の少なくとも一方は素元の積として表すことができない. それを α_2 とおく. α_2 は 0 でも単数でもなく, 素元の積として表されず $(\alpha_1) \subsetneq (\alpha_2)$ をみたす. なぜならば $(\alpha_1) = (\alpha_2)$ とすれば α_1 と α_2 が同伴となることから λ, δ の一方が単数となり, 先に示したことに矛盾するからである． α_2 から上と同様にして 0 でも単数でもなく, 素元の積として表されない元 α_3 が定まる. 以下, 同様にして

$$(\alpha_1) \subsetneq (\alpha_2) \subsetneq (\alpha_3) \subsetneq \cdots\cdots \subsetneq (\alpha_n) \subsetneq (\alpha_{n+1}) \subsetneq \cdots\cdots$$

と無限に続く R の単項イデアルの列が得られるが, これは補題 1.40 に矛盾する. ∎

Euclid 整域

R は整域とする. 写像 $\phi : R \longmapsto \mathbb{N} \cup \{0\}$ で次の条件をみたすものが存在するとき R を Euclid 整域という.

(1) $\alpha \neq 0$ ならば $\phi(\alpha) > 0$

(2) R の任意の元 $\alpha(\neq 0)$, β に対して $\beta = \alpha q + r, \quad \phi(r) < \phi(\alpha)$ をみたす $q, r \in R$ が存在する.

定理 1.52 *Euclid* 整域は単項イデアル整域である.

Proof R を Euclid 整域とし, A を R の 0 でないイデアルとする. 0 でない元 $x \in A$ に対し $\phi(x)$ は自然数だから, その中に最小値が存在する. この最小値を与える A の元を α とする. このとき任意の $\beta \in A$ に対し

$$\beta = \alpha q + r, \qquad \phi(r) < \phi(\alpha)$$

となる q, r が定まる. ここで $r \neq 0$ とすると $r = \beta - \alpha q \in A$ となり $\phi(\alpha)$ の最小性に反する. 従って $r = 0$ となり $\beta \in (\alpha)$ を得る. これより $A = (\alpha)$ となり, R の任意のイデアルが単項イデアルであることが示された. よって R は単項イデアル整域である. ∎

有理整数環 $\mathbb{Z}$ は絶対値をとる写像により Euclid 整域となるので単項イデアル整域である.

定理 1.50, 定理 1.51, 定理 1.52 より次の定理を得る.

定理 1.53 *Euclid* 整域は一意分解整域である.

最後に単項イデアル整域上の加群についての次の定理をあげておく.

定理 1.54 ([2, 3 章 定理 30.3]) R は単項イデアル整域とする. このとき階数 n の自由 R 加群の部分加群は階数が n 以下の自由 R 加群となる.

2章　2次体の整数環

この章では2次体の整数環に関する基本的定理について述べる.

§2.1 では2次体が平方因子をもたない整数 $m \neq 0, 1$ により

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

と与えられること, および $\mathbb{Q}(\sqrt{m})$ に含まれる代数的整数全体 O_m が部分環をなすことを示す. さらに $m \equiv 1 \pmod 4$ の場合と $m \equiv 2, 3 \pmod 4$ の場合に分けて整数環 O_m の $\mathbb{Z}$ 基底を求める.

§2.2 では $m \equiv 2, 3 \pmod 4$ かつ O_m が一意分解整域である場合について, 有理素数 p の素元分解が平方剰余 $\left(\frac{m}{p}\right)$ により定まることを示す. これは4章で証明する (p) の素イデアル分解法則のひな形とも目される.

§2.3 では O_{-2}, O_3 が一意分解整域であることを示し, 有理素数 p の素元分解を例示する.

2.1　2次体の整数環

K を2次体とする. K は有理数体 $\mathbb{Q}$ 上の2次元のベクトル空間であるから適当な複素数 α が存在し

$$K = \mathbb{Q}(\alpha) = \mathbb{Q} + \mathbb{Q} \cdot \alpha = \{\, u + v\alpha \mid u, v \in \mathbb{Q} \,\}$$

と表すことができる. ここで $\alpha^2 \in K$ だから適当な有理数 s, t が存在して

$$\alpha^2 = s \cdot \alpha + t \cdot 1 \quad \text{すなわち} \quad \alpha^2 - s\alpha - t = 0$$

が成り立つ. ここで $n = s^2 + 4t$ とおくと $\alpha \notin \mathbb{Q}$ より $n \notin \mathbb{Q}^2 = \{u^2 \mid u \in \mathbb{Q}\}$ である. 従って $n = \ell^2 \cdot m$ をみたす正の有理数 ℓ と平方因子をもたない整数, すなわち素数の平方で割

り切れない整数 $m \neq 0, 1$ が一意に定まる. $\alpha = \dfrac{s \pm \sqrt{s^2+4t}}{2}$ であるから

$$\begin{aligned}\mathbb{Q}(\alpha) &= \{\, u + v\alpha \mid u, v \in \mathbb{Q} \,\} = \{\, u + \frac{s}{2}v \pm v\ell\frac{\sqrt{m}}{2} \mid u, v \in \mathbb{Q} \,\} \\ &= \{\, a + b\sqrt{m} \mid a, b \in \mathbb{Q} \,\} = \mathbb{Q}(\sqrt{m})\end{aligned}$$

が成り立つ.

定理 2.1 2 次体は平方因子をもたない整数 $m \neq 0, 1$ により

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

と表される. また, このような $\mathbb{Q}(\sqrt{m})$ は 2 次体である.

Proof 2 次体が $\mathbb{Q}(\sqrt{m})$ と表されることはすでに示した. 逆に $\mathbb{Q}(\sqrt{m})$ が 2 次体であることを示せばよい. $\mathbb{Q}(\sqrt{m})$ が $\mathbb{C}$ の部分環であることは容易に確かめられる. 従って $a + b\sqrt{m} \neq 0$ が可逆であることを示せば $\mathbb{Q}(\sqrt{m})$ は $\mathbb{Q}$ と異なり, $\mathbb{Q}$上 2 元で生成されることから 2 次体であることがわかる. ここで a, b が同時に 0 とはならず, m が平方因子をもたないことから $a^2 - mb^2 \neq 0$ であるので

$$\frac{a - b\sqrt{m}}{a^2 - mb^2} \in \mathbb{Q}(\sqrt{m}) \qquad \text{かつ} \qquad (a + b\sqrt{m}) \left(\frac{a - b\sqrt{m}}{a^2 - mb^2} \right) = 1$$

が成り立つ. ゆえに $a + b\sqrt{m}$ は $\mathbb{Q}(\sqrt{m})$ の可逆元である. よって $\mathbb{Q}(\sqrt{m})$ は 2 次体である. ∎

以下 $\mathbb{Q}(\sqrt{m})$ の元 $z = a + b\sqrt{m}$ に対して $z' = a - b\sqrt{m}$ とおき z' を z の共役元 (または共役) という. z' も $\mathbb{Q}(\sqrt{m})$ の元である. 明らかに $z = z'$ となるのは $z \in \mathbb{Q}$ のときのみである. また $\mathbb{Q}(\sqrt{m})$ の元 z_1, z_2 に対して $(z_1 + z_2)' = z_1' + z_2'$, $(z_1 \cdot z_2)' = z_1' \cdot z_2'$ が成り立つことを注意しておく. 次に

$$\mathcal{T}(z) = z + z' = 2a\,, \qquad \mathcal{N}(z) = zz' = a^2 - mb^2$$

と定め, $\mathcal{T}(z), \mathcal{N}(z)$ をそれぞれ z のトレース, ノルムという. z のトレースとノルムは有理数である.

定理 2.2 $\mathbb{Q}(\sqrt{m}) \ni z_1, z_2$ に対して次が成り立つ.

$$\mathcal{T}(z_1 + z_2) = \mathcal{T}(z_1) + \mathcal{T}(z_2)\,, \qquad \mathcal{N}(z_1 z_2) = \mathcal{N}(z_1)\,\mathcal{N}(z_2)$$

Proof $\mathbb{Q}(\sqrt{m}) \ni z_1, z_2$ に対して

$$\begin{aligned} \mathcal{T}(z_1+z_2) &= (z_1+z_2)+(z_1+z_2)' = (z_1+z_1')+(z_2+z_2') = \mathcal{T}(z_1)+\mathcal{T}(z_2) \\ \mathcal{N}(z_1z_2) &= (z_1z_2)(z_1z_2)' = (z_1z_1')(z_2z_2') = \mathcal{N}(z_1)\mathcal{N}(z_2) \end{aligned}$$

が成り立つ. よって定理が証明された. ∎

2 次体 $\mathbb{Q}(\sqrt{m})$ の任意の元 z は

$$X^2 - \mathcal{T}(z)\,X + \mathcal{N}(z) = 0$$

をみたす. 従って定義 1.22 により代数的数である.

定理 2.3 2 次体 $\mathbb{Q}(\sqrt{m})$ の元 α に対して次は同値である.

(1) α は代数的整数である.

(2) $\mathcal{T}(\alpha) \in \mathbb{Z}$ かつ $\mathcal{N}(\alpha) \in \mathbb{Z}$ が成り立つ.

Proof まず (2) を仮定して (1) を導く.

$$f(X) = X^2 - \mathcal{T}(\alpha)X - \mathcal{N}(\alpha)$$

とおくと $f(\alpha) = 0$ である. また $\mathcal{T}(\alpha), \mathcal{N}(\alpha) \in \mathbb{Z}$ より $f(X) \in \mathbb{Z}[X]$ であるから α は代数的整数である.

次に (1) から (2) を導く. α を代数的整数とする. 定義 1.22 より α は $\mathbb{Z}$ 係数モニック多項式 $g(X)$ の根である. ここで α の最小多項式を $p(X)$ とすると定理 1.23 より, $g(X) = p(X)q(X)$ と分解できる. $g(X), p(X)$ はモニックであるから $q(X)$ もモニックで定理 1.24 より $p(X)$ の係数はすべて有理整数である. $\deg(p) = 1$ ならば $\alpha \in \mathbb{Z}$ であるから明らかに (2) が成り立つ. 従って以下 $\deg(p) > 1$ と仮定する.

$$f(X) = X^2 - \mathcal{T}(\alpha)X + \mathcal{N}(\alpha)$$

とおくと $f(\alpha) = 0$ より $p(X) \mid f(X)$ となる. 次数を比較して $\deg(p) = \deg(f)$ を得る. ゆえに $f(X)$ は $p(X)$ の定数倍である. 一方 $f(X), p(X)$ はモニックであることから $p(X) = f(X)$ が得られる. 以上から $f(X)$ の係数が有理整数であり, (2) の成り立つことが示された. ∎

2 次体の整数環

以下, 2 次体 $\mathbb{Q}(\sqrt{m})$ に含まれる代数的整数全体のなす集合を O_m と表し, $\mathbb{Q}(\sqrt{m})$ の整数環と呼ぶ. ただし O_m が $\mathbb{Q}(\sqrt{m})$ の部分環であることは定理 2.7 で証明する.

補題 2.4 2 次体 $\mathbb{Q}(\sqrt{m})$ の元 $\alpha = a + b\sqrt{m}$ について次は同値である.

(1) $\alpha = a + b\sqrt{m} \in O_m$

(2) $u = 2a$, $v = 2b$ は有理整数で $u^2 - mv^2 \equiv 0 \pmod 4$ をみたす.

Proof まず (1) から (2) を導く. $\alpha = a + b\sqrt{m} \in O_m$ であるから定理 2.3 より $\mathcal{T}(\alpha) = 2a = u, \mathcal{N}(\alpha) = a^2 - mb^2$ は有理整数である. よって $u^2 - mv^2 = 4(a^2 - mb^2) \equiv 0 \pmod 4$ が成り立つ. またこれより $mv^2 = m(2b)^2 \in \mathbb{Z}$ を得るが m は平方因子を含まないから有理数 $2b$ の分母は 1 でなければならない. すなわち $v = 2b \in \mathbb{Z}$ である.

次に (2) から (1) を導く. 仮定より $u = 2a, v = 2b \in \mathbb{Z}$, $u^2 - mv^2 \equiv 0 \pmod 4$ であるから $4(a^2 - mb^2) \equiv 0 \pmod 4$ が成り立つ. 従って $\mathcal{N}(\alpha) = a^2 - mb^2 \in \mathbb{Z}$ を得る. これと $\mathcal{T}(\alpha) = u \in \mathbb{Z}$ より定理 2.3 の条件 (2) をみたすから $\alpha \in O_m$ が成立する. ∎

補題 2.5 $m \neq 0, 1$ が平方因子を含まない整数で $m \equiv 2, 3 \pmod 4$ のとき, $\mathbb{Z} \ni u, v$ について次がなり立つ.

$$u^2 - mv^2 \equiv 0 \pmod 4 \quad \Longleftrightarrow \quad u, v \text{ はともに偶数である}$$

Proof $u^2 \equiv mv^2 \pmod 4$ と仮定する. $m \equiv 2 \pmod 4$ のときは $2 \mid u$ となり $4 \mid mv^2$ から $2 \mid v$ が得られる. よって u, v はともに偶数である. また $m \equiv 3 \pmod 4$ のときは v が奇数であるとすれば $mv^2 \equiv 3 \pmod 4$ となるが, このとき u も奇数となり $u^2 \equiv 1 \pmod 4$ に矛盾が生じる. よって v は偶数である. このとき u も明らかに偶数である. 逆に u, v がともに偶数であるときは明らかに $u^2 \equiv mv^2 \pmod 4$ が成り立つ. 以上で補題が証明された. ∎

補題 2.6 $m \neq 0, 1$ が平方因子を含まない整数で $m \equiv 1 \pmod 4$ のとき $\mathbb{Z} \ni u, v$ について次がなり立つ.

$$u^2 - mv^2 \equiv 0 \pmod 4 \quad \Longleftrightarrow \quad u \equiv v \pmod 2$$

Proof $u^2 \equiv mv^2 \pmod 4$ と仮定する. m は奇数であるから u^2 と v^2 の偶奇は一致する. 従って u と v の偶奇も一致する. 逆に $u \equiv v \pmod 2$ であれば $u^2 \equiv v^2 \equiv 0 \pmod 4$ ま

たは $u^2 \equiv v^2 \equiv 1 \pmod 4$ となるから $u^2 - mv^2 \equiv 0 \pmod 4$ が成り立つ. 以上で補題が証明された. ∎

定理 2.7 2 次体 $\mathbb{Q}(\sqrt{m})$ の整数環 O_m は次のように与えられる. 特に O_m は $\mathbb{Q}(\sqrt{m})$ の部分環である.

(1) $m \equiv 2, 3 \pmod 4$ のとき $\quad O_m = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$

(2) $m \equiv 1 \pmod 4$ のとき $\quad O_m = \left\{ \dfrac{u + v\sqrt{m}}{2} \mid u, v \in \mathbb{Z}, u \equiv v \pmod 2 \right\}$

Proof 補題 2.4 より

$$\alpha = a + b\sqrt{m} \in O_m \iff u = 2a, v = 2b \in \mathbb{Z},\ u^2 - mv^2 \equiv 0 \pmod 4$$

が成立する. $m \equiv 2, 3 \pmod 4$ のときは補題 2.5 より

$$u^2 - mv^2 \equiv 0 \pmod 4 \iff u, v \text{ はともに偶数である}$$

が成り立つ. 従ってこの場合

$$\alpha = a + b\sqrt{m} \in O_m \iff a, b \in \mathbb{Z}$$

を得る. よって $O_m = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$ が示された.

次に $m \equiv 1 \pmod 4$ のときは補題 2.6 より

$$u^2 - mv^2 \equiv 0 \pmod 4 \iff u \equiv v \pmod 2$$

が成り立つ. 従って

$$O_m = \left\{ \frac{u + v\sqrt{m}}{2} \mid u, v \in \mathbb{Z}, u \equiv v \pmod 2 \right\}$$

が示された. いずれの場合も O_m が $\mathbb{Q}(\sqrt{m})$ の部分環であることは容易に確かめられる. ∎

さて定理 2.7 より $m \equiv 2, 3 \pmod 4$ のときは

$$O_m = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$$

となる. 明らかに $\{1, \sqrt{m}\}$ は $\mathbb{Z}$ 上 1 次独立であるから O_m の $\mathbb{Z}$ 基底である. 特に O_m は階数 2 の自由 $\mathbb{Z}$ 加群である.

一方 $m \equiv 1 \pmod 4$ のときは定理 2.7 より

$$O_m = \left\{ \frac{u+v\sqrt{m}}{2} \mid u, v \in \mathbb{Z}, u \equiv v \pmod 2 \right\}$$

となる. ここで

$$\frac{u+v\sqrt{m}}{2} = \frac{(u-v)+v+v\sqrt{m}}{2} = \frac{u-v}{2} + v\left(\frac{1+\sqrt{m}}{2}\right)$$

と表され $\dfrac{u-v}{2} \in \mathbb{Z}$ であるから

$$O_m = \left\{ \ a + b\left(\frac{1+\sqrt{m}}{2}\right) \ \middle| \ a, b \in \mathbb{Z} \ \right\}$$

を得る. 明らかに $\{1, \frac{1+\sqrt{m}}{2}\}$ は $\mathbb{Z}$ 上 1 次独立であるから O_m の $\mathbb{Z}$ 基底である. よってこの場合も O_m は階数 2 の自由 $\mathbb{Z}$ 加群である. 以上より次の定理を得る.

定理 2.8 2 次体 $\mathbb{Q}(\sqrt{m})$ の 整数環 O_m は階数 2 の 自由 $\mathbb{Z}$ 加群である. ω を次のように定めると $\{1, \omega\}$ は O_m の $\mathbb{Z}$ 基底である.

$$\omega = \begin{cases} \sqrt{m} & m \equiv 2, 3 \pmod 4 \\ \dfrac{1+\sqrt{m}}{2} & m \equiv 1 \pmod 4 \end{cases}$$

定理 2.9 $O_m \cap \mathbb{Q} = \mathbb{Z}$ である.

Proof　定理 2.8 より O_m の元は有理整数 a, b により $a+b\omega$ と表される. ここで $a+b\omega \in \mathbb{Q}$ であることと $b = 0$ とは同値であるから $O_m \cap \mathbb{Q} = \mathbb{Z}$ が成り立つ. ∎

定理 2.10 O_m の元 α について次が成り立つ.

$$\alpha \text{ が単数} \quad \Longleftrightarrow \quad \mathcal{N}(\alpha) = \pm 1$$

Proof　$\mathcal{N}(\alpha) = \pm 1$ とする. このとき $\alpha\,\alpha' = \pm 1$ であるから α は単数である. 逆に α が単数であるとすると $\alpha\,\beta = 1$ となる $\beta \in O_m$ が存在する. 両辺のノルムをとると

$$\mathcal{N}(\alpha)\mathcal{N}(\beta) = \mathcal{N}(\alpha\,\beta) = \mathcal{N}(1) = 1$$

が得られるが $\mathcal{N}(\alpha), \mathcal{N}(\beta)$ は有理整数だから $\mathcal{N}(\alpha) = \mathcal{N}(\beta) = \pm 1$ である. ∎

定理 2.11 O_m の元 α, β が同伴ならば $\mathcal{N}(\alpha) = \pm\mathcal{N}(\beta)$ が成り立つ.

Proof 仮定より $\alpha = u\,\beta$ をみたす単数 u が存在する. このとき定理 2.10 より

$$\mathcal{N}(\alpha) = \mathcal{N}(u\beta) = \mathcal{N}(u)\mathcal{N}(\beta) = \pm\mathcal{N}(\beta)$$

が得られる. ∎

定理 2.12 $\alpha \in O_m$ とする. $\mathcal{N}(\alpha) = \pm p$ (p は有理素数) ならば α は既約元である.

Proof $\mathcal{N}(\alpha) = \pm p$ より α は 0 でも単数でもない. ここで $\alpha = \beta\gamma$ とすると $\mathcal{N}(\alpha) = \mathcal{N}(\beta)\mathcal{N}(\gamma) = \pm p$ が成り立つ. 従って $\mathcal{N}(\beta), \mathcal{N}(\gamma)$ の一方は ± 1 となり, 定理 2.10 より単数となる. よって α は既約元である. ∎

定理 2.13 $O_m \ni \alpha, \beta, \gamma$ が $\alpha \mid \beta$, $\alpha \mid \gamma$ をみたすとき任意の $\delta, \varepsilon \in O_m$ に対し $\alpha \mid \delta\,\beta + \varepsilon\,\gamma$ が成り立つ.

Proof 有理整数の場合と同様にして証明できる. ∎

2.2 有理素数の $\mathbb{Z}[\sqrt{m}]$ における素元分解

この節では $m \equiv 2, 3 \pmod 4$ と仮定する. 従って $\mathbb{Q}(\sqrt{m})$ の整数環 O_m は $\mathbb{Z}[\sqrt{m}]$ である. 以下 $O = \mathbb{Z}[\sqrt{m}]$ とおき O は一意分解整域であるとする.

π を O の素元とすると (π) は O の素イデアルである. 一方 $\mathbb{Z}$ は O の部分環であるから定理 1.35 より $(\pi) \cap \mathbb{Z}$ は $\mathbb{Z}$ の素イデアルである. 従って $p\mathbb{Z} = (\pi) \cap \mathbb{Z}$ をみたす有理素数 p が存在する. ここで $p \in (\pi)$ であることから $p = \pi\alpha$ をみたす $\alpha \in O$ が存在する. これより O の素元 π はある有理素数 p の約数となる.

次に有理素数 p を任意に選び p の O における素元分解を $p = \pi_1 \ldots \pi_r$ とする. 両辺のノルムをとると

$$p^2 = \mathcal{N}(\pi_1) \cdots \mathcal{N}(\pi_r)$$

を得る. π_i は単数でないので $\mathcal{N}(\pi_i) \neq \pm 1$ である. 従って $r = 1$ または $r = 2$ のいずれかが起こり得る.

