素因数分解と代数体

雪江明彦

京都大学院理学研究科

2012年8月8日

本日の予定

- 整数論とは
- 代数体と代数的整数
- 素因数分解の一意性
- 2 次形式と類数
- 代数的対象のパラメータ化

記号

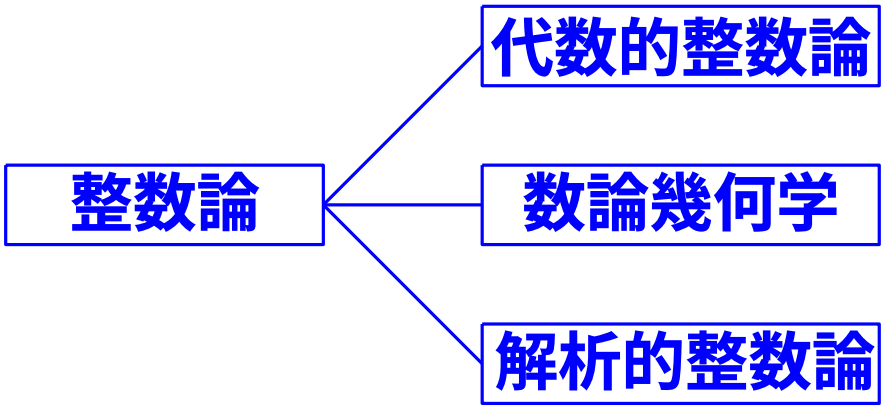
- $\mathbb{Z}$　整数の集合
- $\mathbb{Q}$　有理数の集合　$\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$
- $\mathbb{R}$　実数の集合　$\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$
- $\mathbb{C}$　複素数の集合　$\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$

整数論とは

整数 $1, 2, 3 \cdots$ について

- 割り算の余り，**素因数分解**
- 方程式の**整数解**
- 代数的対象の**分布**

などを調べる数学の 1 分野.



割り算の余り – 百五間算

問題　整数 n で
n を 3 で割った余りが 2
n を 5 で割った余りが 3
n を 7 で割った余りが 1
であるものを全て求めよ.

解答 $n = 8 + 105m$ $m = \cdots, -2, -1, 0, 1, 2, \cdots$
どのような余りを指定しても解答を見つける方法が既に，**紀元前 3 世紀頃，中国**で見つけられていた.

合同式

$a, b \in \mathbb{Z}$ を $n \in \mathbb{Z}$ で割った余りが等しいとき

$$a \equiv b \mod n$$

と書き，a, b は n を法として合同という.

$$a_1 \equiv b_1,\ a_2 \equiv b_2 \mod n$$
$$\Rightarrow a_1 + a_2 \equiv b_1 + b_2 \mod n,$$
$$a_1 a_2 \equiv b_1 b_2 \mod n.$$

高いべきの計算に便利 → 暗号理論

$5^{130} \mod 13$ を計算

$$5^2 \equiv 12,\ 5^4 \equiv 1,\ 5^8 \equiv 1, \ldots, 5^{128} \equiv 1,\ 5^{130} \equiv 5^2 \equiv 12$$

不定方定式とは

不定方定式とは整数係数の方程式で，**整数解，有理解**を求めることを期待されるもの.

例

1. p: 奇素数 $p = x^2 + y^2$ となる整数 x, y はあるか?
2. $y^2 = x^3 - x$ となる有理数 x, y はあるか？

2. については整数解について後で解説.

不定方定式 $p = x^2 + y^2$

答え: p を 4 で割った余りが 1 のときのみ Yes

$$5 = 2^2 + 1^2,$$

$$89 = 5^2 + 8^2$$

$p = x^2 + y^2$

x 偶数，y 奇数 としてよい

$$x = 2\ell \Rightarrow x^2 = 4\ell$$
$$y = 2m + 1 \Rightarrow y^2 = 4(m^2 + m) + 1$$

$p = x^2 + y^2$ なら 4 で割ると 1 余る

$$\mathbb{Z}[\sqrt{-1}] = \{x + y\sqrt{-1} \mid x, y \in \mathbb{Z}\}$$

$\mathbb{Z}[\sqrt{-1}]$ では**素因数分解**のようなことができる.

$p = x^2 + y^2$

$$-1 \equiv a^2 \mod p$$

となる a はあるか? $\Rightarrow$ 平方剰余の概念
$p = 4m + 1$ なら上のような a があることがわかり，

$$p|(a + \sqrt{-1})(a - \sqrt{-1})$$

しかし p は

$$a + \sqrt{-1}, a - \sqrt{-1}$$

どちらも割らず p は $\mathbb{Z}[\sqrt{-1}]$ では素数でない.