(1) $r = 1$ の場合. このとき $p = \pi_1, \mathcal{N}(\pi_1) = p^2$ となる. また p は素元である.

(2) $r = 2$ の場合. このとき $p = \pi_1\pi_2, \mathcal{N}(\pi_1) = \mathcal{N}(\pi_2) = \pm p$ となる.

(i) $\mathcal{N}(\pi_1) = \mathcal{N}(\pi_2) = p$ のとき $p = \pi_1\pi_2 = \mathcal{N}(\pi_1) = \pi_1\pi_1'$ より $\pi_2 = \pi_1', p = \pi_1\pi_1'$ が成り立つ. $\pi_1 = \pi_1'$ とすれば π_1 は有理整数となり $\mathcal{N}(\pi_1) = p$ に矛盾する. よって $\pi_1 \neq \pi_1'$ である.

(ii) $\mathcal{N}(\pi_1) = \mathcal{N}(\pi_2) = -p$ のとき $p = \pi_1\pi_2 = -\mathcal{N}(\pi_1) = -\pi_1\pi_1'$ より $\pi_2 = -\pi_1'$ が成り立つ. この場合も上と同様に $\pi_1 \neq \pi_1'$ である.

上の (2) の場合についてさらに考察する.

$\mathbf{p \neq 2}$ の場合

$p = \pi_1\pi_2$ と仮定し, $\pi_1 = a + b\sqrt{m}$ とおくと $\mathcal{N}(\pi_1) = a^2 - mb^2 = \pm p$ が成り立つ. 今 $p \mid b$ と仮定すると $p \mid a$ より $p^2 \mid (a^2 - mb^2)$ が得られ矛盾が生じる. 従って $p \nmid b$ である.

$p \nmid m$ とする. $p \mid a$ ならば $p \mid mb^2$ より $p \mid b$ となり前述の結果に反する. 従って $p \nmid a$ である. このとき $a^2 \equiv mb^2 \pmod{p}$ より

$$\left(\frac{m}{p}\right) = \left(\frac{b}{p}\right)^2\left(\frac{m}{p}\right) = \left(\frac{mb^2}{p}\right) = \left(\frac{a^2}{p}\right) = 1$$

が成り立つ.

$p \mid m$ のときは $\left(\frac{m}{p}\right) = 0$ である.

以上から $p = \pi_1\pi_2$ と分解されるときは $\left(\frac{m}{p}\right) = 0, 1$ が成り立つ.

逆に $\left(\frac{m}{p}\right) = 1$ とすると $c^2 \equiv m \pmod{p}$ をみたす $c \in \mathbb{Z}$ が存在し

$$p \mid (c^2 - m) = (c + \sqrt{m})(c - \sqrt{m})$$

であるが $p \nmid (c \pm \sqrt{m})$ だから p は O の素元ではない. また $\left(\frac{m}{p}\right) = 0$ すなわち $p \mid m$ のとき $p \mid m = (\sqrt{m})^2$ であるが $p \nmid \sqrt{m}$ より p は O の素元ではない.

以上から p が素元でないこと, すなわち $p = \pi_1\pi_2$ と素元分解されることと $\left(\frac{m}{p}\right) = 0, 1$ となることとが同値であることが示された. これより p が素元であることと $\left(\frac{m}{p}\right) = -1$ であることも同値である.

次に $\left(\frac{m}{p}\right) = 1$ のとき π_1 と π_2 が同伴でないことを示す. π_1 と π_2 が同伴であるとすると単数 ρ が存在し $\pi_2 = \rho\pi_1$ と表される. $c^2 \equiv m \pmod{p}$ をみたす $c \in \mathbb{Z}$ に対して

$$p = \rho\pi_1^2, \qquad \pi_1^2 \mid (c + \sqrt{m})(c - \sqrt{m})$$

が成り立つ. $\pi_1^2 \mid (c+\sqrt{m})$ または $\pi_1^2 \mid (c-\sqrt{m})$ と仮定すると $p \mid (c+\sqrt{m})$ または $p \mid (c-\sqrt{m})$ となり矛盾が生じる. 従って $\pi_1 \mid (c+\sqrt{m})$ かつ $\pi_1 \mid (c-\sqrt{m})$ が成り立つ. このとき $\pi_1 \mid \{(c+\sqrt{m})+(c-\sqrt{m})\} = 2c$ より両辺のノルムをとると $p \mid 4c^2$ を得るが $p \neq 2$ より $p \mid c$ となり矛盾が生じる. よって π_1 と π_2 は同伴でない.

$\left(\frac{m}{p}\right) = 0$ とすると $p \mid m$ かつ $p \mid a^2 - mb^2$ から $p \mid a$ を得る. $\mathcal{N}(\pi_1) = \mathcal{N}(\pi_2) = p$ のときは $\pi_1 + \pi_2 = 2a$ かつ $\pi_1\pi_2 = p$ となるから $\pi_1\pi_2 \mid (\pi_1+\pi_2)$ が成り立つ. また $\mathcal{N}(\pi_1) = \mathcal{N}(\pi_2) = -p$ のときも $\pi_1 - \pi_2 = 2a$ かつ $\pi_1\pi_2 = p$ となるから $\pi_1\pi_2 \mid (\pi_1-\pi_2)$ が成り立つ. いずれの場合も $\pi_1 \mid \pi_2$ かつ $\pi_2 \mid \pi_1$ が成り立つので π_1 と π_2 は同伴である.

$\mathbf{p = 2}$ の場合

m が奇数のときは

$$(1+\sqrt{m})^2 = 2\left(\frac{1+m}{2} + \sqrt{m}\right), \qquad \frac{1+m}{2} + \sqrt{m} \in O$$

より $2 \mid (1+\sqrt{m})^2$ であるが $2 \nmid (1+\sqrt{m})$ より, 2 は素元でない.

m が偶数のときも $2 \mid m = (\sqrt{m})^2$ であるが $2 \nmid \sqrt{m}$ だから 2 は素元ではない. よっていずれの場合も $2 = \pi_1\pi_2$ と素元分解される.

$\pi_1 = a + b\sqrt{m}$ とおく. $\mathcal{N}(\pi_1) = \mathcal{N}(\pi_2) = 2$ のときは $\pi_1 + \pi_2 = 2a, \pi_1\pi_2 = 2$ より $\pi_1\pi_2 \mid (\pi_1+\pi_2)$ が成り立つ. $\mathcal{N}(\pi_1) = \mathcal{N}(\pi_2) = -2$ のときも $\pi_1 - \pi_2 = 2a, \pi_1\pi_2 = 2$ より $\pi_1\pi_2 \mid (\pi_1-\pi_2)$ が成り立つ. 従って $\pi_1 \mid \pi_2$ かつ $\pi_2 \mid \pi_1$ となり π_1 と π_2 は同伴となる.

以上をまとめると次の定理が得られる.

定理 2.14 (p の素元分解) $m \equiv 2, 3 \pmod 4$ とする. $O = \mathbb{Z}[\sqrt{m}]$ が一意分解整域であるとき O における有理素数 p の素元分解は次のようになる.

- $p \neq 2$ の場合.
  - (1) $\left(\frac{m}{p}\right) = 1$ のとき $p = \pm\pi\pi'$ となる. ここで $\mathcal{N}(\pi) = \pm p$ であり π と π' は同伴でない.
  - (2) $\left(\frac{m}{p}\right) = -1$ のとき p は O の素元である.
  - (3) $\left(\frac{m}{p}\right) = 0$ のとき $p = \rho\pi^2$ となる. ただし $\mathcal{N}(\pi) = \pm p$, ρ は単数である.
- $p = 2$ の場合. $2 = \rho\pi^2$ となる. ただし $\mathcal{N}(\pi) = \pm 2$, ρ は単数である.

2.3 $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{3}]$ における素元分解

ここでは前節の結果をふまえて, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{3}]$ における有理素数の素元分解について考察する. まず必要な補題を準備する.

補題 2.15 奇素数 p について次が成り立つ.

(1) $\left(\frac{-2}{p}\right) = 1$ ならば $p \equiv 1, 3 \pmod 8$ である.

(2) $\left(\frac{-2}{p}\right) = -1$ ならば $p \equiv 5, 7 \pmod 8$ である.

(3) $\left(\frac{3}{p}\right) = 1$ ならば $p \equiv 1, 11 \pmod{12}$ である.

(4) $\left(\frac{3}{p}\right) = -1$ ならば $p \equiv 5, 7 \pmod{12}$ である.

Proof

(1) $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ であるから $\left(\frac{-2}{p}\right) = 1$ より $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = 1$ であるかまたは $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = -1$ が成り立つ. 従って $p \equiv 1 \pmod 4$ かつ $p \equiv 1, 7 \pmod 8$ であるかまたは $p \equiv 3 \pmod 4$ かつ $p \equiv 3, 5 \pmod 8$ が成り立つ. よって $p \equiv 1, 3 \pmod 8$ を得る.

(2) (1) と同様にして $p \equiv 5, 7 \pmod 8$ を得る.

(3) $\left(\frac{3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)$ であるから $\left(\frac{3}{p}\right) = 1$ より $\left(\frac{-1}{p}\right) = \left(\frac{p}{3}\right) = 1$ であるかまたは $\left(\frac{-1}{p}\right) = \left(\frac{p}{3}\right) = -1$ が成り立つ. 従って $p \equiv 1 \pmod 4$ かつ $p \equiv 1 \pmod 3$ であるかまたは $p \equiv 3 \pmod 4$ かつ $p \equiv 2 \pmod 3$ が成り立つ. ゆえに $p \equiv 1, 11 \pmod{12}$ を得る.

(4) (3) と同様にして $p \equiv 5, 7 \pmod{12}$ を得る.

∎

$\mathbb{Z}[\sqrt{-2}]$

次の図 (1) のように, 複素平面上に x 軸を $\pm 1, \pm 2, \ldots$ 平行移動した直線と y 軸を $\pm\sqrt{2}, \pm 2\sqrt{2}, \ldots$ 平行移動した直線を描く. このときこれらの直線の交点と $\mathbb{Z}[\sqrt{-2}]$ の元 $\alpha = a + b\sqrt{-2}$ とが 1 対 1 に対応する. 以下このような点を格子点と呼ぶことにする.

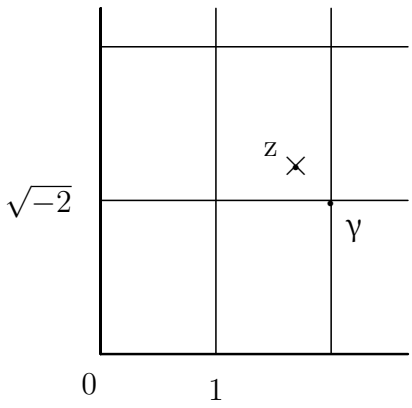
補題 2.16 任意の複素数 z に対して $|\, z - \gamma \,| \leq \frac{\sqrt{3}}{2}$ をみたす $\gamma \in \mathbb{Z}[\sqrt{-2}]$ が存在する.

Proof 右図の複素平面において, 格子点と $\mathbb{Z}[\sqrt{-2}]$ の各元が 1 対 1 に対応し, $\forall z \in \mathbb{C}$ は格子点を頂点とする辺の長さが 1, $\sqrt{2}$ の長方形の内部または辺上にあるから, z と最も近い格子点 $\gamma \in \mathbb{Z}[\sqrt{-2}]$ との距離について,

$$| z - \gamma | \leq \frac{\sqrt{3}}{2}$$

が成り立つ. よって補題が示された. ∎

図 (1)



$\mathbb{Z}[\sqrt{-2}] \ni \alpha = a + b\sqrt{-2}$ のノルムは $a^2 + 2b^2$ であり, $\alpha \neq 0$ のときは自然数である. また $\mathcal{N}(\alpha) = |\alpha|^2$ であることを注意しておく.

定理 2.17 $\mathbb{Z}[\sqrt{-2}]$ は一意分解整域である.

Proof 定理 1.53 より $\mathbb{Z}[\sqrt{-2}]$ がノルムに関して Euclid 整域であることを示せばよい. そのためには $\mathbb{Z}[\sqrt{-2}]$ の任意の元 $\alpha(\neq 0)$, β に対して

$$\beta = \alpha\gamma + \kappa \qquad \mathcal{N}(\kappa) < \mathcal{N}(\alpha)$$

をみたす $\gamma, \kappa \in \mathbb{Z}[\sqrt{-2}]$ が存在することを示せばよい. 補題 2.16 より

$$\left|\frac{\beta}{\alpha} - \gamma\right| \leq \frac{\sqrt{3}}{2} < 1 \implies |\beta - \alpha\gamma| < |\alpha|$$

をみたす $\gamma \in \mathbb{Z}[\sqrt{-2}]$ が存在する. ここで $\kappa = \beta - \alpha\gamma$ とおけば $\kappa \in \mathbb{Z}[\sqrt{-2}]$ であり

$$\mathcal{N}(\kappa) = \mathcal{N}(\beta - \alpha\gamma) = |\beta - \alpha\gamma|^2 < |\alpha|^2 = \mathcal{N}(\alpha)$$

が成り立つ. ゆえに $\mathbb{Z}[\sqrt{-2}]$ はノルムに関して Euclid 整域である. ∎

$\mathbb{Z}[\sqrt{-2}]$ は一意分解整域である. 従って, 定理 2.14 より $\mathbb{Z}[\sqrt{-2}]$ における有理素数 p の素元分解は次のようになる.

- $p = 2$ のとき, $2 = -(\sqrt{-2})^2$ である. ここで $\sqrt{-2}$ は素元である.
- $p \neq 2$ のとき.
  (1) $\left(\frac{-2}{p}\right) = 1$, すなわち $p \equiv 1, 3 \pmod 8$ のとき, $p = \pi\pi'$ である. ここで π と π' は同伴でない素元である. また $\pi = a + b\sqrt{-2}$ とすると $a^2 + 2b^2 = p$ である.

(2) $\left(\frac{-2}{p}\right) = -1$, すなわち $p \equiv 5, 7 \pmod 8$ のとき p は素元である.

(3) $\left(\frac{-2}{p}\right) = 0$ は起こり得ない.

$\mathbb{Z}[\sqrt{3}]$

$\mathbb{Z}[\sqrt{3}] \ni \alpha = a + b\sqrt{3}$ のノルムは $\mathcal{N}(\alpha) = a^2 - 3b^2$ であり, $\alpha \neq 0$ のとき $\mathcal{N}(\alpha) \neq 0$ である. 従って $\mathbb{Z}[\sqrt{3}]$ の 0 でない元のノルムの絶対値は自然数である.

定理 2.18 $\mathbb{Z}[\sqrt{3}]$ は一意分解整域である.

Proof $\mathbb{Z}[\sqrt{3}]$ がノルムに関して Euclid 整域であることを示せばよい. そのためには $\mathbb{Z}[\sqrt{3}]$ の任意の元 $\alpha(\neq 0), \beta$ に対して

$$\beta = \alpha\gamma + \kappa \qquad |\mathcal{N}(\kappa)| < |\mathcal{N}(\alpha)|$$

をみたす $\gamma, \kappa \in \mathbb{Z}[\sqrt{3}]$ が存在することを示せばよい. $\frac{\beta}{\alpha} = x + y\sqrt{3}$ とおき, x, y に最も近い有理整数を m, n とする. このとき

$$|x - m| \leq \frac{1}{2}, \qquad |y - n| \leq \frac{1}{2}$$

が成り立つ. ここで $\gamma = m + n\sqrt{3}$, $\kappa = \beta - \alpha\gamma$ とおくと $\gamma, \kappa \in \mathbb{Z}[\sqrt{3}]$ であり

$$\begin{aligned} |\mathcal{N}(\kappa)| &= |\kappa\kappa'| = |(\beta - \alpha\gamma)(\beta' - \alpha'\gamma')| = \left|\left(\frac{\beta}{\alpha} - \gamma\right)\left(\frac{\beta'}{\alpha'} - \gamma'\right)\right| \cdot |\alpha\alpha'| \\ &= \left|\left((x-m) + (y-n)\sqrt{3}\right)\left((x-m) - (y-n)\sqrt{3}\right)\right| \cdot |\mathcal{N}(\alpha)| \\ &= |(x-m)^2 - 3(y-n)^2| \cdot |\mathcal{N}(\alpha)| \\ &\leq \frac{3}{4}|\mathcal{N}(\alpha)| < |\mathcal{N}(\alpha)| \end{aligned}$$

が成り立つ. ゆえに $\mathbb{Z}[\sqrt{3}]$ はノルムに関して Euclid 整域である. ∎

$\mathbb{Z}[\sqrt{3}]$ は一意分解整域である. 従って, 定理 2.14 より $\mathbb{Z}[\sqrt{3}]$ における有理素数 p の素元分解は次のようになる.

- $p = 2$ のときは $2 = (2 - \sqrt{3})(1 + \sqrt{3})^2$ である. ここで $1 + \sqrt{3}$ は素元である.
- $p \neq 2$ のとき.

(1) $\left(\frac{3}{p}\right) = 1$, すなわち $p \equiv 1, 11 \pmod{12}$ のときは $p = \pm\pi\pi'$ である. ただし π と π' は同伴でない素元である. また $\pi = a + b\sqrt{3}$ とすると $a^2 - 3b^2 = \pm p$ が成り立つ.

(2) $\left(\frac{3}{p}\right) = -1$, すなわち $p \equiv 5, 7 \pmod{12}$ のとき p は素元である.

(3) $\left(\frac{3}{p}\right) = 0$, すなわち $p = 3$ のとき $3 = (\sqrt{3})^2$ である. ここで $\sqrt{3}$ は素元である.

3章　Euclid 体

この章では Euclid 体について考察する. 整数環がノルムに関して Euclid 整域である 2 次体を Euclid 体という. 特に実 2 次体, 虚 2 次体である場合をそれぞれ実 Euclid 体, 虚 Euclid 体という. また整数環が一意分解整域である 2 次体を単純体という. Euclid 体は単純体であるが逆は成り立たない. 2 次体 $\mathbb{Q}(\sqrt{m})$ が Euclid 体となるのは m が

$$-11,\ -7,\ -3,\ -2,\ -1,\ 2,\ 3,\ 5,\ 6,\ 7,\ 11,\ 13,\ 17,\ 19,\ 21,\ 29,\ 33,\ 37,\ 41,\ 57,\ 73$$

の 21 個の場合に限ることが 1950 年 Chatland と Davenport によって証明された. §3.1 では Euclid 体, 単純体を定義し, 2 次体 $\mathbb{Q}(\sqrt{m})$ が虚 Euclid 体となるのは m が $-1, -2, -3, -7, -11$ の場合に限ることを証明する. §3.2 では $m \equiv 2, 3 \pmod 4$ となる実 Euclid 体 $\mathbb{Q}(\sqrt{m})$ が有限個であることを示し, Chatland と Davenport のリストにあるいくつかの m について $\mathbb{Q}(\sqrt{m})$ が Euclid 体であることを確かめる.

3.1　Euclid 体

2 次体 $\mathbb{Q}(\sqrt{m})$ の整数環 O_m において次の条件がみたされているとする.

- 任意の $\alpha(\neq 0), \beta$ に対して $\beta = \alpha q + r$, $|\mathcal{N}(r)| < |\mathcal{N}(\alpha)|$ となる q, r が存在する.

このとき写像 ϕ を

$$\phi : O_m \ni \alpha \longmapsto |\mathcal{N}(\alpha)| \in \mathbb{N} \cup \{0\}$$

と定めると $\alpha \neq 0$ のとき $\mathcal{N}(\alpha) \neq 0$ であることより, 条件

(1)　$\alpha \neq 0$ ならば $\phi(\alpha) > 0$

(2)　O_m の任意の元 $\alpha(\neq 0), \beta$ に対して $\beta = \alpha q + r, \quad \phi(r) < \phi(\alpha)$ をみたす $q, r \in O_m$ が存在する.

をみたす. 従って O_m は Euclid 整域となる. 以下, このような O_m はノルムに関して Euclid 整域であるということにする.

O_m がノルムに関して Euclid 整域であるとき $\mathbb{Q}(\sqrt{m})$ を Euclid 体という. 特に $m<0$ のとき虚 Euclid 体, $m>0$ のとき実 Euclid 体という. 定理 1.53 より Euclid 整域は一意分解整域であるから Euclid 体は単純体である.

定理 3.1 *Euclid* 体は単純体である.

定理 3.2 $\mathbb{Q}(\sqrt{m})$ が *Euclid* 体であることと次の条件が成り立つこととは同値である.

O_m の任意の元 $\alpha(\neq 0), \beta$ に対して $\left|\mathcal{N}\left(\frac{\beta}{\alpha}-q\right)\right|<1$ をみたす $q\in O_m$ が存在する.

Proof　明らかに次の 2 条件は同値である.

- 任意の $\alpha(\neq 0)$, β に対して $\beta=\alpha q+r$, $|\mathcal{N}(r)|<|\mathcal{N}(\alpha)|$ となる q, r が存在する.
- ∘ 任意の $\alpha(\neq 0)$, β に対して $|\mathcal{N}(\beta-\alpha\, q)|<|\mathcal{N}(\alpha)|$ となる q が存在する.

また O_m の任意の元 $\alpha(\neq 0)$, β, q に対して

$$\left|\mathcal{N}\left(\frac{\beta}{\alpha}-q\right)\right|<1 \iff |\mathcal{N}(\beta-\alpha\, q)|<|\mathcal{N}(\alpha)|$$

が成り立つことから, 上の 2 条件は次の条件に同値である.

- ⊙ 任意の $\alpha(\neq 0)$, β に対して $\left|\mathcal{N}\left(\frac{\beta}{\alpha}-q\right)\right|<1$ となる q が存在する.

以上から定理の成り立つことは明らかである. ∎

補題 3.3 $\mathbb{Q}(\sqrt{m})$ が虚 *Euclid* 体で $m\equiv 2,3 \pmod 4$ ならば $m=-1,-2$ である.

Proof　補題 3.2 より $\mathbb{Q}(\sqrt{m})$ が虚 Euclid 体となる条件は, 任意の $\alpha(\neq 0)$, β に対して $\left|\mathcal{N}\left(\frac{\beta}{\alpha}-\kappa\right)\right|<1$ をみたす $\kappa\in O_m$ が存在することである. ここで

$$\frac{\beta}{\alpha}=a+b\sqrt{m}\quad(a,b\in\mathbb{Q}),\qquad \kappa=r+s\sqrt{m}\quad(r,s\in\mathbb{Z})$$

とおく.

$$\mathcal{N}\Big(\frac{\beta}{\alpha}-\kappa\Big)=\mathcal{N}\Big((a-r)+(b-s)\sqrt{m}\Big)=(a-r)^2+\mid m\mid(b-s)^2$$

であるから $\mathbb{Q}(\sqrt{m})$ が虚 Euclid 体となることと $(a-r)^2+\mid m \mid (b-s)^2<1$ をみたす有理整数 r,s が存在することとは同値である.

$\mid a-r \mid \leq \frac{1}{2},\ \mid b-s \mid \leq \frac{1}{2}$ となるように $r,s\in\mathbb{Z}$ を選ぶと

$$\mathcal{N}\Big(\frac{\beta}{\alpha}-\kappa\Big)=(a-r)^2+\mid m \mid (b-s)^2\leq\Big(\frac{1}{2}\Big)^2+\mid m \mid \Big(\frac{1}{2}\Big)^2=\frac{1}{4}+\frac{\mid m \mid}{4}$$

となる. 従って $m=-1,-2$ のときは $\dfrac{1}{4}+\dfrac{\mid m \mid}{4}<1$ となるから $\mathbb{Q}(\sqrt{m})$ は Euclid 体である.

一方 $m<-2$ のときは $m\equiv 2,3 \pmod 4$ より $m\leq -5$ となる. ここで $\beta=1+\sqrt{m}$, $\alpha=2$ とすると $\dfrac{\beta}{\alpha}=\dfrac{1}{2}+\dfrac{1}{2}\sqrt{m}$ となる. $|m|\geq 5$ であることから任意の $r,s\in\mathbb{Z}$ に対して

$$\Big(\frac{1}{2}-r\Big)^2+\mid m \mid \Big(\frac{1}{2}-s\Big)^2\geq\Big(\frac{1}{2}\Big)^2+\mid m \mid \Big(\frac{1}{2}\Big)^2=\frac{1}{4}+\frac{\mid m \mid}{4}>1$$

となる. 従って $m<-2$ のとき $\mathbb{Q}(\sqrt{m})$ は Euclid 体でない. 以上で補題が示された. ∎

補題 3.4 $\mathbb{Q}(\sqrt{m})$ が虚 *Euclid* 体で $m\equiv 1 \pmod 4$ ならば $m=-3,-7,-11$ である.

Proof　補題 3.3 と同様に任意の $\alpha(\neq 0),\beta$ に対して $\left|\mathcal{N}\left(\frac{\beta}{\alpha}-\kappa\right)\right|<1$ をみたす $\kappa\in O_m$ が存在するかどうかが問題である. ここで

$$\frac{\beta}{\alpha}=a+b\sqrt{m}\quad(a,b\in\mathbb{Q}),\qquad \kappa=r+s\,\frac{1+\sqrt{m}}{2}\quad(r,s\in\mathbb{Z})$$

とおくと

$$\mathcal{N}\left(\frac{\beta}{\alpha}-\kappa\right)=\mathcal{N}\left(\left(a-r-\frac{s}{2}\right)+\left(b-\frac{s}{2}\right)\sqrt{m}\right)=\left(a-r-\frac{s}{2}\right)^2+\frac{|m|}{4}(2b-s)^2$$

となる. $\mid 2b-s \mid \leq \frac{1}{2},\ \mid a-\frac{s}{2}-r \mid \leq \frac{1}{2}$ となるように $r,s\in\mathbb{Z}$ を選ぶと $m=-3,-7,-11$ のときは

$$\mathcal{N}\Big(\frac{\beta}{\alpha}-\kappa\Big)\leq\Big(\frac{1}{2}\Big)^2+\frac{\mid m \mid}{4}\Big(\frac{1}{2}\Big)^2=\frac{1}{4}+\frac{\mid m \mid}{16}<1$$

が成り立つ. 従って $m=-3,-7,-11$ のとき $\mathbb{Q}(\sqrt{m})$ は Euclid 体である.

一方 $m<-11$ のときは $m\equiv 1 \pmod 4$ であるから $m\leq -15$ となり, $\beta=\frac{1+\sqrt{m}}{2}$, $\alpha=2$ とすると $a=b=\frac{1}{4}$ より

$$\mathcal{N}\Big(\frac{\beta}{\alpha}-\kappa\Big)=\Big(\frac{1}{4}-r-\frac{s}{2}\Big)^2+\frac{\mid m \mid}{4}\Big(2\cdot\frac{1}{4}-s\Big)^2$$

が成り立つ. ここで

$$\Big|\,\frac{1}{2}-s\,\Big|\geq\frac{1}{2},\quad \Big|\,\frac{1}{4}-r-\frac{s}{2}\,\Big|=\frac{|\,1-2(2r+s)\,|}{4}\geq\frac{1}{4}$$

であることから

$$\mathcal{N}\Big(\frac{\beta}{\alpha}-\kappa\Big)\geq\Big(\frac{1}{4}\Big)^2+\frac{|\,m\,|}{4}\Big(\frac{1}{2}\Big)^2=\frac{1}{16}+\frac{|\,m\,|}{16}\geq 1$$

となる. 従って $m<-11$ のとき $\mathbb{Q}(\sqrt{m})$ は Euclid 体でない. ∎

補題 3.3 と補題 3.4 より次の定理が得られる

定理 3.5 $\mathbb{Q}(\sqrt{m})$ が虚 *Euclid* 体になるのは $m=-1,-2,-3,-7,-11$ のときに限る.

3.2 実 Euclid 体

$\mathbb{Q}(\sqrt{m})$ が Euclid 体となる m が 21 個に限ることはすでに述べたが, ここでは Chatland と Davenport のリストの中の $m=2,3,5,6,7,13,17,21,29$ について $\mathbb{Q}(\sqrt{m})$ が Euclid 体であることを確かめる. また $m\equiv 2,3 \pmod 4$ をみたす実 Euclid 体 $\mathbb{Q}(\sqrt{m})$ が有限個であることを示す. なお実 2 次体の場合はノルムが負になる場合があるので注意されたい.

補題 3.6 $m=2,3,6,7$ のとき $\mathbb{Q}(\sqrt{m})$ は実 *Euclid* 体である.

Proof　$m>0$, $m\equiv 2,3 \pmod 4$ として, $\mathbb{Q}(\sqrt{m})$ が Euclid 体でないと仮定する. 以下 $m\geq 8$ であることを示そう. 仮定より条件

- 任意の $\alpha(\neq 0)$, β に対して $\left|\mathcal{N}\left(\frac{\beta}{\alpha}-\kappa\right)\right|<1$ をみたす $\kappa\in O_m$ が存在する.

は成り立たない. 従って, ある $\alpha(\neq 0)$, β が存在して $\frac{\beta}{\alpha}=a+b\sqrt{m}$ とおくと, 任意の $\kappa=r+s\sqrt{m}$ に対して

$$\Big|\mathcal{N}\Big(\frac{\beta}{\alpha}-\kappa\Big)\Big|=|\,(a-r)^2-m(b-s)^2\,|\geq 1$$

が成り立つ. まず

$$0\leq a\leq\frac{1}{2},\qquad 0\leq b\leq\frac{1}{2}$$

とできることを示そう. β を $\beta-\alpha\,(x+y\sqrt{m})$ に置き換えると

$$\frac{\beta-\alpha\,(x+y\sqrt{m})}{\alpha}=\frac{\beta}{\alpha}-(x+y\sqrt{m})=(a-x)+(b-y)\sqrt{m}$$

となる. x, y として適当な整数を選べば $\beta-\alpha\,(x+y\sqrt{m})\in O_m$ であり $0\le|a|\le\frac{1}{2}, 0\le|b|\le\frac{1}{2}$ となるようにできる. 次に $a<0$ ならば β を $-\beta$ に置き換えて $0\le a\le\frac{1}{2}$ が成り立つようにできる. ここで $b<0$ ならば α, β を共役で置き換えれば $0\le b\le\frac{1}{2}$ が成り立つようにできる. これらの操作により, 任意の $\kappa=r+s\sqrt{m}$ に対して

$$\left|\mathcal{N}\Big(\frac{\beta}{\alpha}-\kappa\Big)\right| =|\,(a-r)^2-m(b-s)^2\,|\ge 1$$

が成り立つことに変わりはない. 従って以下, $0\le a\le\frac{1}{2}$, $0\le b\le\frac{1}{2}$ がみたされているものとする. ここで

$$\begin{aligned} P(r,s) &: (a-r)^2-m(b-s)^2\ge 1 \quad \big(\Longleftrightarrow\quad (a-r)^2\ge 1+m(b-s)^2\,\big)\\ Q(r,s) &: (a-r)^2-m(b-s)^2\le -1 \quad \big(\Longleftrightarrow\quad m(b-s)^2\ge 1+(a-r)^2\,\big)\end{aligned}$$

とおく. 仮定より任意の $r,s\in\mathbb{Z}$ に対して $P(r,s)$, $Q(r,s)$ のいずれかが成り立つ. 特に

$$\begin{aligned} &① \quad P(0,0) : a^2\ge 1+mb^2\,, && Q(0,0): mb^2\ge 1+a^2\\ &② \quad P(1,0) : (a-1)^2\ge 1+mb^2\,, && Q(1,0): mb^2\ge 1+(a-1)^2\\ &③ \quad P(-1,0) : (a+1)^2\ge 1+mb^2\,, && Q(-1,0): mb^2\ge 1+(a+1)^2\end{aligned}$$

とおくと ①〜③ の各組について少なくとも一方が成り立つ.

$a=b=0$ とすると ① の両方が成り立たない. 従って a または b のどちらか一方は 0 でない.

$b=0$ とすると $0<a\le\frac{1}{2}$ であるから ① の両方とも成り立たない. 従って $b\ne 0$ である.

$a=0$ とすると $0<b\le\frac{1}{2}$ であるから $P(-1,0)$ が成り立たない. 従って $Q(-1,0)$ が成り立つ. これより $mb^2\ge 2$ が得られるが $0<b\le\frac{1}{2}$ であることから $m\ge 8$ が導かれる. 従って以下 a, b 共に 0 でないとして $m\ge 8$ を示せばよい.

$0<a,b\le\frac{1}{2}$ より $P(0,0)$, $P(1,0)$ が成り立たない. 従って $Q(0,0)$, $Q(1,0)$ が成り立つ.

ここで $P(-1,0)$, $Q(-1,0)$ のいずれが成り立つかで場合分けすることにする.

$P(-1,0)$ が成り立つとする. このとき $Q(0,0)$, $Q(1,0)$ とあわせて次を得る.

$$mb^2\ge 1+a^2\,,\qquad mb^2\ge 1+(a-1)^2\,,\qquad (a+1)^2\ge 1+mb^2$$

第 2 式と第 3 式より

$$(a+1)^2 \geq 1+mb^2 \geq 2+(a-1)^2 \implies (a+1)^2 \geq 2+(a-1)^2 \implies a \geq \frac{1}{2}$$

よって $a=\frac{1}{2}$ を得る. これを上式に代入すると

$$\Big(\frac{3}{2}\Big)^2 \geq 1+mb^2 \geq 2+\Big(\frac{1}{2}\Big)^2 \implies \frac{5}{4} \geq mb^2 \geq \frac{5}{4} \implies mb^2=\frac{5}{4}$$

となるがこれは起こり得ない. なぜならば $b=\frac{q}{p},\ (p,q)=1$ とおくと

$$m\Big(\frac{q}{p}\Big)^2=\frac{5}{4} \implies 4mq^2=5p^2 \implies q^2 \mid 5,\ q=1$$

となり, $4m=5p^2$ より $p=2$, $m=5$ が導かれるが, これは $m \equiv 2,3 \pmod 4$ に矛盾するからである. よって $P(-1,0)$ は起こり得ない.

$Q(-1,0)$ が成り立つとする. このとき $Q(0,0)$, $Q(1,0)$ とあわせて次を得る.

$$mb^2 \geq 1+a^2\,, \qquad mb^2 \geq 1+(a-1)^2\,, \qquad mb^2 \geq 1+(a+1)^2$$

ここで $0<a\leq\frac{1}{2}$ より

$$mb^2 \geq 1+(a+1)^2 > 2 \implies \frac{m}{4} \geq mb^2 > 2 \implies m>8$$

を得る. 以上で $\mathbb{Q}(\sqrt{m})$ が Euclid 体でないときは $m \geq 8$ の成り立つことが示された. 従って $m=2,3,6,7$ のとき $\mathbb{Q}(\sqrt{m})$ は Euclid 体である. ∎

補題 3.7 $m=5,13,17,21,29$ のとき $\mathbb{Q}(\sqrt{m})$ は実 *Euclid* 体である.

Proof　$m>0$, $m \equiv 1 \pmod 4$ として, $\mathbb{Q}(\sqrt{m})$ が Euclid 体でないと仮定する. $m \geq 32$ であることを示せばよい. 仮定より条件

- 任意の $\alpha(\neq 0)$, β に対して $\left|\mathcal{N}\left(\frac{\beta}{\alpha}-\kappa\right)\right|<1$ をみたす $\kappa \in O_m$ が存在する.

は成り立たない. 従って, ある $\alpha(\neq 0)$, β が存在して $\frac{\beta}{\alpha}=a+b\sqrt{m}$ とおくと, 任意の $\kappa=r+s\,\frac{1+\sqrt{m}}{2}$ に対して

$$\Big|\mathcal{N}\Big(\frac{\beta}{\alpha}-\kappa\Big)\Big| = \Big|\ \Big(a-r-\frac{s}{2}\Big)^2-\frac{m}{4}(2b-s)^2\ \Big| \geq 1$$

が成り立つ. まず

$$0 \leq a \leq \frac{1}{2}\,, \qquad 0 \leq b \leq \frac{1}{4}$$

としてよいことを示そう. β を $\beta-\alpha\,(x+y\,\frac{1+\sqrt{m}}{2})$ に置き換えると

$$\frac{\beta-\alpha\,(x+y\,\frac{1+\sqrt{m}}{2})}{\alpha}=\frac{\beta}{\alpha}-\left(x+y\,\frac{1+\sqrt{m}}{2}\right)=\left(a-x-\frac{y}{2}\right)+\left(b-\frac{y}{2}\right)\sqrt{m}$$

となる. 従って有理整数 y を適当に選び, 次いで x を適当に選ぶことにより

$$0\le|a|\le\frac{1}{2}\,,\qquad 0\le|b|\le\frac{1}{4}$$

が成り立つようにできる. 次に $a<0$ ならば β を $-\beta$ に置き換えて $0\le a\le\frac{1}{2}$ が成り立つようにできる. ここで $b<0$ ならば α,β を共役で置き換えれば $0\le b\le\frac{1}{4}$ が成り立つようにできる. これらの操作により, 任意の $\kappa=r+s\,\frac{1+\sqrt{m}}{2}$ に対して

$$\left|\mathcal{N}\Big(\frac{\beta}{\alpha}-\kappa\Big)\right|=\left|\,\Big(a-r-\frac{s}{2}\Big)^2-\frac{m}{4}(2b-s)^2\,\right|\ge 1$$

が成り立つことに変わりがない. 従って以下, $0\le a\le\frac{1}{2}$, $0\le b\le\frac{1}{4}$ がみたされているものとする.

ここで

$$\begin{aligned}
P(r,s)\ &:\ \Big(a-r-\frac{s}{2}\Big)^2-\frac{m}{4}(2b-s)^2\ge 1\quad\left(\Longleftrightarrow\quad\Big(a-r-\frac{s}{2}\Big)^2\ge 1+\frac{m}{4}(2b-s)^2\right)\\
Q(r,s)\ &:\ \Big(a-r-\frac{s}{2}\Big)^2-\frac{m}{4}(2b-s)^2\le -1\quad\left(\Longleftrightarrow\quad\frac{m}{4}(2b-s)^2\ge 1+\Big(a-r-\frac{s}{2}\Big)^2\right)
\end{aligned}$$

とおく. 仮定より任意の $r,s\in\mathbb{Z}$ に対して $P(r,s)$, $Q(r,s)$ のいずれかが成り立つ. 特に

$$\begin{aligned}
&①\quad P(0,0)\ :\ a^2\ge 1+mb^2\,,\qquad Q(0,0):mb^2\ge 1+a^2\\
&②\quad P(1,0)\ :\ (a-1)^2\ge 1+mb^2\,,\qquad Q(1,0):mb^2\ge 1+(a-1)^2\\
&③\quad P(-1,0)\ :\ (a+1)^2\ge 1+mb^2\,,\qquad Q(-1,0):mb^2\ge 1+(a+1)^2
\end{aligned}$$

とおくと ①〜③ の各組について少なくとも一方が成り立つ.

$a=b=0$ とすると ① の両方とも成り立たない. 従って a または b の一方は 0 でない.

$b=0$ とすると ① の両方とも成り立たない. 従って $b\neq 0$ である.

$a=0$ とすると $P(-1,0)$ が成り立たないから $Q(-1,0)$ が成り立ち, $mb^2\ge 2$ を得る. これより $\frac{m}{16}\ge mb^2\ge 2$, すなわち $m\ge 32$ が導かれる. 従って, 以下 a, b 共に 0 でないとして $m\ge 32$ を示せばよい.

$0<a\le\frac{1}{2}$, $0<b\le\frac{1}{4}$ より $P(0,0)$, $P(1,0)$ が成り立たない. 従って $Q(0,0)$, $Q(1,0)$ が成り立つ.

ここで $P(-1,0)$, $Q(-1,0)$ のいずれが成り立つかで場合分けすることにする.

$P(-1,0)$ が成り立つとする. このとき $Q(0,0)$, $Q(1,0)$ とあわせて次を得る.

$$mb^2 \geq 1+a^2\,, \qquad mb^2 \geq 1+(a-1)^2\,, \qquad (a+1)^2 \geq 1+mb^2$$

第2式と第3式より

$$(a+1)^2 \geq 1+mb^2 \geq 2+(a-1)^2 \implies (a+1)^2 \geq 2+(a-1)^2 \implies a \geq \frac{1}{2}$$

よって $a=\frac{1}{2}$ を得る. これを上式に代入すると

$$\left(\frac{3}{2}\right)^2 \geq 1+mb^2 \geq 2+\left(\frac{1}{2}\right)^2 \implies \frac{5}{4} \geq mb^2 \geq \frac{5}{4} \implies mb^2=\frac{5}{4}$$

となるがこれは起こり得ない. なぜならば $b=\frac{q}{p},\ (p,q)=1$ とおくと

$$m\left(\frac{q}{p}\right)^2=\frac{5}{4} \implies 4mq^2=5p^2 \implies q^2 \mid 5,\ q=1$$

となり, $4m=5\,p^2$ より $p=2$, $b=\frac{1}{2}$ が導かれ $0 \leq b \leq \frac{1}{4}$ に矛盾するからである. よって $P(-1,0)$ は起こり得ない.

$Q(-1,0)$ が成り立つとする. このとき $Q(0,0)$, $Q(1,0)$ とあわせて次を得る.

$$mb^2 \geq 1+a^2\,, \qquad mb^2 \geq 1+(a-1)^2\,, \qquad mb^2 \geq 1+(a+1)^2$$

ここで $0<a \leq \frac{1}{2}$ より

$$mb^2 \geq 1+(a+1)^2 > 2 \implies \frac{m}{16} \geq mb^2 > 2 \implies m > 32$$

を得る. 以上で $\mathbb{Q}(\sqrt{m})$ が Euclid 体でないときは $m \geq 32$ の成り立つことが示された. 従って $m=5,13,17,21,29$ のとき $\mathbb{Q}(\sqrt{m})$ は Euclid 体である. ∎

補題 3.6 と補題 3.7 より次の定理が得られる

定理 3.8 $m=2,3,5,6,7,13,17,21,29$ のとき $\mathbb{Q}(\sqrt{m})$ は実 *Euclid* 体である.

補題 3.9 実数 a, b が $a-b>2$ をみたすならば $b<t<a$ となる奇数 t が存在する.

Proof　背理法で示す. $b<t<a$ となる奇数 t が存在しないと仮定する. $a-b>2$ より $b<s<a$ をみたす整数 s が存在する. 仮定より s は偶数である. このとき $s+1 \geq a$, $s-1 \leq b$ となることから $a-b \leq 2$ となり仮定に矛盾する. よって補題が示された. ∎

補題 3.10 自然数 n について次がなり立つ.

(1) $n \geq 45$ のとき $2n < t^2 < 3n$ をみたす奇数 t が存在する.

(2) $n \geq 100$ のとき $5n < t^2 < 6n$ をみたす奇数 t が存在する.

Proof $\sqrt{3} - \sqrt{2} = 0.317... > 0.3$, $\sqrt{45} = 6.708...$ であるから $n \geq 45$ のときは

$$\sqrt{3n} - \sqrt{2n} = (\sqrt{3} - \sqrt{2})\sqrt{n} > 0.3 \cdot \sqrt{45} = 2.01... > 2$$

が成り立つ. 従って $\sqrt{3n} - \sqrt{2n} > 2$ となり補題 3.9 より $\sqrt{2n} < t < \sqrt{3n}$ をみたす奇数 t が存在する. このとき $2n < t^2 < 3n$ が成り立つ.

$\sqrt{6} - \sqrt{5} = 0.213... > 0.2$ であるから $n \geq 100$ のときは

$$\sqrt{6n} - \sqrt{5n} = (\sqrt{6} - \sqrt{5})\sqrt{n} > 0.2 \cdot \sqrt{100} = 2$$

が成り立つ. 従って $\sqrt{6n} - \sqrt{5n} > 2$ となり $\sqrt{5n} < t < \sqrt{6n}$ をみたす奇数 t が存在する. このとき $5n < t^2 < 6n$ が成り立つ. ∎

定理 3.11 $m \equiv 2, 3 \pmod 4$ をみたす実 *Euclid* 体 $\mathbb{Q}(\sqrt{m})$ は有限個である.

Proof $m \equiv 2, 3 \pmod 4$ で $\mathbb{Q}(\sqrt{m})$ が Euclid 体であると仮定する. 以下 $m < 100$ であることを示そう. これより定理が導かれることは明らかである.

O_m の任意の元 $\alpha(\neq 0)$, β に対して $\frac{\beta}{\alpha} = a + b\sqrt{m}$ とおくと, ある $\kappa = r + s\sqrt{m} \in O_m$ が存在して

$$\left|\mathcal{N}\Big(\frac{\beta}{\alpha} - \kappa\Big)\right| = \left|\mathcal{N}\Big((a-r) + (b-s)\sqrt{m}\Big)\right| = |\,(a-r)^2 - m(b-s)^2\,| < 1$$

が成り立つ. ここで任意の有理整数 t に対して $\alpha = m$, $\beta = t\sqrt{m}$ とおくと $a = 0$, $b = \frac{t}{m}$ となる. このとき

$$\left|r^2 - m\Big(\frac{t}{m} - s\Big)^2\right| < 1 \quad \text{すなわち} \quad |\,(ms - t)^2 - mr^2\,| < m$$

をみたす $r, s \in \mathbb{Z}$ が存在する. ここで $(ms-t)^2 - mr^2 \equiv t^2 \pmod m$ であるから $z^2 = (ms-t)^2$ とおけば $z^2 - mr^2 \equiv t^2 \pmod m$ を得る. 以上から任意の有理整数 t に対して

$$z^2 - mr^2 \equiv t^2 \pmod m, \qquad |\,z^2 - mr^2\,| < m$$

をみたす有理整数 z, r の存在することが示された.

以下 $m \geq 100$ と仮定し, 上の条件がみたされたとして矛盾を導く. これより $\mathbb{Q}(\sqrt{m})$ が Euclid 体であれば $m < 100$ でなければならないことがわかる.

まず $m \equiv 3 \pmod 4$ とする. 補題 3.10 より $5m < t^2 < 6m$ をみたす奇数 t が存在する. ここで $t^2 = 5m + k$ とおく. $0 < k < m$ である.

$$z^2 - mr^2 \equiv t^2 \equiv k \pmod m \qquad \text{かつ} \qquad |\, z^2 - mr^2 \,| < m$$

より $z^2 - mr^2 = k$ または $k - m$ である. これより

$$z^2 - mr^2 = t^2 - 5m \quad \text{または} \quad z^2 - mr^2 = t^2 - 6m$$

が得られるので

$$t^2 - z^2 = m(5 - r^2) \qquad \text{または} \quad t^2 - z^2 = m(6 - r^2) \qquad \cdots\cdots \text{①}$$

が成り立つ. ここで 8 を法として考えると t が奇数であることから

$$t^2 \equiv 1, \quad z^2 \equiv 0, 1, 4, \quad r^2 \equiv 0, 1, 4, \quad m \equiv 3, 7 \pmod 8$$

となり, $t^2 - z^2 \equiv 0, 1, 5 \pmod 8$ を得る. 一方

$$5 - r^2 \equiv 1, 4, 5\,, \qquad 6 - r^2 \equiv 2, 5, 6 \pmod 8$$

であることから

$$m(5 - r^2) \equiv 3, 4, 7\,, \qquad m(6 - r^2) \equiv 2, 3, 6, 7 \pmod 8$$

となり ① に矛盾する.

次に $m \equiv 2 \pmod 4$ とする. 補題 3.10 より $2m < t^2 < 3m$ をみたす奇数 t が存在する. ここで $t^2 = 2m + k$ とおく. $0 < k < m$ である.

$$z^2 - mr^2 \equiv t^2 \equiv k \pmod m \qquad \text{かつ} \qquad |\, z^2 - mr^2 \,| < m$$

より $z^2 - mr^2 = k$ または $k - m$ である. これより

$$z^2 - mr^2 = t^2 - 2m \qquad \text{または} \qquad z^2 - mr^2 = t^2 - 3m$$

が得られるので

$$t^2 - z^2 = m(2 - r^2) \qquad \text{または} \qquad t^2 - z^2 = m(3 - r^2) \quad \cdots\cdots\cdots \text{②}$$

が成り立つ. ここで 8 を法として考えると

$$t^2 \equiv 1, \quad z^2 \equiv 0, 1, 4, \quad r^2 \equiv 0, 1, 4, \quad m \equiv 2, 6 \pmod 8$$

より $t^2 - z^2 \equiv 0, 1, 5 \pmod 8$ を得る. 一方

$$2 - r^2 \equiv 1, 2, 6\,, \qquad\qquad 3 - r^2 \equiv 2, 3, 7 \pmod 8$$

であることから

$$m(2 - r^2) \equiv 2, 4, 6\,, \qquad\qquad m(3 - r^2) \equiv 2, 4, 6 \pmod 8$$

となり ② に矛盾する. 以上で定理が証明された. ∎

4章　2次体のイデアル

この章では2次体のイデアル論について述べる．2次体 $\mathbb{Q}(\sqrt{m})$ の整数環 O_m において 0 でないイデアルが素イデアルの積として一意的に分解できること, 有理素数 p で生成される O_m の単項イデアル (p) の素イデアル分解が Artin 記号により判定できることなどを証明する.

§4.1 では O_m の 0 でないイデアルに標準的基底が存在すること, および 0 でないイデアルが階数 2 の自由 $\mathbb{Z}$ 加群であることを示す. §4.2 では標準的基底からイデアルのノルムを求め, 単項イデアルのノルムが生成元のノルムの絶対値に一致することを示す. §4.3 では 0 でないイデアルが素イデアルの積として一意的に分解できること, すなわち O_m が Dedekind 整域であることを示す. また O_m が単項イデアル整域であることと一意分解整域であることとが同値であることを示す. §4.4 では有理素数 p で生成される O_m の単項イデアル (p) の素イデアル分解が 3 つの型に分類できること, Artin 記号により統一的に述べられることなどを示す．また (p) を割る素イデアルの標準的基底が明示されるが, これは 5 章での類数計算に用いられる.

4.1　イデアルの基底

定理 2.8 (p.26) より 2 次体 $\mathbb{Q}(\sqrt{m})$ の整数環 O_m は $1, \omega$ を基底とする階数 2 の自由 $\mathbb{Z}$ 加群である. 従って O_m の元は $a + b\omega$, $a, b \in \mathbb{Z}$, と一意的に表される. ただし ω は次のように与えられる.

$$\omega = \begin{cases} \sqrt{m} & m \equiv 2, 3 \pmod 4 \\ \dfrac{1+\sqrt{m}}{2} & m \equiv 1 \pmod 4 \end{cases}$$

O_m の 0 でないイデアル A は O_m の部分加群だから, 定理 1.54 より, 階数が 2 以下の自由 $\mathbb{Z}$ 加群である. ここで $A \ni a \neq 0$ に対して $a, a\omega$ は明らかに $\mathbb{Z}$ 上1次独立である. 従って A の階数は 2 である. 以上から次の定理を得る.

定理 4.1 O_m の 0 でないイデアルは階数 2 の自由 $\mathbb{Z}$ 加群である.

補題 4.2 A を O_m の 0 でないイデアルとする. このとき次がなり立つ.

(1) A は自然数を含む. A に含まれる自然数の中で最小のものを a とすると A に含まれる全ての有理整数は a の倍数である.

(2) A は $x+y\omega,\ y\neq 0,$ の形の元を含む. そのような元の中で y の値が最小の自然数となるものを $b+c\omega$ とすると任意の A の元 $x+y\,\omega$ に対して $c \mid y$ が成り立つ.

Proof (1) $A \ni \alpha(\neq 0)$ とする. $n=\mathcal{N}(\alpha)=\alpha\alpha'$ とおく. 明らかに $n\in A,\ n\neq 0$ であるが, 定理2.3 より $n\in A\cap\mathbb{Z}$ が成り立つ. ここで $\pm n\in A$ であるから A は自然数を含む.

A の中の最小の自然数を a とする. このとき, 任意の $\ell\in A\cap\mathbb{Z}$ に対して $\ell=aq+r,$ $0\leq r<a,$ となる $q,r\in\mathbb{Z}$ が存在する. ここで $aq\in A$ より $r\in A$ となり, a の選び方から $r=0$ が得られる. 従って $a \mid \ell$ が成り立つ. ゆえに A に含まれる全ての有理整数は a の倍数である.

(2) (1) で定まる a に対して $a\omega\in A$ だから A は $x+y\omega,\ y\neq 0,$ の形の元を含む. このような元の中で y の値が最小の自然数となるものを $b+c\omega$ とおく. このとき 任意の $x+y\omega\in A$ に対し $y=cq+r,\ 0\leq r<c$ とおくと

$$x+y\omega-q(b+c\omega)=x-qb+(y-qc)\omega=x-qb+r\omega\in A$$

となるが, c の選び方より $r=0$ である. よって $c \mid y$ が得られた. ∎

補題 4.3 補題4.2で定まる $\{a,b+c\omega\}$ はイデアル A の $\mathbb{Z}$ 基底をなす.

Proof $a\in\mathbb{Q},\ b+c\omega\notin\mathbb{Q}$ より a と $b+c\omega$ は $\mathbb{Z}$ 上1次独立である. 従って A の任意の元が $a,\ b+c\omega$ の1次結合として表されることを示せばよい. 以下 $\beta=b+c\omega$ とおく.

任意の $\alpha=x+y\,\omega$ に対して補題4.2より $y=cq$ となる $q\in\mathbb{Z}$ が存在する. このとき $\alpha-q\,\beta=x-bq\in\mathbb{Z}$ となる. また $x-bq=ar$ となる $r\in\mathbb{Z}$ が存在するから $\alpha=a\,r+q\,\beta$ を得る. 従って A の任意の元は a と β の1次結合として表される. ゆえに $\{a,\beta\}$ は A の $\mathbb{Z}$ 基底である. ∎

定義 4.4 (標準的基底) O_m の 0 でないイデアル A に対して次の条件をみたす $\mathbb{Z}$ 基底 $\{a, b+c\omega\}$ を A の標準的基底といい $A=(a, b+c\omega)$ と表す.

(1) a, c は自然数, b は整数である.

(2) A に含まれる全ての有理整数は a の倍数である.

(3) 任意の A の元 $x+y\omega$ に対して $c \mid y$ が成り立つ.

以下, 特に断らない限りイデアルは2次体の整数環のイデアルである. 補題 4.2, 補題 4.3 より任意のイデアルは標準的基底をもつ.

補題 4.5 イデアル A の標準的基底 $(a, b+c\omega)$ について $c \mid a$, $c \mid b$ が成り立つ.

Proof $a\omega \in A$ であるから補題 4.2 より $c \mid a$ を得る. 次に $\omega=\sqrt{m}$ のときは

$$(b+c\omega)\,\omega = cm + b\omega$$

より $c \mid b$ を得る. また $\omega=\frac{1+\sqrt{m}}{2}$ のときは

$$(b+c\omega)\,\omega = \frac{m-1}{4}\,c + (b+c)\,\omega$$

となるから $c \mid (b+c)$ より $c \mid b$ が得られる. ∎

補題 4.5 よりイデアル A の標準的基底 $(a, b+c\omega)$ に対して $a=ca_0$, $b=cb_0$ とおくことができる. このとき

$$A=(a, b+c\omega)=c(a_0, b_0+\omega)$$

と表すことができる. これより A の元はすべて有理整数 c の倍数であることがわかる. ここで $A_0=(a_0, b_0+\omega)$ とおくと, $A=c\,A_0$ であり, A_0 の全ての元に共通の約数で有理整数であるものは ± 1 に限る.

定義 4.6 (原始的イデアル) 全ての元の約数で, 有理整数であるものが ± 1 のみであるイデアルを原始的イデアルという.

上述のことから次の定理を得る (証明略).

定理 4.7 すべてのイデアルは原始的イデアルの整数倍である.

補題 4.8 0 でないイデアル A の標準的基底 $(a, b+c\omega)$ について次がなり立つ.

(1) $0 \leq b < a$ となるような標準的基底が存在する.

(2) $-\frac{a}{2} \leq b < \frac{a}{2}$ となるような標準的基底が存在する.

Proof (1) a は自然数であるから除法の定理が適用できて $b = aq + b_1$, $0 \leq b_1 < a$, をみたす $q, b_1 \in \mathbb{Z}$ が定まる. ここで $b + c\omega$ を $b + c\omega - aq = b_1 + c\omega$ で置き換えた標準的基底 $(a, b_1 + c\omega)$ は $0 \leq b_1 < a$ をみたす. (2) も同様である. ∎

以上をまとめて次の定理を得る.

定理 4.9 0 でないイデアル A の標準的基底 $(a, b+c\omega)$ について次がなり立つ.

(1) A に含まれる有理整数はすべて a の倍数である.

(2) A に含まれる任意の元 $x + y\omega$ について $c \mid y$ が成り立つ.

(3) $c \mid a$, $c \mid b$ が成り立つ.

(4) $0 \leq b < a$ または $-\frac{a}{2} \leq b < \frac{a}{2}$ をみたすように b を選ぶことができる.

以下, 行列 M の行列式を $\det M$ と表す.

定理 4.10 η_1, η_2 をイデアル A の基底, $c_{ij} \in \mathbb{Z}$ とする. このとき次がなり立つ.

$$\begin{cases} \omega_1 = c_{11}\eta_1 + c_{12}\eta_2 \\ \omega_2 = c_{21}\eta_1 + c_{22}\eta_2 \end{cases} \text{が } A \text{ の基底である} \iff \det \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} = \pm 1$$

Proof ω_1, ω_2 が A の基底であるとする. このとき

$$\begin{bmatrix} \eta_1 \\ \eta_2 \end{bmatrix} = \begin{bmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{bmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix} = \begin{bmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{bmatrix} \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \begin{bmatrix} \eta_1 \\ \eta_2 \end{bmatrix}$$

をみたす有理整数 d_{ij} が存在するが η_1, η_2 が基底であることから

$$\begin{bmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{bmatrix} \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

を得る. 従って $\det \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} = \pm 1$ が成り立つ.

逆に $\det \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} = \pm 1$ が成り立つとすると

$$\begin{bmatrix} \eta_1 \\ \eta_2 \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}^{-1} \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}$$

となるが $\begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}^{-1}$ の成分は有理整数であるから ω_1, ω_2 は A を生成する. A の階数は 2 であるから ω_1, ω_2 は 1 次独立となり, A の基底である. ∎

4.2 イデアルのノルム

整数環 O_m の 0 でないイデアル A を法とする剰余類の個数を A のノルムといい $\mathcal{N}(A)$ と表す. 明らかに $\mathcal{N}(A) = 1$ であることと $A = O_m$ であることとは同値である.

定理 4.11 イデアル A の標準的基底を $(a_{11}, a_{21} + a_{22}\,\omega)$ とすると $\mathcal{N}(A) = det \begin{bmatrix} a_{11} & 0 \\ a_{21} & a_{22} \end{bmatrix} = a_{11}a_{22}$ が成り立つ.

Proof まず $b_1 + b_2\omega$, $0 \le b_1 < a_{11}$, $0 \le b_2 < a_{22}$, と表される $a_{11}a_{22}$ 個の元は A を法として互いに合同でないことを示そう.

$b_1 + b_2\omega \equiv b_1' + b_2'\omega \pmod{A}$ と仮定すると

$$b_1 + b_2\,\omega - (b_1' + b_2'\,\omega) = (b_1 - b_1') + (b_2 - b_2')\,\omega \equiv 0 \pmod{A}$$

を得る. ここで $b_2 - b_2'$ は a_{22} の倍数であるが $0 \le b_2, b_2' < a_{22}$ であるから $b_2 = b_2'$ が成り立つ. これより $b_1 - b_1' \in A$ を得るが $b_1 - b_1'$ は a_{11} の倍数であり, $0 \le b_1, b_1' < a_{11}$ であるから $b_1 = b_1'$ となる. ゆえに $b_1 + b_2\omega$, $0 \le b_1 < a_{11}$, $0 \le b_2 < a_{22}$, と表される $a_{11}a_{22}$ 個の元は A を法として互いに合同でない. 従って $\mathcal{N}(A) \ge a_{11}\,a_{22}$ が成り立つ.

次に任意に $\alpha = c_1 + c_2\omega \in O_m$ を選ぶと $c_2 = a_{22}q_2 + r_2$, $0 \le r_2 < a_{22}$, となる q_2, r_2 が定まる. このとき

$$\alpha - q_2(a_{21} + a_{22}\,\omega) = c_1 - a_{21}q_2 + (c_2 - a_{22}q_2)\omega = c_1' + r_2\omega$$

となる. ただし $c_1' = c_1 - a_{21}q_2$ である. 従って $\alpha \equiv c_1' + r_2\,\omega \pmod{A}$ $0 \le r_2 < a_{22}$, が得られた. さらに $c_1' = a_{11}q_1 + r_1$, $0 \le r_1 < a_{11}$ とすると

$$c_1' + r_2\omega - a_{11}q_1 = r_1 + r_2\,\omega$$

を得る. 以上から

$$\alpha \equiv c_1' + r_2\,\omega \equiv r_1 + r_2\,\omega \pmod{A}$$

を得る. ここで $0 \le r_1 < a_{11}, 0 \le r_2 < a_{22}$ であるから任意の剰余類は $b_1 + b_2\omega$, $0 \le b_1 < a_{11}$, $0 \le b_2 < a_{22}$, なる形の元を含むことが示された. よって $\mathcal{N}(A) \le a_{11}\,a_{22}$ が成り立ち, 前の結果とあわせると $\mathcal{N}(A) = a_{11}\,a_{22}$ が示された. ∎

定理 4.12 $a + b\omega$, $c + d\omega$ が A の基底であるとき $\mathcal{N}(A) = \left|\det \begin{bmatrix} a & b \\ c & d \end{bmatrix}\right|$ が成り立つ.

Proof　A の標準的基底の1つを $\eta_1 = a_{11}$, $\eta_2 = a_{21} + a_{22}\omega$ とすると定理 4.10 より

$$\begin{bmatrix} a + b\omega \\ c + d\omega \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \begin{bmatrix} \eta_1 \\ \eta_2 \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \begin{bmatrix} a_{11} & 0 \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} 1 \\ \omega \end{bmatrix}$$

をみたす $[c_{ij}]$ が存在する. ここで $\det[c_{ij}] = \pm 1$ である. 一方

$$\begin{bmatrix} a + b\omega \\ c + d\omega \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 \\ \omega \end{bmatrix}$$

と表されるから

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \begin{bmatrix} a_{11} & 0 \\ a_{21} & a_{22} \end{bmatrix}$$

が成り立つ. 従って

$$det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \pm a_{11}a_{22} = \pm\mathcal{N}(A)$$

より定理が得られる. ∎

単項イデアル (α) の任意の元は O_m の元 $a + b\,\omega$ を α 倍したものであるから $a\cdot\alpha + b\cdot\alpha\omega$ と表される. 従って α, $\alpha\,\omega$ は (α) を生成し, 明らかに1次独立であるから (α) の基底である.

定理 4.13 単項イデアル (α) に対して $\mathcal{N}((\alpha)) = \mid \mathcal{N}(\alpha) \mid$ が成り立つ.

Proof $\alpha = a + b\omega$ とおく. 上で述べたことから $\alpha, \alpha\,\omega$ が (α) の基底である. まず $m \equiv 2, 3 \pmod 4$ とすると $\omega = \sqrt{m}$ だから

$$\alpha = a + b\omega, \qquad \alpha\omega = a\omega + b\omega^2 = mb + a\omega$$

となるが定理 4.12 より

$$\mathcal{N}((\alpha)) = \left| det \begin{bmatrix} a & b \\ mb & a \end{bmatrix} \right| = \mid a^2 - mb^2 \mid = \mid \mathcal{N}(\alpha) \mid$$

が成り立つ. 次に $m \equiv 1 \pmod 4$ とする. $\omega = \frac{1+\sqrt{m}}{2}$ より

$$\alpha = a + b\omega, \qquad \alpha\omega = a\omega + b\omega^2 = \frac{m-1}{4}b + (a+b)\omega$$

となる. 従って

$$\mathcal{N}((\alpha)) = \left| det \begin{bmatrix} a & b \\ \frac{m-1}{4}b & a+b \end{bmatrix} \right| = \left| a^2 + ab + (1-m)\frac{b^2}{4} \right| = \mid \mathcal{N}(\alpha) \mid$$

を得る. よってこの場合も $\mathcal{N}((\alpha)) = \mid \mathcal{N}(\alpha) \mid$ が成り立つ. ∎

4.3 Dedekind 整域

この節では O_m の 0 でないイデアルが素イデアルの積として一意的に分解されること, すなわち O_m が Dedekind 整域であることを証明する. なおイデアルは, 特に断らない限り 0 でないものとする.

定理 4.14 (共役イデアル)

(1) イデアル A の各元の共役元全体の集合 $A' = \{\alpha' \mid \alpha \in A\}$ はイデアルである. A' を A の共役イデアルという. 特に単項イデアルについて $(\alpha)' = (\alpha')$ が成り立つ.

(2) イデアル A, B に対し $(AB)' = A'B'$ が成り立つ.

Proof (1) $\alpha', \beta' \in A'$ とする. $\alpha + \beta \in A$ に注意すれば $\alpha' + \beta' = (\alpha + \beta)' \in A'$ が成り立つ. また $\gamma \in O_m$ と $\alpha' \in A'$ に対して $\gamma\alpha' = (\gamma'\alpha)' \in A'$ が成り立つ. 従って A' はイデアルである. 単項イデアル (α) については

$$(\alpha)' = \{\alpha\, x \mid x \in O_m\}' = \{\alpha' x' \mid x' \in O_m\} = \{\alpha' y \mid y \in O_m\} = (\alpha')$$

が成り立つ.

(2) A は2元で生成されるから $A=(\alpha_1,\alpha_2)$, $B=(\beta_1,\beta_2)$ おくことができる. ここで $A'=(\alpha_1',\alpha_2')$, $B'=(\beta_1',\beta_2')$ であることに注意すれば, イデアルの積の定義から

$$(AB)'=(\alpha_1\beta_1,\alpha_1\beta_2,\alpha_2\beta_1,\alpha_2\beta_2)'=(\alpha_1'\beta_1',\alpha_1'\beta_2',\alpha_2'\beta_1',\alpha_2'\beta_2')=A'B'$$

が得られる. ∎

定理 4.15 任意のイデアル A に対して, ある整数 n が存在して $AA'=(n)$ と表すことができる.

Proof $A=0$ のときは $AA'=(0)$ より成り立つ. 以下 $A\neq 0$ として A の標準的基底を (α,β) とおく. α は自然数である. このとき $A'=(\alpha',\beta')$ であるから

$$AA'=(\alpha\alpha',\alpha\beta',\alpha'\beta,\beta\beta')$$

となる. $\alpha\alpha'=a$, $\alpha\beta'+\alpha'\beta=b$, $\beta\beta'=c$ とおくと $a,b,c\in\mathbb{Z}$ である. ここで $(a,b,c)=n$ とする. a が自然数の積であるから $n>0$ である. また $ax+by+cz=n$ をみたす $x,y,z\in\mathbb{Z}$ が存在することから

$$n\in AA',\qquad \text{となり}\qquad (n)\subseteq AA'$$

を得る. ここで $\alpha\alpha'$, $\beta\beta'\in(n)$ であることを注意しておく. さて

$$p=\frac{\alpha\beta'}{n}+\frac{\alpha'\beta}{n}=\frac{b}{n},\qquad q=\frac{\alpha\beta'}{n}\cdot\frac{\alpha'\beta}{n}=\frac{ac}{n^2}$$

とおくと, これらは有理整数である. $\dfrac{\alpha\beta'}{n}$, $\dfrac{\alpha'\beta}{n}$ は $X^2-pX+q=0$ の根だから $\dfrac{\alpha\beta'}{n}$, $\dfrac{\alpha'\beta}{n}$ は O_m に含まれる. $\alpha\beta'=n\cdot\dfrac{\alpha\beta'}{n}$, $\alpha'\beta=n\cdot\dfrac{\alpha'\beta}{n}$ であるから $\alpha\beta'$, $\alpha'\beta\in(n)$ となる. これより $AA'\subseteq(n)$ となるので $AA'=(n)$ が示された. ∎

定義 4.16 A,B,C をイデアルとする. $A=BC$ が成り立つとき A は B で割り切れるといい $B\mid A$ と表す. またこのとき, B を A の約イデアルという.

定理 4.17 A,B,C がイデアルで $AB=AC$, $A\neq 0$ であるとき $B=C$ が成り立つ.

Proof 定理 4.15 より $AA'=(a)$ とおくことができる. ここで $a\in\mathbb{Z}$ である. 定理 1.33 よりイデアルの積は交換可能で結合律もみたすから

$$AB=AC\implies A'AB=A'AC\implies (a)B=(a)C\implies aB=aC\implies B=C$$

が成り立つ. ∎

定理 4.18 A, B をイデアルとする. このとき, $A \subseteq B$ が成り立つことと $A = BC$ をみたすイデアル C が存在することとは同値である.

Proof $A = BC$ となるイデアル C が存在するならば $C \subseteq O_m$ より $A = BC \subseteq BO_m = B$ が成り立つ. 逆に $A \subseteq B$ と仮定する. 定理 4.15 より $AB' \subseteq BB' = (b)$ となる有理整数 b が存在する. これより AB' の各元は b の倍数だから

$$AB' = (b\gamma_1, b\gamma_2) = b(\gamma_1, \gamma_2)$$

と表される. ここで $C = (\gamma_1, \gamma_2)$ とおくと $AB' = bC = (b)C = BB'C = BCB'$ が成り立つ. 従って定理 4.17 より $A = BC$ を得る. ∎

定義 4.19 イデアル A, B に対して, $D \mid A$, $D \mid B$ をみたすイデアル D を A, B の公約イデアルという.

イデアル A, B に対して A, B を含むイデアルすべての共通部分を M とすると, 明らかに M もイデアルで, A, B を含むことから定理 4.18 より A, B の公約イデアルである. D を A, B の公約イデアルとすると $A \subseteq D$, $B \subseteq D$ より $M \subseteq D$ が成り立ち, $D \mid M$ となる.

いま N が A, B の公約イデアルで, すべての公約イデアルで割りきれるとすると $M \mid N$ かつ $N \mid M$, すなわち $N \subseteq M$ かつ $M \subseteq N$ が成り立つ. よって, $N = M$ である. M を A, B の最大公約イデアルといい, $(A, B) = M$ と表す.

定理 4.20 0 でないイデアル $P \neq O_m$ について次の (1) ~ (3) は同値である.

(1) P は極大イデアルである. すなわち $P \subsetneq I \subsetneq O_m$ をみたすイデアル I が存在しない.

(2) $AB \subseteq P$ ならば $A \subseteq P$ または $B \subseteq P$ が成り立つ. すなわち $P \mid AB$ ならば $P \mid A$ または $P \mid B$ が成り立つ.

(3) $\alpha\beta \in P$ ならば $\alpha \in P$ または $\beta \in P$ が成り立つ. すなわち P は素イデアルである.

Proof (2)⇒(3) $\alpha\beta \in P$ と仮定する. このとき $(\alpha)(\beta) \subseteq P$ であるから, (2) より $(\alpha) \subseteq P$ または $(\beta) \subseteq P$ が成り立つ. よって $\alpha \in P$ または $\beta \in P$ が成り立つ.

(3) $\Rightarrow$ (2)　$AB \subseteq P$ であり, $A \not\subseteq P$ かつ $B \not\subseteq P$ と仮定する. このとき $\alpha \in A - P$ かつ $\beta \in B - P$ が存在して $\alpha\beta \in P$ となるが, (3) より $\alpha \in P$ または $\beta \in P$ となり矛盾が生じる. ゆえに $A \subseteq P$ または $B \subseteq P$ が成り立つ.

(1) $\Rightarrow$ (3)　$\alpha\beta \in P$ とする. $\alpha \notin P$ と仮定すると $P \subsetneq (\alpha, P)$ が成り立つ. (1) より $(\alpha, P) = O_m$ である. 従って $1 = \alpha\kappa + \gamma$ をみたす $\kappa \in O_m$, $\gamma \in P$ が存在する. このとき

$$\beta = \beta \cdot 1 = \beta\alpha\kappa + \beta\gamma$$

であるが, $\alpha\beta, \gamma \in P$ であるから $\beta \in P$ を得る.

(3) $\Rightarrow$ (1)　P は素イデアルとする. $P \subsetneq A \subseteq O_m$ として $A = O_m$ であることを示せばよい. P に標準的基底が存在するから $P \cap \mathbb{Z}$ は 0 でない. 定理 1.35 より $P \cap \mathbb{Z}$ は $\mathbb{Z}$ の素イデアルである. 従って $P \cap \mathbb{Z} = (p)$ となる有理素数 p が存在する.

ここで $\alpha \in A - P$ を選び $\alpha + a \in P$ をみたす $a \in \mathbb{Z}$ が存在する場合と存在しない場合に分けて考える.

まず $\alpha + a \in P$ をみたす $a \in \mathbb{Z}$ が存在すると仮定する. $a = (\alpha + a) - \alpha \in A$ である. ここで $a \in P$ とすると $\alpha = (\alpha + a) - a \in P$ となり矛盾が生じるから, $a \notin P$ である. よって $p \nmid a$ である. これより $pe + af = 1$ をみたす $e, f \in \mathbb{Z}$ が存在するが $p, a \in A$ より $1 \in A$ が成り立つ. ゆえに $A = O_m$ である.

次に $\alpha + a \in P$ をみたす $a \in \mathbb{Z}$ が存在しないとする. このとき $\alpha \notin \mathbb{Z}$ であるから α の最小多項式は 2 次式である. 従って

$$\alpha^2 + a_1\alpha + a_2 = 0$$

をみたす $a_1, a_2 \in \mathbb{Z}$ が存在する. ここで $a_2 \in P$ とすると

$$\alpha(\alpha + a_1) = (\alpha^2 + a_1\alpha + a_2) - a_2 \in P$$

を得るが, 仮定より $\alpha \notin P$ だから $\alpha + a_1 \in P$ となり矛盾が生じる. よって $a_2 \notin P$ である. これより $p \nmid a_2$ となり, $pe + a_2 f = 1$ をみたす $e, f \in \mathbb{Z}$ が存在することになる. 一方

$$a_2 = (\alpha^2 + a_1\alpha + a_2) - (\alpha^2 + a_1\alpha) \in A$$

より $p, a_2 \in A$ であるから $pe + a_2 f = 1$ より $1 \in A$ を得る. ゆえにこの場合も $A = O_m$ が成り立つ. ∎

定理 4.21 (素イデアル分解) 0 でない任意のイデアルは素イデアルの積に分解される.

Proof 0 でないイデアルを任意に選び A とおく. A が素イデアルの積に分解されることを示せばよい.

まず A の約イデアルが有限個であることを示す. $A \ni \alpha \neq 0$ に対して $a = \alpha\alpha'$ は A に属する有理整数で, 0 でない. 必要ならば $-a$ と置き換えることにより $a > 0$ と仮定してよい. さて A の約イデアル B は $B \supseteq A$ をみたすから元 a を含む. ここで $B = (\alpha_1, \alpha_2)$ とおき

$$\begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \begin{bmatrix} 1 \\ \omega \end{bmatrix}$$

とする. ただし $c_{ij} \in \mathbb{Z}$ である. 除法の定理より $c_{ij} = q_{ij}a + r_{ij},\ 0 \leq r_{ij} < a$ と表されることから

$$\begin{aligned} \begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} &= a \begin{bmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{bmatrix} \begin{bmatrix} 1 \\ \omega \end{bmatrix} + \begin{bmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{bmatrix} \begin{bmatrix} 1 \\ \omega \end{bmatrix} \\ &= a \begin{bmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{bmatrix} \begin{bmatrix} 1 \\ \omega \end{bmatrix} + \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix} \end{aligned}$$

が得られる. これより $B = (\alpha_1, \alpha_2) = (\beta_1, \beta_2, a)$ が成り立つ. このような β_1, β_2 は有限個だから A の約イデアルも有限個である.

A の約イデアルが有限個であるから A を含むイデアルの列 $A \subsetneq A_1 \subsetneq \cdots \subsetneq A_r \subsetneq O_m$ において r は A の約イデアルの個数を越えない. 従ってこのような列の中で r が最大となるものがある. それを改めて $A \subsetneq A_1 \subsetneq \cdots \subsetneq A_r \subsetneq O_m$ とする. ここで定理 4.18 より

$$A = B_1A_1\,,\quad A_1 = B_2A_2\,,\quad A_2 = B_3A_3\,,\ \ldots\ldots\,,\ A_{r-1} = B_rA_r$$

をみたすイデアル $B_1, ..., B_r$ が定まる. このとき $A = B_1B_2\cdots B_rA_r$ が成り立つ. 従って A_r, B_i が素イデアルであることを示せばよい. A_r は極大イデアルであるから定理 4.20 より素イデアルである. 一方 B_k が素イデアルでないとすると $B_k \subsetneq C \subsetneq O_m$ をみたすイデアル C が存在する. これより $B_k = CD$ となるイデアル D が定まるが $B_k \subsetneq C$ であるから $D \subsetneq O_m$ である. 従って

$$A_{k-1} = B_kA_k = CDA_k \subsetneq O_mDA_k = DA_k, \qquad DA_k \subsetneq O_mA_k = A_k$$

となり $A_{k-1} \subsetneq DA_k \subsetneq A_k$ を得る. これは A を含むイデアルの列の中で r が最大になるように選んだことに矛盾する. よって B_k は素イデアルである. ∎

定理 4.22 (素イデアル分解の一意性) 0 でないイデアルの素イデアルの積への分解は一意的である.

Proof 0 でないイデアルを任意に選び A とする. A が $A = P_1 \cdots P_r = Q_1 \cdots Q_s$ と素イデアル分解されたとき $r = s$ かつ適当に番号を付けかえることにより $P_1 = Q_1$,..., $P_r = Q_r$ となることを r に関する帰納法で示す.

$r = 1$ として $A = P_1 = Q_1 \cdots Q_s$ であるとする. $s \geq 2$ と仮定すると $Q_2 \cdots Q_s \subsetneq O_m$ より

$$P_1 = Q_1 \cdots Q_s \subsetneq Q_1 O_m = Q_1 \subsetneq O_m$$

となり P_1 が極大イデアルであることに矛盾する. よって $s = 1$ かつ $P_1 = Q_1$ を得る.

次に $r > 1$ とし $r-1$ のときは素イデアル分解の一意性が成り立つとする. $P_1 \cdots P_r = Q_1 \cdots Q_s$ であるとする. このとき $Q_1 \mid P_1 \cdots P_r$ であるから定理 4.20 (2) より Q_1 はある P_i を割り切る. 一般性を失うことなく $Q_1 \mid P_1$ としてよい. このとき定理 4.18 より $P_1 \subseteq Q_1$ であるが P_1 も極大イデアルであるから $P_1 = Q_1$ を得る. このとき定理 4.17 より

$$P_2 \cdots P_r = Q_2 \cdots Q_s$$

が得られる. ここで帰納法の仮定を適用すれば, $r = s$ かつ適当に番号を付けかえることにより $P_2 = Q_2$,..., $P_r = Q_r$ とできる. よって r のときも成り立つことが示された. ∎

一般に可換環 R において, 0 でない任意のイデアルが素イデアルの積として一意的に分解されるとき R を Dedekind 整域という. 定理 4.21, 定理 4.22 より次の定理を得る.

定理 4.23 2次体 $\mathbb{Q}(\sqrt{m})$ の整数環 O_m は *Dedekind* 整域である.

定理 4.24 2次体の整数環 O_m が単項イデアル整域であることと一意分解整域であることとは同値である.

Proof 定理 1.50 と定理 1.51 により単項イデアル整域は一意分解整域である. 従って O_m が一意分解整域ならば単項イデアル整域であることを示せばよい. O_m の 0 でないイデアルは素イデアルの積として分解できるから, 0 でない素イデアルが単項イデアルであることを示せばよい. 0 でない素イデアルを任意に選び P とする. P の 0 でない元を 1 つ選び

α とする. $P \neq O_m$ より α は単数でない. O_m は一意分解整域であるから $\alpha = \pi_1\pi_2\cdots\pi_r$ と素元 π_i の積として表すことができる. P は素イデアルであるから $\pi_i \in P$ となる i が存在する. このとき $(\pi_i) \subseteq P$ であるが (π_i) は素イデアル, 従って極大イデアルであるから $(\pi_i) = P$ が成り立つ. ゆえに P は単項イデアルである. 以上で O_m が単項イデアル整域であることが示された. ∎

4.4 (p) の素イデアル分解

この節では有理素数 p で生成される単項イデアル (p) の素イデアル分解について考察する.

補題 4.25 O_m の 0 でないイデアル A と素イデアル P に対して $\mathcal{N}(AP) = \mathcal{N}(A)\mathcal{N}(P)$ が成り立つ.

Proof $\mathcal{N}(A) = r, \mathcal{N}(P) = s$ とし, A を法とする剰余類の代表元を $\alpha_1, \ldots, \alpha_r$, P を法とする剰余類の代表元を $\beta_1, \ldots, \beta_s$ とする.

$A = AO_m \supsetneq AP$ より A に属して AP に属さない元 γ がある. このとき $(\gamma) \subseteq A$ より $A \mid (\gamma)$ となるので $(\gamma) = AC$ をみたすイデアル C が存在する. 一方 $(\gamma) \not\subseteq AP$ より $P \nmid C$ であることを注意しておく. さて

$$\alpha_i + \gamma\beta_j \qquad (1 \leq i \leq r,\ 1 \leq j \leq s)$$

とおき, これら rs 個の元が AP を法とする剰余類の代表系であることを示そう. まず, ある i, j, k, ℓ に対して

$$\alpha_i + \gamma\beta_j \equiv \alpha_k + \gamma\beta_\ell \pmod{AP}$$

が成り立つと仮定する. このとき

$$\alpha_i - \alpha_k + \gamma(\beta_j - \beta_\ell) \in AP \subset A \quad \text{かつ} \quad \gamma(\beta_j - \beta_\ell) \in A$$

であることから

$$\alpha_i - \alpha_k + \gamma(\beta_j - \beta_\ell) \equiv \alpha_i - \alpha_k \equiv 0 \pmod{A}$$

となり $i = k$ を得る. これより $\gamma(\beta_j - \beta_\ell) \equiv 0 \pmod{AP}$ が得られるので 2 つの単項イデアル (γ) と $(\beta_j - \beta_\ell)$ の積 $(\gamma)(\beta_j - \beta_\ell)$ は AP に含まれる. 従って $AP \mid (\gamma)(\beta_j - \beta_\ell)$ が成り立つ. このとき $P \mid C(\beta_j - \beta_\ell)$ かつ $P \nmid C$ となるが P が素イデアルであることから

$P \mid (\beta_j - \beta_\ell)$, すなわち $\beta_j - \beta_\ell \in P$ を得る. ゆえに $j = \ell$ が示された. よって

$$\alpha_i + \gamma\beta_j \equiv \alpha_k + \gamma\beta_\ell \pmod{AP}$$

が成り立つのは $i = k$ かつ $j = \ell$ のときに限る. すなわち

$$\alpha_i + \gamma\beta_j \qquad (1 \le i \le r,\ 1 \le j \le s)$$

は AP を法として互いに合同でない. 次に 任意の $\delta \in O_m$ が AP を方として上の rs 個の元のいずれかに合同であることを示す. $\delta \equiv \alpha_i \pmod{A}$ となる α_i に対して $\delta - \alpha_i \in A$ であるが $((\gamma), AP) = A$ であることより $\delta - \alpha_i = \gamma\kappa + \lambda$ をみたす $\kappa \in O_m$, $\lambda \in AP$ が存在する. この κ に対して $\kappa \equiv \beta_j \pmod{P}$ となる β_j を選ぶと $\gamma(\kappa - \beta_j) \in AP$ であるから

$$\delta - \alpha_i = \gamma\kappa + \lambda \equiv \gamma\kappa \equiv \gamma\beta_j \pmod{AP} \implies \delta \equiv \alpha_i + \gamma\beta_j \pmod{AP}$$

を得る. 以上で

$$\alpha_i + \gamma\beta_j \qquad (1 \le i \le r,\ 1 \le j \le s)$$

が AP を法とする剰余類の代表系であることが示された. ゆえに $\mathcal{N}(AP) = rs$ より, $\mathcal{N}(AP) = \mathcal{N}(A)\mathcal{N}(P)$ が得られる. ∎

定理 4.26 O_m の 0 でないイデアル A, B に対して $\mathcal{N}(AB) = \mathcal{N}(A)\mathcal{N}(B)$ が成り立つ.

Proof $A = P_1 \cdots P_r$, $B = Q_1 \cdots Q_s$ と素イデアル分解されたとする. このとき補題 4.25 より

$$\mathcal{N}(A) = \mathcal{N}(P_1 \cdots P_r) = \mathcal{N}(P_1 \cdots P_{r-1})\mathcal{N}(P_r) = \cdots = \mathcal{N}(P_1) \cdots \mathcal{N}(P_r)$$

が成り立つ. 同様にして $\mathcal{N}(B) = \mathcal{N}(Q_1) \cdots \mathcal{N}(Q_s)$ が得られる. これより

$$\begin{aligned}
\mathcal{N}(AB) &= \mathcal{N}(P_1 \cdots\cdots P_r Q_1 \cdots\cdots\cdots Q_s) \\
&= \mathcal{N}(P_1 \cdots\cdots P_r Q_1 \cdots\cdots Q_{s-1})\mathcal{N}(Q_s) \\
&= \mathcal{N}(P_1 \cdots\cdots P_r Q_1 \cdots Q_{s-2})\mathcal{N}(Q_{s-1})\mathcal{N}(Q_s) \\
&\qquad\qquad \vdots \\
&= \mathcal{N}(P_1) \cdots \mathcal{N}(P_r)\mathcal{N}(Q_1) \cdots \mathcal{N}(Q_s) \\
&= \mathcal{N}(A)\mathcal{N}(B)
\end{aligned}$$

が導かれる. ∎

定理 4.27 0 でないイデアル A に対して $AA' = (\mathcal{N}(A))$ が成り立つ.

Proof イデアル A の基底を選び $a+b\omega$, $c+d\omega$ とする. このとき明らかに $a+b\omega'$, $c+d\omega'$ は A' の基底である. $m \equiv 2,3 \pmod 4$ のときは $\omega' = -\omega$ より A' の基底は $a-b\omega, c-d\omega$ となる. 従って定理 4.12 より

$$\mathcal{N}(A') = \left| det \begin{bmatrix} a & -b \\ c & -d \end{bmatrix} \right| = \mid -ad+bc \mid = \mid ad-bc \mid = \mathcal{N}(A)$$

が成り立つ.

$m \equiv 1 \pmod 4$ のときは $\omega' = \frac{1-\sqrt{m}}{2} = 1-\omega$ より A' の基底は $a+b-b\omega$, $c+d-d\omega$ となるので

$$\mathcal{N}(A') = \left| det \begin{bmatrix} a+b & -b \\ c+d & -d \end{bmatrix} \right| = \mid -(a+b)d+(c+d)b \mid = \mid ad-bc \mid = \mathcal{N}(A)$$

となる. ここで 定理 4.15 より $AA' = (n)$ となる $n \in \mathbb{Z}$ が存在するが, $n > 0$ となるように選ぶことができるから, 定理 4.26 を適用すると

$$\mathcal{N}(A)\mathcal{N}(A') = \mathcal{N}(AA') = \mathcal{N}((n)) = n^2 \quad \Longrightarrow \quad \mathcal{N}(A) = \mathcal{N}(A') = n$$

が得られる. ゆえに $AA' = (\mathcal{N}(A))$ が成り立つ. ∎

定理 4.28 O_m のイデアルについて次が成り立つ.

(1) 素イデアル P に対して $P \mid (p)$ をみたす有理素数 p が存在し, $\mathcal{N}(P) = p$ 又は p^2 が成り立つ. 特に $\mathcal{N}(P) = p^2$ のときは $P = (p)$ が成り立つ.

(2) $\mathcal{N}(P) = p$, p は有理素数, となるイデアル P は素イデアルで $PP' = (p)$ が成り立つ. 特に $P \mid (p)$ かつ $P' \mid (p)$ である.

Proof (1) P を素イデアルとすると定理 1.35 より $P \cap \mathbb{Z}$ は $\mathbb{Z}$ の素イデアルである. 従って $P \cap \mathbb{Z} = (p)$ となる有理素数 p が存在する. このとき $P \supseteq (p)$ より $PC = (p)$ をみたすイデアル C が存在する. 両辺のノルムをとり, 定理 4.13 を適用すれば

$$\mathcal{N}(P)\mathcal{N}(C) = \mathcal{N}(PC) = \mathcal{N}((p)) = \mid \mathcal{N}(p) \mid = p^2$$

を得る. $P \neq O_m$ より $\mathcal{N}(P) \neq 1$ であるから $\mathcal{N}(P) = p$ または p^2 である. ここで $\mathcal{N}(P) = p^2$ と仮定すると $\mathcal{N}(C) = 1$ であるから $C = O_m$ となり $P = (p)$ が得られる.

(2) $\mathcal{N}(P) = p$ とする. P が素イデアルでないと仮定すると O_m が Dedekind 整域であることから $P = P_1 \dots P_r$, $r \geq 2$, と素イデアル分解される. 従って

$$p = \mathcal{N}(P) = \mathcal{N}(P_1) \cdots \mathcal{N}(P_r)$$

を得るが, (1) より $\mathcal{N}(P_i)$ は素数か素数の平方であるから矛盾が生じる. 従って P は素イデアルである. またこのとき定理 4.27 より $PP' = (\mathcal{N}(P)) = (p)$ が得られるので $P \mid (p)$ かつ $P' \mid (p)$ が成り立つ. ∎

上の定理より O_m の任意の素イデアル P はある有理素数 p で生成される単項イデアル (p) の約イデアルであることがわかる. また有理素数 p で生成される単項イデアル (p) が $(p) = P_1 \cdots P_r$ と素イデアル分解されたとすると, ノルムをとり

$$\mathcal{N}((p)) = p^2 = \mathcal{N}(P_1) \cdots \mathcal{N}(P_r), \qquad \mathcal{N}(P_i) = p \text{ または } p^2$$

が得られる. これより次の 2 つの場合が起こり得る.

$$(p) = P_1 P_2, \quad \mathcal{N}(P_1) = \mathcal{N}(P_2) = p \tag{4.1}$$

$$(p) = P_1, \quad \mathcal{N}(P_1) = p^2 \quad \text{すなわち } (p) \text{ は素イデアルである.} \tag{4.2}$$

(4.1) の場合, 定理 4.28 より $(p) = P_1 P_1'$ が成り立つので $P_2 = P_1'$ が得られる.

次に素イデアル P の標準的基底を $(a, b + c\omega)$ とすると, 素イデアルに属する最小の自然数は有理素数 p であるから $a = p$ が成り立つ. このとき補題 4.5 より $c \mid a$ となるので $c = 1$ または $c = p$ である. $c = p$ とすると, b も c の倍数だから

$$P = (p, b + p\omega) \subseteq (p) \quad \Longrightarrow \quad P = (p)$$

が成り立つ. これは(4.2) の場合である. $c = 1$ とすると P の標準的基底は $(p, b + \omega)$ となり, 定理 4.11 より $\mathcal{N}(P) = \det \begin{bmatrix} p & 0 \\ b & 1 \end{bmatrix} = p$ が成り立つ. これは(4.1) の場合である. またこのとき

$$\mathcal{N}(b + \omega) = (b + \omega)(b - \omega) \in P \cap \mathbb{Z} \quad \Longrightarrow \quad p \mid \mathcal{N}(b + \omega)$$

となることから

- $m \equiv 2, 3 \pmod 4$ のとき $\mathcal{N}(b + \omega) = b^2 - m \equiv 0 \pmod p$
- $m \equiv 1 \pmod 4$ のとき $\mathcal{N}(b + \omega) = \frac{(2b+1)^2 - m}{4} \equiv 0 \pmod p$

が成り立つ. 以上をまとめて次の定理を得る.

定理 4.29 p が有理素数で $(p) = PP'$ と素イデアル分解されるとき P の標準的基底は適当な整数 b により $(p, b+\omega)$ と表される. また

$$\begin{cases} b^2 - m & \equiv 0 \pmod{p}, \quad m \equiv 2, 3 \pmod{4} \\ \dfrac{(2b+1)^2 - m}{4} & \equiv 0 \pmod{p}, \quad m \equiv 1 \pmod{4} \end{cases}$$

が成り立つ. 特に $p \neq 2$ のとき $\left(\dfrac{m}{p}\right) = 0, 1$ である.

補題 4.30 $m \equiv 2, 3 \pmod{4}$, $P = (p, a+\sqrt{m})$ とする. ただし p は有理素数, a は有理整数であり, $(p, a+\sqrt{m})$ は必ずしも標準的基底を表すものではないとする. このとき, 次のいずれかの条件がみたされれば $P = p\mathbb{Z} + (a+\sqrt{m})\mathbb{Z}$ が成り立つ.

(1) $m \equiv a^2 \pmod{p}$

(2) $p \mid m$ かつ $a = 0$

(3) $p = 2$ かつ $m \equiv 2 \pmod{4}$ かつ $a = 0$

(4) $p = 2$ かつ $m \equiv 3 \pmod{4}$ かつ $a = 1$

Proof $p\mathbb{Z} + (a+\sqrt{m})\mathbb{Z} \subseteq P$ が成り立つことは明らかであるから $P \subseteq p\mathbb{Z} + (a+\sqrt{m})\mathbb{Z}$ が成り立つことを示せばよい. P の任意の元 α は適当な $r, s, t, u \in \mathbb{Z}$ により

$$\alpha = p(r + s\sqrt{m}) + (a+\sqrt{m})(t + u\sqrt{m}) = (pr + at + um) + (ps + au + t)\sqrt{m}$$

と表される. ここで

$$y = ps + au + t, \qquad px + ay = pr + at + um$$

とおく. 明らかに $y \in \mathbb{Z}$ である. さて $x \in \mathbb{Z}$ が示されれば

$$\alpha = px + ay + y\sqrt{m} = xp + y(a+\sqrt{m}) \in p\mathbb{Z} + (a+\sqrt{m})\mathbb{Z}$$

となり, $P = p\mathbb{Z} + (a + \sqrt{m})\mathbb{Z}$ が得られる.

$$\begin{aligned} xp &= pr + at + um - ay \\ &= pr + at + um - a(ps + au + t) \\ &= p(r - as) + (m - a^2)u \end{aligned}$$

より $x = r - as + \dfrac{m - a^2}{p}u$ を得る. 従って

(1) $m \equiv a^2 \pmod{p}$

(2) $p \mid m$ かつ $a = 0$

(3) $p = 2$ かつ $m \equiv 2 \pmod{4}$ かつ $a = 0$

(4) $p = 2$ かつ $m \equiv 3 \pmod{4}$ かつ $a = 1$

の各場合について $x \in \mathbb{Z}$ が成り立つ. よって補題が示された. ∎

補題 4.31 $m \equiv 1 \pmod{4}$, $P = (p, a + \frac{1+\sqrt{m}}{2})$ とする. ただし p は有理素数, a は有理整数であり, $(p, a + \frac{1+\sqrt{m}}{2})$ は必ずしも標準的基底を表すものではないとする. このとき, 次のいずれかの条件がみたされれば $P = p\mathbb{Z} + (a + \frac{1+\sqrt{m}}{2})\mathbb{Z}$ が成り立つ.

(1) $p \neq 2$ かつ $(2a + 1)^2 - m \equiv 0 \pmod{p}$

(2) $p \neq 2$ かつ $p \mid m$ かつ $2a + 1 = p$

(3) $m \equiv 1 \pmod{8}$ かつ $p = 2$ かつ $a = 0$

Proof $p\mathbb{Z} + (a + \frac{1+\sqrt{m}}{2})\mathbb{Z} \subseteq P$ が成り立つことは明らかであるから $P \subseteq p\mathbb{Z} + (a + \frac{1+\sqrt{m}}{2})\mathbb{Z}$ が成り立つことを示せばよい. $\omega = \frac{1+\sqrt{m}}{2}$, $\omega^2 = \frac{m-1}{4} + \omega$ を想起されたい. P の任意の元 α は適当な $r, s, t, u \in \mathbb{Z}$ により

$$\alpha = p(r + s\omega) + (a + \omega)(t + u\omega) = pr + at + \frac{m - 1}{4}u + (ps + (a + 1)u + t)\,\omega$$

と表される. ここで $y = ps + (a + 1)u + t$, $px + ay = pr + at + \frac{m-1}{4}u$ とおく. 明らかに $y \in \mathbb{Z}$ である. また $x \in \mathbb{Z}$ が示されれば

$$\alpha = px + ay + y\omega = xp + y(a + \omega) \in p\mathbb{Z} + (a + \omega)\mathbb{Z}$$

となり, $P = p\mathbb{Z} + (a + \frac{1+\sqrt{m}}{2})\mathbb{Z}$ が得られる.

$$\begin{aligned} xp &= pr + at + \frac{m-1}{4}u - ay \\ &= pr + at + \frac{m-1}{4}u - a(ps + (a+1)u + t) \\ &= p(r - as) + \frac{m - (2a+1)^2}{4}u \end{aligned}$$

より $x = r - as + \dfrac{m-(2a+1)^2}{4p}u$ を得る. 従って

(1) $p \neq 2$ かつ $(2a+1)^2 - m \equiv 0 \pmod{p}$ のとき $4 \mid (2a+1)^2 - m$ かつ $p \mid (2a+1)^2 - m$

(2) $p \neq 2$ かつ $p \mid m$ かつ $2a+1 = p$ のとき $4 \mid (2a+1)^2 - m$ かつ $p \mid (2a+1)^2 - m$

(3) $m \equiv 1 \pmod{8}$ かつ $p = 2$ かつ $a = 0$ のとき $8 \mid m - 1$

が成り立ち, 各場合について $x \in \mathbb{Z}$ を得る. よって $P = p\mathbb{Z} + (a + \frac{1+\sqrt{m}}{2})\mathbb{Z}$ が示された. ∎

$\mathbf{p \neq 2,\ \left(\frac{m}{p}\right) = 1}$ の場合

(i) $m \equiv 2, 3 \pmod{4}$ のとき.

$a^2 \equiv m \pmod{p}$ をみたす整数 a を選び $P = (p, a + \sqrt{m})$ とおく. このとき $P' = (p, a - \sqrt{m})$ である. 補題 4.30 (1) より $P = \mathbb{Z}p + \mathbb{Z}(a + \sqrt{m})$ となるから $\{p, a + \sqrt{m}\}$ は自由 $\mathbb{Z}$ 加群 P の $\mathbb{Z}$ 基底である. このとき定理 4.12 より

$$\mathcal{N}(P) = \left| \det \begin{bmatrix} p & 0 \\ a & 1 \end{bmatrix} \right| = p$$

が成り立つ. 従って定理 4.28 より P は素イデアルで $(p) = PP'$ が成り立つ. またこのとき $(p, 2a) = 1$ より $ps + 2at = 1$ をみたす $s, t \in \mathbb{Z}$ が存在することから

$$(P, P') = (p, a + \sqrt{m}, a - \sqrt{m}) = (p, 2a) = (1) = O_m$$

となるので $P \neq P'$ である.

(ii) $m \equiv 1 \pmod{4}$ のとき.

$(2a+1)^2 \equiv m \pmod{p}$ をみたす整数 a を選び $P = (p, a + \frac{1+\sqrt{m}}{2})$ とおく. $P' = (p, a + \frac{1-\sqrt{m}}{2})$ である. 補題 4.31 (1) より $P = \mathbb{Z}p + \mathbb{Z}(a + \frac{1+\sqrt{m}}{2})$ が成り立つ. 従って

$\{p, a+\frac{1+\sqrt{m}}{2}\}$ は P の $\mathbb{Z}$ 基底である. このとき

$$\mathcal{N}(P) = \left|\det \begin{bmatrix} p & 0 \\ a & 1 \end{bmatrix}\right| = p$$

だから定理 4.28 より P は素イデアルで $(p) = PP'$ が成り立つ. またこのとき $(p, 2a+1) = 1$ より $ps + (2a+1)t = 1$ をみたす $s, t \in \mathbb{Z}$ が存在するから

$$(P, P') = (p, a + \frac{1+\sqrt{m}}{2}, a + \frac{1-\sqrt{m}}{2}) = (p, 2a+1) = (1) = O_m$$

が成り立つ. 従って $P \neq P'$ である.

$\mathbf{p \neq 2,\ \left(\frac{m}{p}\right) = 0}$ の場合

(i) $m \equiv 2, 3 \pmod 4$ のとき.

$P = (p, \sqrt{m})$ とおく. 補題 4.30 (2) より $P = \mathbb{Z}p + \mathbb{Z}\sqrt{m}$ となるので $\{p, \sqrt{m}\}$ は P の $\mathbb{Z}$ 基底である. このとき $\mathcal{N}(P) = p$ より定理 4.28 より P は素イデアルで $(p) = PP'$ が成り立つ. また $P' = (p, -\sqrt{m}) = P$ であるから $(p) = P^2$ である.

(ii) $m \equiv 1 \pmod 4$ のとき.

$2a + 1 = p$, $P = (p, a + \frac{1+\sqrt{m}}{2})$ とおく. 補題 4.31 (2) より $P = \mathbb{Z}p + \mathbb{Z}(a + \frac{1+\sqrt{m}}{2})$ となるので $\{p, a + \frac{1+\sqrt{m}}{2}\}$ は P の $\mathbb{Z}$ 基底である. このとき $\mathcal{N}(P) = p$ であるから定理 4.28 より P は素イデアルで $(p) = PP'$ が成り立つ. ここで

$$P' = (p, a + \frac{1-\sqrt{m}}{2}) = (p, \frac{p-1}{2} + \frac{1-\sqrt{m}}{2}) = (p, -a - \frac{1+\sqrt{m}}{2}) = P$$

より $(p) = P^2$ となる.

$\mathbf{p \neq 2,\ \left(\frac{m}{p}\right) = -1}$ の場合

定理 4.29 より (p) は素イデアル P に一致し $\mathcal{N}(P) = p^2$ が成り立つ. 以上をまとめて次の定理を得る.

定理 4.32 有理素数 $p \neq 2$ に対して O_m における (p) の素イデアル分解は次のようになる.

(1) $\left(\frac{m}{p}\right) = 1$ のとき $(p) = PP'$, $P \neq P'$, $\mathcal{N}(P) = \mathcal{N}(P') = p$ が成り立つ. また a を次のように選べば $(p, a+\omega)$ は P の標準的基底である.

$$\begin{cases} a^2 & \equiv m \pmod{p} \quad m \equiv 2,3 \pmod{4} \\ (2a+1)^2 & \equiv m \pmod{p} \quad m \equiv 1 \pmod{4} \end{cases}$$

(2) $\left(\frac{m}{p}\right) = -1$ のとき (p) は素イデアルで $\mathcal{N}((p)) = p^2$ が成り立つ.

(3) $\left(\frac{m}{p}\right) = 0$ のとき $(p) = P^2, \mathcal{N}(P) = p$ が成り立つ. また a を次のように選べば $(p, a+\omega)$ は P の標準的基底である.

$$\begin{cases} a & = 0 \quad m \equiv 2,3 \pmod{4} \\ a & = \frac{p-1}{2} \quad m \equiv 1 \pmod{4} \end{cases}$$

p = 2 の場合

(i) $m \equiv 2 \pmod{4}$ のとき.

$P = (2, \sqrt{m})$ とおくと補題 4.30 (3) より $P = \mathbb{Z} \cdot 2 + \mathbb{Z} \cdot \sqrt{m}$ となるから $\{2, \sqrt{m}\}$ は P の $\mathbb{Z}$ 基底である. このとき $\mathcal{N}(P) = 2$ であるから定理 4.28 より P は素イデアルで $(2) = PP'$ が成り立つ. また $P' = (2, -\sqrt{m}) = P$ より $(2) = P^2$ である.

(ii) $m \equiv 3 \pmod{4}$ のとき.

$P = (2, 1+\sqrt{m})$ とおくと, 補題 4.30 (4) より $P = \mathbb{Z} \cdot 2 + \mathbb{Z} \cdot (1+\sqrt{m})$ となるから $\{2, 1+\sqrt{m}\}$ は P の $\mathbb{Z}$ 基底である. このとき $\mathcal{N}(P) = 2$ であるから, 定理 4.28 より P は素イデアルで $(2) = PP'$ が成り立つ. また $P' = (2, 1-\sqrt{m}) = P$ より $(2) = P^2$ である.

(iii) $m \equiv 1 \pmod{8}$ のとき.

$P = (2, \frac{1+\sqrt{m}}{2})$ とおくと補題 4.31 (3) より $P = \mathbb{Z} \cdot 2 + \mathbb{Z} \cdot \left(\frac{1+\sqrt{m}}{2}\right)$ となるから $\{2, \frac{1+\sqrt{m}}{2}\}$ は P の $\mathbb{Z}$ 基底である. このとき $\mathcal{N}(P) = 2$ だから定理 4.28 より P は素イデアルで $(2) = PP'$ が成り立つ. このとき

$$(P, P') = (2, \frac{1+\sqrt{m}}{2}, \frac{1-\sqrt{m}}{2}) = (2, 1) = (1) = O_m$$

より $P \neq P'$ である.

(iv) $m \equiv 5 \pmod{8}$ のとき.

定理 4.29 より (2) は素イデアルである.

以上をまとめて次の定理が得られる.

定理 4.33 O_m における (2) の素イデアル分解は次のようになる.

(1) $m \equiv 2,3 \pmod 4$ のとき $(2) = P^2$, $\mathcal{N}(P) = 2$ が成り立つ. また $a \equiv m \pmod 2$ となる整数 a に対して $(2, a+\omega)$ は P の標準的基底である.

(2) $m \equiv 1 \pmod 8$ のとき, $(2) = PP'$, $P \neq P'$, $\mathcal{N}(P) = \mathcal{N}(P') = 2$ が成り立つ. また $(2, \omega)$ は P の標準的基底である.

(3) $m \equiv 5 \pmod 8$ のとき (2) は素イデアルである. また $\mathcal{N}((2)) = 4$ である.

さて 2 次体 $\mathbb{Q}(\sqrt{m})$ に対してその判別式 D を次式で定義する.

$$D = D[1, \omega] = \det \begin{bmatrix} 1 & \omega \\ 1 & \omega' \end{bmatrix}^2 = (\omega - \omega')^2$$

このとき次の定理が成り立つ (証明略).

定理 4.34 2 次体 $\mathbb{Q}(\sqrt{m})$ の判別式の値は次のようになる.

(1) $m \equiv 2,3 \pmod 4$ のとき $\omega = \sqrt{m}$ であるから $D = 4m$ である.

(2) $m \equiv 1 \pmod 4$ のとき $\omega = \frac{1+\sqrt{m}}{2}$ であるから $D = m$ である.

定義 4.35 (Artin 記号) $\mathbb{Q}(\sqrt{m})$ の判別式を D とする. 素数 p に対して *Artin* 記号 $\left(\frac{D}{p}\right)$ を, $p \neq 2$ のときは平方剰余記号, $p = 2$ のときは次のように定めることにする.

$$\left(\frac{D}{2}\right) = \begin{cases} 1, & D \equiv 1 \pmod 8 \quad (\Longleftrightarrow m \equiv 1 \pmod 8) \\ -1, & D \equiv 5 \pmod 8 \quad (\Longleftrightarrow m \equiv 5 \pmod 8) \\ 0, & 2 \mid D \qquad\qquad\quad (\Longleftrightarrow m \equiv 2,3 \pmod 4) \end{cases}$$

定理 4.32, 定理 4.33 より O_m における (p) の素イデアル分解は次の 3 つの型に分けることができる.

(1) $(p) = PP'$, $P \neq P'$, $\mathcal{N}(P) = \mathcal{N}(P') = p$ となる. この場合 p は $\mathbb{Q}(\sqrt{m})$ で完全分解するという.

(2) $(p) = P^2$, $P = P'$, $\mathcal{N}(P) = p$ となる. この場合 p は $\mathbb{Q}(\sqrt{m})$ で分岐するという.

(3) (p) は素イデアル, $\mathcal{N}((p)) = p^2$ となる. この場合 p は $\mathbb{Q}(\sqrt{m})$ で惰性するという.

定理 4.32, 定理 4.33 は Artin 記号を用いて次のように述べることができる.

定理 4.36 O_m における (p) の素イデアル分解は次のようになる. ただし p は有理素数, $\left(\frac{D}{p}\right)$ は *Artin* 記号である.

(1) p が完全分解する条件は $\left(\frac{D}{p}\right) = 1$ となることである.

(2) p が分岐する条件は $\left(\frac{D}{p}\right) = 0$ となることである.

(3) p が惰性する条件は $\left(\frac{D}{p}\right) = -1$ となることである.

5 章　イデアル類と類数

この章ではイデアル類の全体 CL_m が有限アーベル群をなすことを証明する. また類数 h が 1 であることと O_m が一意分解整域であることとが同値であることを示す. これより整数環 O_m が一意分解整域であるかどうかは類数を計算することにより判定できる.

§5.1 ではイデアルの間に対等という同値関係を定義し, このときの同値類としてイデアル類を, それらの個数として類数を定義する. また Minkowski の定数 κ を定義し, すべてのイデアル類にノルムが κ 以下のイデアルが存在することを示す. これより類数が有限であることが導かれる. さらにイデアル類全体のなす有限アーベル群として, イデアル類群を定義する. §5.2 では §5.1 の結果をふまえて, いくつかの 2 次体についてその類数を決定する.

5.1　イデアル類群と類数

2 次体 $\mathbb{Q}(\sqrt{m})$ の整数環 O_m の 0 でないイデアル A, B に対し

$$A = \gamma B = \{\ \gamma x\ \mid\ x \in B\ \}$$

をみたす $\gamma \in \mathbb{Q}(\sqrt{m})$, $\gamma \neq 0$ が存在するとき, A と B は対等であるといい $A \sim B$ と表す. 明らかに対等という関係は 0 でないイデアル全体のなす集合上の同値関係である. このときの同値類をイデアル類といい, イデアル類全体の集合を CL_m, イデアル A を含むイデアル類を $cl(A)$ と表す. またイデアル類の個数を類数といい, $h(m)$ または単に h と表す. 0 でない 2 つの単項イデアル (α), (β) は $(\alpha) = \frac{\alpha}{\beta}(\beta)$ より, 互いに対等である. 従って 0 でない単項イデアル全体は 1 つのイデアル類をなす.

類数の定義より次の定理が得られる (証明略).

定理 5.1 $h = 1$ であることと O_m が単項イデアル整域であることとは同値である.

定理 5.1 と定理 4.24 より次の定理を得る (証明略).

定理 5.2 $h=1$ であることと O_m が一意分解整域であることとは同値である.

定義 5.3 (Minkowski の定数) D を $\mathbb{Q}(\sqrt{m})$ の判別式とする. このとき 次式で与えられる κ を *Minkowski* の定数という.

$$\kappa = \begin{cases} \frac{1}{2}\sqrt{D} & (m>0) \\ \sqrt{\frac{|D|}{3}} & (m<0) \end{cases}$$

以下 κ は Minkowski の定数を表すこととする.

定理 5.4 任意のイデアル類は $\mathcal{N}(A) \leq \kappa$ をみたすイデアル A を含む.

Proof　イデアル類を任意に選び, その中でノルムが最小のものを A とする. 定理 4.7 により $A = \gamma B$ と表される. ここで B は原始的イデアルである. 一方 $B \in cl(A)$ であるが $\mathcal{N}(A) = |\mathcal{N}(\gamma)|\mathcal{N}(B)$ となることから $\mathcal{N}(A)$ の最小性より $|\mathcal{N}(\gamma)| = 1$ を得る. ゆえに γ は単数で $A = B$ が得られる. よって A は原始的イデアルである.

A は原始的イデアルであるから, その標準的基底が $(a, r+\omega)$ と与えられる. 従って定理 4.11 より $\mathcal{N}(A) = a$ である. また定理 4.9 より $-\frac{a}{2} \leq r < \frac{a}{2}$ をみたすとしてよい. さて $\mathcal{N}(r+\omega) \in A \cap \mathbb{Z}$ であるから定理 4.9 より $a \mid \mathcal{N}(r+\omega)$ が成り立つ. ここで $\mathcal{N}(r+\omega) = ac$, $c \in \mathbb{Z}$ とおく. $(r+\omega) \subseteq A$ だから, 定理 4.18 より $(r+\omega) = AB$ をみたすイデアル B が存在する. このとき

$$\mathcal{N}(A)\mathcal{N}(B) = \mathcal{N}((r+\omega)) = \mid \mathcal{N}(r+\omega) \mid = \mid ac \mid$$

となることから $\mathcal{N}(B) = \mid c \mid$ が得られる. 従って定理 4.27 より $BB' = (\mathcal{N}(B)) = (c)$ を得る. これより

$$(r+\omega)B' = ABB' = (c)A$$

となり $A \sim B'$ が得られる. 仮定より $\mathcal{N}(B') \geq \mathcal{N}(A)$ であるから, $\mathcal{N}(B) = \mathcal{N}(B')$ より $\mid c \mid \geq a$ が成り立つ.

一方 $\mathcal{T}(r+\omega) = (r+\omega) + (r+\omega') = b$ とおくと $m \equiv 2, 3 \pmod 4$ のときは $\omega' = -\omega$ より $b = 2r$ が成り立ち, $m \equiv 1 \pmod 4$ のときは $\omega' = 1-\omega$ より $b = 2r+1$ が成り立つ. よっていずれの場合も $|b| \leq a$ が成り立つ. 以上で $\mid b \mid \leq a \leq \mid c \mid$ が示された.

さて $r+\omega, r+\omega'$ は

$$x^2 - \mathcal{T}(r+\omega)x + \mathcal{N}(r+\omega) = x^2 - bx + ac = 0$$

の根だから $\mathbb{Q}(\sqrt{m})$ の判別式を D とすると, 定義 (p.66) より

$$b^2 - 4ac = ((r+\omega) - (r+\omega'))^2 = (\omega - \omega')^2 = D$$

が成り立つ. ここで定理 4.34 より $m \equiv 2, 3 \pmod 4$ のとき $D = 4m$, $m \equiv 1 \pmod 4$ のとき $D = m$ であることを注意しておく.

$m > 0$ のとき $D > 0$ であるから $|b| \leq a \leq |c|$ より $\mid ac \mid \geq b^2 = D + 4ac > 4ac$ が成り立つから $c < 0$ を得る. 従って

$$D = b^2 - 4ac = b^2 + 4 \mid ac \mid \geq \mid 4ac \mid \geq 4a^2$$

より

$$\mathcal{N}(A) = a \leq \frac{\sqrt{D}}{2}$$

が成り立つ.

$m < 0$ のとき $D = b^2 - 4ac < 0$ より $ac > 0$, $c > 0$ だから

$$4a^2 \leq 4ac = b^2 - D = b^2 + \mid D \mid \leq a^2 + \mid D \mid$$

を得る. これより $3a^2 \leq \mid D \mid$ となり

$$\mathcal{N}(A) = a \leq \sqrt{\frac{\mid D \mid}{3}}$$

が成り立つ. 以上で定理が証明された. ∎

定理 5.5 正の実数 λ に対して, ノルムが λ 以下のイデアルの個数は有限である.

Proof　O_m は Dedekind 整域だから任意のイデアル A は $A = P_1 \cdots P_r$ と素イデアル P_i の積に分解される. ここで $\mathcal{N}(A) \leq \lambda$ とすると

$$\mathcal{N}(A) = \mathcal{N}(P_1) \cdots \mathcal{N}(P_r) \leq \lambda$$

が成り立つ. これより $\mathcal{N}(P_i) \leq \lambda$ が得られる. ここで定理 4.28 より有理素数 p_i が存在して $\mathcal{N}(P_i) = p_i$ または $\mathcal{N}(P_i) = p_i^2$ が成り立つが, $p_i \leq \lambda$ となるので, このような p_i は有限個である. $P_i \mid (p_i)$ より $\mathcal{N}(P_i) \leq \lambda$ をみたす P_i も有限個である. 一方 $\mathcal{N}(P_i) \geq 2$ より

$$2^r \leq \mathcal{N}(P_1) \cdots \mathcal{N}(P_r) \leq \lambda$$

が成り立つことから $r \leq \log_2 \lambda$ を得る. よって, ノルムが λ 以下のイデアルは有限個の素イデアル P_i の高々 r 個の積である. ゆえにノルムが λ 以下のイデアルは有限個である. ∎

以上で任意のイデアル類にノルムが κ 以下であるイデアルが存在すること, およびノルムが κ 以下のイデアルが有限個であることが示された. よって次の定理を得る.

定理 5.6 2 次体 $\mathbb{Q}(\sqrt{m})$ の類数は有限である.

定理 5.7 イデアル A, B を含むイデアル類 $cl(A)$ と $cl(B)$ の積を $cl(A)cl(B) = cl(AB)$ と定義することにより CL_m はアーベル群をなす. CL_m をイデアル類群という.

Proof　まず積が well-defined であることを示そう. $cl(A) = cl(A_1)$, $cl(B) = cl(B_1)$ とする. このとき 0 でない λ, ρ が存在して $A = \lambda A_1$, $B = \rho B_1$ と表すことができる. 従って $AB = \lambda\rho A_1 B_1$ より $cl(AB) = cl(A_1B_1)$ を得る. よって積は well-defined である.

定理 1.33 より, イデアル A, B, C は $AB = BA$, $(AB)C = A(BC)$ をみたすので

$$cl(A)cl(B) = cl(AB) = cl(BA) = cl(B)cl(A)$$

および

$$\begin{aligned}(cl(A)cl(B))cl(C) &= cl(AB)cl(C) = cl((AB)C) = cl(A(BC)) \\ &= cl(A)cl(BC) = cl(A)(cl(B)cl(C))\end{aligned}$$

が成り立つ. 従って積は交換可能で, 結合律をみたす.

次に $cl(A)cl((1)) = cl(A(1)) = cl(A)$ より $cl((1))$ は単位元である. また定理 4.27 より $cl(A)cl(A') = cl(AA') = cl((\mathcal{N}(A))) = cl((1))$ となるから $cl(A')$ は $cl(A)$ の逆元である. 以上で CL_m がアーベル群をなすことが示された. ∎

定理 5.8 類数が h のとき, 0 でないイデアル A に対して A^h は単項イデアルである.

Proof　イデアル類群の位数が h であるから Lagrange の定理 (cf. 定理 1.10) より $cl(A)^h = cl((1))$ が成り立つ. ゆえに A^h は単項イデアルである. ∎

定理 5.9 有理素数 p が完全分解するならば, 互いに素な有理整数 a, b が存在して, 次をみたす. ただし h は類数である.

$$a^2 - mb^2 = \begin{cases} \pm\, p^h & m \equiv 2, 3 \pmod 4 \\ \pm 4p^h & m \equiv 1 \pmod 4 \end{cases}$$

Proof　仮定より $(p) = PP'$, $P' \neq P, \mathcal{N}(P) = \mathcal{N}(P') = p$ をみたす素イデアル P が存在する. 定理 5.8 より P^h は単項イデアルである. $P^h = (\alpha)$ とし

$$\alpha = \begin{cases} a + b\sqrt{m} & \cdots\cdots\cdots\cdots \quad m \equiv 2, 3 \pmod 4 \\ \frac{a+b\sqrt{m}}{2},\ a \equiv b \pmod 2 & \cdots \quad m \equiv 1 \pmod 4 \end{cases}$$

とおく. ただし a, b は有理整数である. このとき

$$p^h = (\mathcal{N}(P))^h = \mathcal{N}(P^h) = \mathcal{N}((\alpha)) = \mid \mathcal{N}(\alpha) \mid = \mid a^2 - mb^2 \mid \quad \text{または} \quad \left| \frac{a^2 - mb^2}{4} \right|$$

が成り立つ. 従って

$$a^2 - mb^2 = \begin{cases} \pm\, p^h & m \equiv 2, 3 \pmod 4 \\ \pm 4p^h & m \equiv 1 \pmod 4 \end{cases}$$

が示された. また $(a, b) \neq 1$ とすると, $q \mid a$ かつ $q \mid b$ をみたす有理素数 q が存在し, $q \mid \alpha$ より $(q) \mid (\alpha)$ を得る. これより $(q) \mid P^h$ となるので $(q) = P^r$ と表される. 両辺のノルムをとって $q = p$ を得るが, このとき $P^r = (q) = (p) = PP'$ より $P = P'$ となり矛盾が生じる. ゆえに $(a, b) = 1$ である. ∎

5.2　類数の計算例

前節の結果により, 次の手順で類数, イデアル類群を計算することができる

(1) Minkowski の定数 κ と κ 以下の有理素数 p を求める.

(2) 単項イデアル (p) の素イデアル分解に現れる素イデアルを決定する.

(3) 上で求めた素イデアルの積でノルムが κ 以下となるものを求め, イデアル類に分類する.

$\mathbb{Q}(\sqrt{-14})$ の場合

$m = -14 \equiv 2 \pmod 4$, $D = 4m = -56$ より $\kappa = \sqrt{\frac{|-56|}{3}} = 4.3\cdots < 5$ となる. 次に定理 4.32, 定理 4.33 を用いて $p = 2, 3$ の場合について (p) の素イデアル分解を求める.

- $p = 2$ のとき, $m \equiv 2 \pmod 4$ より 2 は分岐する. $P_2 = (2, \sqrt{-14})$ とおけば $(2) = P_2^2$, $\mathcal{N}(P_2) = 2$ となる.

◦ $p=3$ のとき, $\left(\frac{-14}{3}\right)=\left(\frac{1}{3}\right)=1$ より 3 は完全分解する. $P_3=(3,1+\sqrt{-14})$, $P_3'=(3,1-\sqrt{-14})$ とおけば $(3)=P_3P_3'$, $P_3\neq P_3'$, $\mathcal{N}(P_3)=\mathcal{N}(P_3')=3$ となる.

以上からノルムが 4 以下のイデアルは (1), P_2, $P_2^2=(2)$, P_3, P_3' の 5 個である. また類数は 4 以下である.

- P_2 が単項イデアルであるとすると $P_2=(a+b\sqrt{-14})$ と表されるので定理 4.13 より

$$\mathcal{N}(P_2)=\mathcal{N}((a+b\sqrt{-14}))=\mid a^2+14b^2\mid=a^2+14b^2=2$$

を得るが, これをみたす $a,b\in\mathbb{Z}$ は存在しない. 従って $P_2\nsim(1)$ である. また $P_2^2=(2)\sim(1)$ より $cl(P_2^2)=cl(P_2)^2=1$ であるから $cl(P_2)$ の位数は 2 で $cl(P_2)^{-1}=cl(P_2)$ が成り立つ.

- P_2 と同様にして $P_3,P_3'\nsim(1)$ が得られる. また $P_3P_3'=(3)$ より $cl(P_3P_3')=cl(P_3)cl(P_3')=1$ となるので $cl(P_3)^{-1}=cl(P_3')$ である.

- $P_3^2=(9,3+3\sqrt{-14},-13+2\sqrt{-14})=(9,-2+\sqrt{-14})$,

$$\begin{aligned}P_2P_3^2&=(2,\sqrt{-14})(9,-2+\sqrt{-14})=(18,-4+2\sqrt{-14},9\sqrt{-14},-14-2\sqrt{-14})\\&=(18,-2+\sqrt{-14})=(-2+\sqrt{-14})\end{aligned}$$

より

$$cl(P_2P_3^2)=cl(P_2)cl(P_3)^2=1\implies cl(P_3)^2=cl(P_2)^{-1}=cl(P_2)\neq1$$

$$cl(P_3)^4=cl(P_2)^2=1\implies cl(P_3)^3=cl(P_3)^4cl(P_3)^{-1}=cl(P_3')\neq1$$

が成り立つ. よって $cl(P_3)$ の位数は 4 である.

以上により $\mathbb{Q}(\sqrt{-14})$ のイデアル類群 CL_{-14} の類数は 4 である. また $cl(P_3)=A$ とおくと $CL_{-14}=\{1,A,A^2,A^3\}$ となり, CL_{-14} は A を生成元とする位数 4 の巡回群である.

$\mathbb{Q}(\sqrt{-21})$ の場合

$m=-21\equiv3\pmod4$, $D=4m=-84$ より $\kappa=\sqrt{\frac{|-84|}{3}}=5.2\cdots<6$ となる. 次に $p=2,3,5$ の場合について (p) の素イデアル分解を求める.

◦ $p=2$ のとき, $m\equiv3\pmod4$ より 2 は分岐する. $P_2=(2,1+\sqrt{-21})$ とおけば $(2)=P_2^2$, $\mathcal{N}(P_2)=2$ となる.

- $p=3$ のとき, $\left(\frac{-21}{3}\right)=0$ より 3 は分岐する. $P_3=(3,\sqrt{-21})$ とおけば $(3)=P_3^2$, $\mathcal{N}(P_3)=3$ となる.
- $p=5$ のとき, $\left(\frac{-21}{5}\right)=\left(\frac{4}{5}\right)=1$ より 5 は完全分解し, $P_5=(5,2+\sqrt{-21})$, $P_5'=(5,2-\sqrt{-21})$ とおけば $(5)=P_5P_5'$, $P_5\neq P_5'$, $3N(P_5)=\mathcal{N}(P_5')=5$ となる.

  以上からノルムが 5 以下のイデアルは (1), P_2, $P_2^2=(2)$, P_3, P_5, P_5' の 6 個である. また類数は 5 以下である.

- P_2 が単項イデアルであるとすると $P_2=(a+b\sqrt{-21})$ と表され

$$\mathcal{N}(P_2)=\mathcal{N}((a+b\sqrt{-21}))=\mid a^2+21b^2\mid=a^2+21b^2=2$$

  となるが, これをみたす整数 a,b は存在しない. よって $P_2\nsim(1)$ である.

- P_2 と同様にして $P_3,P_5,P_5'\nsim(1)$ が得られる.

- $P_2^2,P_3^2\sim(1)$ より $cl(P_2),cl(P_3)$ の位数は 2 で $cl(P_2)^{-1}=cl(P_2)$, $cl(P_3)^{-1}=cl(P_3)$ が成り立つ.

- $\mathcal{N}(P_2P_3)=6$ かつ $6=a^2+21b^2$ をみたす整数 a,b が存在しないことから $P_2P_3\nsim(1)$ である. 従って

$$cl(P_2)cl(P_3)\neq 1,\quad cl(P_2)\neq cl(P_3)^{-1}=cl(P_3)$$

  が成り立つ. 特に類数は 3 以上である. 一方, 類数は $cl(P_2)$ の位数 2 の倍数で 5 以下であることから 4 となる. また

$$\begin{aligned}P_2P_3P_5&=(2,1+\sqrt{-21})(3,\sqrt{-21})(5,2+\sqrt{-21})\\&=(6,3+3\sqrt{-21},2\sqrt{-21},-21+\sqrt{-21})(5,2+\sqrt{-21})\\&=(6,3+\sqrt{-21})(5,2+\sqrt{-21})\\&=(30,15+5\sqrt{-21},12+6\sqrt{-21},-15+5\sqrt{-21})\\&=(30,-3+\sqrt{-21})=(-3+\sqrt{-21})\sim(1)\end{aligned}$$

  が成り立つ. よって

$$cl(P_2)cl(P_3)cl(P_5)=1,\ \ cl(P_5)=cl(P_2)^{-1}cl(P_3)^{-1}=cl(P_2)cl(P_3)=cl(P_5)^{-1}=cl(P_5')$$

  を得る.

以上より $\mathbb{Q}(\sqrt{-21})$ の類数は 4 であり, $cl(P_2) = A$, $cl(P_3) = B$ とおくと $CL_{-21} = \{1, A, B, AB\}$ と表される.

$\mathbb{Q}(\sqrt{105})$ の場合

$m = 105 \equiv 1 \pmod 8$, $D = m = 105$ より $\kappa = \frac{\sqrt{105}}{2} = 5.1\cdots < 6$ となる. $p = 2, 3, 5$ の場合について (p) の素イデアル分解を求める.

- $p = 2$ のとき, $105 \equiv 1 \pmod 8$ より 2 は完全分解する. $P_2 = (2, \frac{1+\sqrt{105}}{2})$ とおけば $(2) = P_2P_2'$, $P_2 \neq P_2'$, $\mathcal{N}(P_2) = \mathcal{N}(P_2') = 2$ が成り立つ.

- $p = 3$ のとき, $\left(\frac{105}{3}\right) = 0$ より 3 は分岐する. $P_3 = (3, 1 + \frac{1+\sqrt{105}}{2})$ とおけば $(3) = P_3^2$, $P_3 = P_3'$, $\mathcal{N}(P_3) = 3$ が成り立つ.

- $p = 5$ のとき, $\left(\frac{105}{5}\right) = 0$ より 5 も分岐する. $P_5 = (5, 2 + \frac{1+\sqrt{105}}{2})$ とおけば $(5) = P_5^2$, $P_5 = P_5'$, $\mathcal{N}(P_5) = 5$ が成り立つ. ここで $P_5 = (5, \frac{5+\sqrt{105}}{2}) = (10 + \sqrt{105})$ となるので $P_5 \sim (1)$ を得る.

  以上からノルムが 5 以下のイデアルは (1), P_2, P_2', $P_2P_2' = (2)$, P_3, P_5 の 6 個である. また類数は 4 以下である.

- P_2 が単項イデアルであるとすると $P_2 = (\frac{a+b\sqrt{105}}{2})$ と表される. ただし $a \equiv b \pmod 2$ である. このとき

$$\mathcal{N}(P_2) = \left|\frac{a^2 - 105b^2}{4}\right| = 2, \quad a^2 - 105b^2 = \pm 8$$

  となり, $a^2 \equiv 2, 3 \pmod 5$ より矛盾が生じる. 従って $P_2 \nsim (1)$ である.

- P_2 と同様にして $P_3 \nsim (1)$ が得られる. $P_3^2 = (3)$ より $cl(P_3)$ の位数は 2 となり, 類数が 2 か 4 であることがわかる.

- $P_2^2 = (4, 1 + \sqrt{105}, \frac{53+\sqrt{105}}{2}) = (4, \frac{5+\sqrt{105}}{2}) = (\frac{31+3\sqrt{105}}{2})$ より $cl(P_2)$ の位数は 2 となり, $cl(P_2)^{-1} = cl(P_2') = cl(P_2)$ が成り立つ.

- $P_2P_3 = (6, 3 + \sqrt{105}, \frac{3+3\sqrt{105}}{2}, 27 + \sqrt{105}) = (6, \frac{-3+\sqrt{105}}{2}) = (\frac{9+\sqrt{105}}{2})$ より $cl(P_3) = cl(P_2)^{-1} = cl(P_2)$ が得られる.

  以上より O_{105} の類数は 2 である. また $cl(P_2) = A$ とおくと $CL_{105} = \{1, A\}$ と表される.

定理 5.2 で 2 次体が単純体であることと, 類数が 1 であることとが同値であることを示した. ここで $\mathbb{Q}(\sqrt{m})$ が Euclid 体以外の単純体, すなわち

$$m = -163, -67, -43, -19,\ \ 14,\ \ 22,\ \ 23,\ \ 31,\ \ 38,\ \ 43,\ \ 46,\ \ 47$$

の場合について, 実際に類数が 1 となることを確認することにする.

$\mathbb{Q}(\sqrt{-19})$ の場合

$m = -19 \equiv 1 \pmod 4$, $D = m = -19$ より

$$\kappa = \sqrt{\frac{|\,-19\,|}{3}} = 2.5\cdots < 3$$

が成り立つ. $p = 2$ のとき, $m \equiv 5 \pmod 8$ より (2) は素イデアルで, ノルムは 4 である. 従って, ノルムが 3 より小さいイデアルは (1) のみとなるから, 類数は 1 である.

$\mathbb{Q}(\sqrt{-43})$ の場合

$m = -43 \equiv 1 \pmod 4$, $D = m = -43$ より

$$\kappa = \sqrt{\frac{|\,-43\,|}{3}} = 3.7\cdots < 4$$

が成り立つ. $p = 2$ のとき, $m \equiv 5 \pmod 8$ より (2) は素イデアルで, ノルムは 4 である. $p = 3$ のとき, $\left(\frac{-43}{3}\right) = \left(\frac{2}{3}\right) = -1$ より (3) も素イデアルで, ノルムは 9 である. よってノルムが 4 より小さいイデアルは (1) のみとなるから, 類数は 1 である.

$\mathbb{Q}(\sqrt{-67})$ の場合

$m = -67 \equiv 1 \pmod 4$, $D = m = -67$ より

$$\kappa = \sqrt{\frac{|\,-67\,|}{3}} = 4.7\cdots < 5$$

が成り立つ. $p = 2$ のとき, $m \equiv 5 \pmod 8$ より (2) は素イデアルで, ノルムは 4 である. $p = 3$ のとき, $\left(\frac{-67}{3}\right) = \left(\frac{2}{3}\right) = -1$ より (3) も素イデアルで, ノルムは 9 である. 従って, ノルムが 5 より小さいイデアルは (1), (2) のみで (1) $\sim$ (2) より類数は 1 である.

$\mathbb{Q}(\sqrt{-163})$ の場合

$m = -163 \equiv 1 \pmod 4$, $D = m = -163$ より

$$\kappa = \sqrt{\frac{|\,-163\,|}{3}} = 7.3\cdots < 8$$

が成り立つ. $p=2$ のとき, $m\equiv 5 \pmod 8$ より (2) は素イデアルで, ノルムは 4 である. $p=3$ のとき, $\left(\frac{-163}{3}\right)=\left(\frac{2}{3}\right)=-1$ より (3) も素イデアルで, ノルムは 9 である. $p=5$ のとき, $\left(\frac{-163}{5}\right)=\left(\frac{2}{5}\right)=-1$ より (5) も素イデアルで, ノルムは 25 である. $p=7$ のとき, $\left(\frac{-163}{7}\right)=\left(\frac{5}{7}\right)=-1$ より (7) も素イデアルで, ノルムは 49 である. よってノルムが 8 より小さいイデアルは (1), (2) のみで (1) $\sim$ (2) より類数は 1 である.

$\mathbb{Q}(\sqrt{14})$ の場合

$m=14\equiv 2 \pmod 4$, $D=4m=56$ より

$$\kappa=\frac{\sqrt{56}}{2}=3.7\cdots<4$$

が成り立つ. $14\equiv 2 \pmod 4$ より 2 は分岐し, $P_2=(2,\sqrt{14})$ とおけば $(2)=P_2^2$, $P_2=(4+\sqrt{14})$, $\mathcal{N}(P_2)=2$ が成り立つ. $p=3$ のとき $\left(\frac{14}{3}\right)=\left(\frac{2}{3}\right)=-1$ より (3) は素イデアルで, ノルムは 9 である. よってノルムが 4 より小さいイデアルは (1) と P_2 のみで (1) $\sim P_2$ より, 類数は 1 である.

$\mathbb{Q}(\sqrt{22})$ の場合

$m=22\equiv 2 \pmod 4$, $D=4m=88$ より

$$\kappa=\frac{\sqrt{88}}{2}=4.6\cdots<5$$

が成り立つ. $22\equiv 2 \pmod 4$ より 2 は分岐し, $P_2=(2,\sqrt{22})$ とおけば $(2)=P_2^2$, $P_2=(14+3\sqrt{22})$, $\mathcal{N}(P_2)=2$ が成り立つ. $p=3$ のとき, $\left(\frac{22}{3}\right)=\left(\frac{1}{3}\right)=1$ より $P_3=(3,1+\sqrt{22})$ とおけば $(3)=P_3P_3'$, $P_3=(61+13\sqrt{22})$, $P_3'=(61-13\sqrt{22})$, $\mathcal{N}(P_3)=\mathcal{N}(P_3')=3$ が成り立つ. よってノルムが 5 より小さいイデアルは (1), P_2, P_2^2, P_3, P_3' であるが (1) $\sim P_2, P_2^2, P_3, P_3'$ より, 類数は 1 である.

$\mathbb{Q}(\sqrt{23})$ の場合

$m=23\equiv 3 \pmod 4$, $D=4m=92$ より

$$\kappa=\frac{\sqrt{92}}{2}=4.7\cdots<5$$

が成り立つ. $23\equiv 3 \pmod 4$ より 2 は分岐し, $P_2=(2,1+\sqrt{23})$ とおけば $(2)=P_2^2$, $P_2=(5+\sqrt{23})$, $\mathcal{N}(P_2)=2$ が成り立つ. $p=3$ のとき, $\left(\frac{23}{3}\right)=\left(\frac{2}{3}\right)=-1$ より (3) は素イデアルで, ノルムは 9 となる. よってノルムが 5 より小さいイデアルは (1), P_2, P_2^2 であるが (1) $\sim P_2, P_2^2$ より, 類数は 1 である.

$\mathbb{Q}(\sqrt{31})$ の場合

$m = 31 \equiv 3 \pmod 4$, $D = 4m = 124$ より

$$\kappa = \frac{\sqrt{124}}{2} = 5.5\cdots < 6$$

が成り立つ. $31 \equiv 3 \pmod 4$ より, 2 は分岐し $P_2 = (2, 1+\sqrt{31})$ とおけば $(2) = P_2^2$, $P_2 = (39+7\sqrt{31})$, $\mathcal{N}(P_2) = 2$ が成り立つ. $p = 3$ のとき, $\left(\frac{31}{3}\right) = \left(\frac{1}{3}\right) = 1$ より $P_3 = (3, 1+\sqrt{31})$ とおけば $(3) = P_3P_3'$, $P_3 = (11+2\sqrt{31})$, $P_3' = (11-2\sqrt{31})$, $\mathcal{N}(P_3) = \mathcal{N}(P_3') = 3$ が成り立つ. $p = 5$ のとき, $\left(\frac{31}{5}\right) = \left(\frac{1}{5}\right) = 1$ より $P_5 = (5, 1+\sqrt{31})$ とおけば $(5) = P_5P_5'$, $P_5 = (6+\sqrt{31})$, $P_5' = (6-\sqrt{31})$, $\mathcal{N}(P_5) = \mathcal{N}(P_5') = 5$ が成り立つ. よってノルムが 6 より小さいイデアルは $(1), P_2, P_2^2, P_3, P_3', P_5, P_5'$ であるが $(1) \sim P_2, P_2^2, P_3, P_3', P_5, P_5'$ より, 類数は 1 である.

$\mathbb{Q}(\sqrt{38})$ の場合

$m = 38 \equiv 2 \pmod 4$, $D = 4m = 152$ より

$$\kappa = \frac{\sqrt{152}}{2} = 6.1\cdots < 7$$

が成り立つ. $38 \equiv 2 \pmod 4$ より 2 は分岐し, $P_2 = (2, \sqrt{38})$ とおけば $(2) = P_2^2$, $P_2 = (6+\sqrt{38})$, $\mathcal{N}(P_2) = 2$ が成り立つ. $p = 3$ のとき, $\left(\frac{38}{3}\right) = \left(\frac{2}{3}\right) = -1$ より (3) は素イデアルで, ノルムは 9 である. $p = 5$ のとき, $\left(\frac{38}{5}\right) = \left(\frac{3}{5}\right) = -1$ より (5) は素イデアルで, ノルムは 25 である. よってノルムが 7 より小さいイデアルは $(1), P_2, P_2^2$ であるが $(1) \sim P_2, P_2^2$ より, 類数は 1 である.

$\mathbb{Q}(\sqrt{43})$ の場合

$m = 43 \equiv 3 \pmod 4$, $D = 4m = 172$ より

$$\kappa = \frac{\sqrt{172}}{2} = 6.5\cdots < 7$$

が成り立つ. $43 \equiv 3 \pmod 4$ より 2 は分岐し, $P_2 = (2, 1+\sqrt{43})$ とおけば $(2) = P_2^2$, $P_2 = (59+9\sqrt{43})$, $\mathcal{N}(P_2) = 2$ が成り立つ. $p = 3$ のとき, $\left(\frac{43}{3}\right) = \left(\frac{1}{3}\right) = 1$ より $P_3 = (3, 1+\sqrt{43})$ とおけば $(3) = P_3P_3'$, $P_3 = (400+61\sqrt{43})$, $P_3' = (400-61\sqrt{43})$, $\mathcal{N}(P_3) = \mathcal{N}(P_3') = 3$ が成り立つ. $p = 5$ のとき, $\left(\frac{43}{5}\right) = \left(\frac{3}{5}\right) = -1$ より (5) は素イデアルで, ノルムは 25 である. よってノルムが 7 より小さいイデアルは $(1), P_2, P_2^2, P_3, P_3', P_2P_3, P_2P_3'$ であるが, すべて (1) に対等になるので類数は 1 である.

$\mathbb{Q}(\sqrt{46})$ の場合

$m = 46 \equiv 2 \pmod 4$, $D = 4m = 184$ より

$$\kappa = \frac{\sqrt{184}}{2} = 6.7\cdots < 7$$

が成り立つ. $p = 2$ のとき, 2 は分岐し $P_2 = (2, \sqrt{46})$ とおけば $(2) = P_2^2$, $P_2 = (156 + 23\sqrt{46})$, $\mathcal{N}(P_2) = 2$ が成り立つ. $p = 3$ のとき, $\left(\frac{46}{3}\right) = \left(\frac{1}{3}\right) = 1$ より $P_3 = (3, 1 + \sqrt{46})$ とおけば $(3) = P_3P_3'$, $P_3 = (7 + \sqrt{46})$, $P_3' = (7 - \sqrt{46})$, $\mathcal{N}(P_3) = \mathcal{N}(P_3') = 3$ が成り立つ. $p = 5$ のとき, $\left(\frac{46}{5}\right) = \left(\frac{1}{5}\right) = 1$ より $P_5 = (5, 1 + \sqrt{46})$ とおけば $(5) = P_5P_5'$, $P_5 = (997 + 147\sqrt{46})$, $P_5' = (997 - 147\sqrt{46})$, $\mathcal{N}(P_5) = \mathcal{N}(P_5') = 5$ が成り立つ. よってノルムが 7 より小さいイデアルは $(1), P_2, P_2^2, P_3, P_3', P_2P_3, P_2P_3', P_5, P_5'$ であるが, すべて (1) に対等になるので類数は 1 である.

$\mathbb{Q}(\sqrt{47})$ の場合

$m = 47 \equiv 3 \pmod 4$, $D = 4m = 188$ より

$$\kappa = \frac{\sqrt{188}}{2} = 6.8\cdots < 7$$

が成り立つ. $47 \equiv 3 \pmod 4$ より 2 は分岐する. $P_2 = (2, 1 + \sqrt{47})$ とおけば $(2) = P_2^2$, $P_2 = (7 + \sqrt{47})$, $\mathcal{N}(P_2) = 2$ が成り立つ. $p = 3$ のとき, $\left(\frac{47}{3}\right) = \left(\frac{2}{3}\right) = -1$ より (3) は素イデアルで, ノルムは 9 である. $p = 5$ のとき, $\left(\frac{47}{5}\right) = \left(\frac{2}{5}\right) = -1$ より (5) は素イデアルで, ノルムは 25 である. よってノルムが 7 より小さいイデアルは $(1), P_2, P_2^2$ であるが, すべて (1) に対等になるので類数は 1 である.

以上で

$$m = -163, -67, -43, -19,\ 14,\ 22,\ 23,\ 31,\ 38,\ 43,\ 46,\ 47$$

の場合について $\mathbb{Q}(\sqrt{m})$ が単純体であることが確認できた.

応用

最後に不定方程式への $2, 3$ の応用を述べておく.

補題 5.10 $a, b \in \mathbb{Z}$, $(a, b) = c$ とする. このとき $\alpha \in O_m$ が $\alpha \mid a$ かつ $\alpha \mid b$ をみたせば $\alpha \mid c$ である. 特に a と b が互いに素のとき, α は単数である.

Proof $(a, b) = c$ なら, $ar + bs = c$ をみたす $r, s \in \mathbb{Z}$ が存在する. $\alpha \mid a$, $\alpha \mid b$ であるから定理 2.13 より $\alpha \mid ar + bs$ が成り立つ. 従って $\alpha \mid c$ が得られる. また a と b が互いに素の

とき, $c=1$ であるから, $\alpha \mid 1$ となるので α は単数である. ∎

補題 5.11 2次体 $\mathbb{Q}(\sqrt{-5})$ の類数は 2 である.

Proof $m=-5$ とおく. このとき $m=-5\equiv 3 \pmod 4$, $D=4m=-20$ より $\kappa=\sqrt{\frac{|-20|}{3}}=2.5\cdots<3$ が成り立つ. $-5\equiv 3 \pmod 4$ より 2 は分岐する. $P_2=(2,1+\sqrt{-5})$ とおけば $(2)=P_2^2$, $\mathcal{N}(P_2)=2$ が成り立つ.

ここで P_2 が単項イデアルであると仮定し, $P_2=(a+b\sqrt{-5})$ とおくと

$$\mathcal{N}(P_2)=\mathcal{N}((a+b\sqrt{-5}))=\mid a^2+5b^2 \mid = a^2+5b^2=2$$

が得られるが, これをみたす $a,b\in\mathbb{Z}$ は存在しない. よって $P_2 \nsim (1)$ である. ノルムが 2 以下のイデアルは (1), P_2 のみであるから $\mathbb{Q}(\sqrt{-5})$ の類数は 2 である. ∎

補題 5.12 有理整数 x,y が $x^2+2=y^3$ をみたすとき, 2次体 $\mathbb{Q}(\sqrt{-2})$ の整数 $x+\sqrt{-2}$ と $x-\sqrt{-2}$ は互いに素である.

Proof $x+\sqrt{-2}$ と $x-\sqrt{-2}$ が単数以外に公約数を持たないことを示せばよい. $2\mid x$ とすると $2\mid x^2+2$ より $2\mid y^3$, $2\mid y$, $8\mid y^3$ となり $4\mid x^2+2$ が得られるが, これは $x^2+2\equiv 2,3 \pmod 4$ であることに矛盾する. よって $2\nmid x$, すなわち $(x,2)=1$ である.

次に α を O_{-2} の素元とし, $\alpha\mid x+\sqrt{-2}$, $\alpha\mid x-\sqrt{-2}$ とすると

$$\alpha \,\Big|\, (x+\sqrt{-2})+(x-\sqrt{-2}) \implies \alpha\mid 2x$$

$$\alpha \,\Big|\, \sqrt{-2}(x+\sqrt{-2})-\sqrt{-2}(x-\sqrt{-2}) \implies \alpha\mid -4$$

が得られる. これより $\alpha\mid(2x,-4)=2(x,-2)$ となるので $\alpha\mid 2$ が成り立つ. ここで $\alpha=a+b\sqrt{-2}$ とおき, ノルムを計算すると $\mathcal{N}(\alpha)\mid\mathcal{N}(2)$ より $a^2+2b^2\mid 4$ となる. これをみたす有理整数 a,b は $(a,b)=(\pm1,0),(0,\pm1),(\pm2,0)$ のいずれかである.

ここで $\alpha=\pm\sqrt{-2}$ とすると $\alpha\mid x+\sqrt{-2}$ より $\sqrt{-2}\mid x$ が得られる. ノルムを計算すると $2\mid x^2$ となり, $(x,2)=1$ に矛盾する. $\alpha=\pm2$ としても同様に矛盾を得る. 従って $\alpha=\pm1$ となるので α は単数である. ∎

定理 5.13 $x^2+2=y^3$ の整数解は $x=\pm5$, $y=3$ のみである.

Proof 定理3.5より $\mathbb{Q}(\sqrt{-2})$ は Euclid 体であり, 類数は 1 である.

$$x^2+2=(x+\sqrt{-2})(x-\sqrt{-2})=y^3$$

とおくと補題5.12より $x+\sqrt{-2}$ と $x-\sqrt{-2}$ は互いに素であるから $(x+\sqrt{-2})$ と $(x-\sqrt{-2})$ の公約イデアルは (1) のみである. よって $(x+\sqrt{-2})$ はあるイデアルの 3 乗として表される. $\mathbb{Q}(\sqrt{-2})$ のイデアルはすべて単項イデアルであり, 単数は $=\pm 1$ のみであるから

$$x+\sqrt{-2}=(a+b\sqrt{-2})^3=a^3-6ab^2+(3a^2b-2b^3)\sqrt{-2}$$

が成り立つ. 従って $3a^2b-2b^3=b(3a^2-2b^2)=1$ より $b=\pm 1$ となるので $3a^2-2b^2=1$ を得る. 従って $b=1$, $a=\pm 1$ が成り立つ. これより $x=\pm 5$, $y=3$ が導かれる. ∎

定理 5.14 $x^2+5=y^3$ は整数解を持たない.

Proof $x^2+5=y^3$ をみたす有理整数 x,y が存在すると仮定する. このとき

$$x^2+5=(x+\sqrt{-5})(x-\sqrt{-5})=y^3$$

となる. $5\mid x$ と仮定すると $5\mid y$ より, $y^3\equiv 0 \pmod{25}$ となるが, $x^2+5\equiv 5 \pmod{25}$ となり, 矛盾が生じる. ゆえに $(5,x)=1$ である.

イデアル $(x+\sqrt{-5})$ と $(x-\sqrt{-5})$ の公約イデアルである素イデアルが存在したとして, それを P とする. P は $(2x)$, (10) の公約イデアルとなる. $(2x,10)=2(x,5)=2$ より P は (2) を割り切る. 補題5.11の証明中で示したように, $(2)=P_2^2$ が成り立つ. ここで $P_2=(2,1+\sqrt{-5})$ である. これより $P=P_2$ を得る. P は (y) を割り切るので y は偶数である. 従って $y^3\equiv 0 \pmod 8$ が成り立つ. 一方, x は奇数となるが, このとき $x^2+5\equiv 6 \pmod 8$ となり矛盾が生じる. よってイデアル $(x+\sqrt{-5})$ と $(x-\sqrt{-5})$ の公約イデアルは (1) のみである.

上の結果より, 単項イデアル $(x+\sqrt{-5})$ はあるイデアル J の 3 乗として表される. ここで $(x+\sqrt{-5})=J^3$ とおく. 補題5.11より $\mathbb{Q}(\sqrt{-5})$ の類数は 2 であるから, 定理5.8より J^2 は単項イデアルとなる. ゆえに J 自身が単項イデアルである. 今 $J=(a+b\sqrt{-5})$ とおけば単数は ± 1 のみであるから

$$x+\sqrt{-5}=(a+b\sqrt{-5})^3=a^3-15ab^2+(3a^2b-5b^3)\sqrt{-5}$$

より $3a^2b-5b^3=b(3a^2-5b^2)=1$ が得られる. これより $b=\pm 1$ が導かれる. 従って $3a^2=5\pm 1$ となるがこれをみたす有理整数 a,b は存在しない. 以上で定理が証明された. ∎

References

[1] 高木貞治, 「初等整数論講義」第 2 版, 共立, 1971.

[2] 永尾 汎, 「代数学」朝倉, 1983.

[3] 山本芳彦, 「数論入門１」岩波, 1996.

[4] 山本芳彦, 「数論入門２」岩波, 1996.

[5] H.Chatland, H.Davenport, *Euclid's algorithm in real quadratic fields* , Canadian Journal of Mathematics, 2 (1950), pp. 289-296.

[6] H.M. Stark, *A complete determination of the complex quadratic fields of class-number one*, Michigan Mathematical Journal, 14 (1967), pp. 1-27.