$p = x^2 + y^2$

$\mathbb{Z}[\sqrt{-1}]$ で素因数分解

$$p = (x + y\sqrt{-1})(z + w\sqrt{-1})$$

p が実数なので $z + w\sqrt{-1} = x - y\sqrt{-1}$

$$\Rightarrow p = x^2 + y^2$$

楕円曲線

楕円曲線 とは: k: 定数

$$y^2 = (1 - x^2)(1 - k^2x^2)$$

を満たす (x, y) の集合. 変数変換で

$$y^2 = x^3 + ax + b$$

とも表せる.

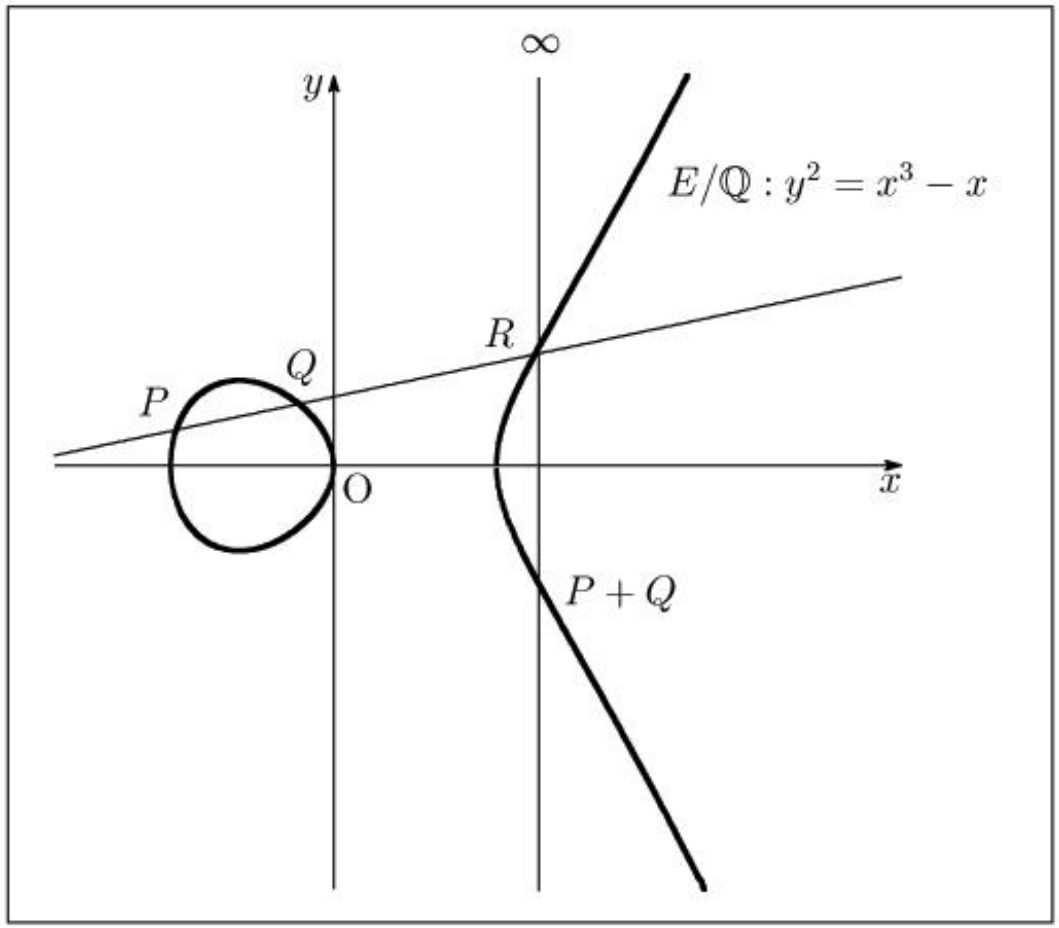
楕円曲線の有理解の例

$y^2 = x^3 - x$ の有理解は？

答え: $(x, y) = (0, 0), (1, 0), (-1, 0)$

楕円曲線

楕円曲線上である意味で『足し算』を定義することができる.



楕円曲線

$y^2 = x^3 + 17$ を考える.

$$P_1 = (-2, 3),\ P_2 = (2, 5)$$

上の楕円曲線上の点 $P = (x, y)$ で $x, y \in \mathbb{Q}$ であるものは全て

$$P = [m]P_1 + [n]P_2$$

という形をしている.

Mordell-Weil **の定理**: 楕円曲線の有理点の集合は有限生成である.

楕円曲線の有理点を全てもとめるアルゴリズムは知られていない. いまだに数学者の研究対象となっている.

解析的整数論

素数が無限個ある.

$$p_1, \cdots, p_N \text{ 素数}$$
$$\Rightarrow p_1 \cdots p_N + 1 \text{は } p_1, \cdots, p_N \text{ で割り切れない.}$$

問題: a, b 整数　$p = a + bm\ (m \in \mathbb{Z})$ という形の素数は無限個あるか?

$d|a, b$ なら $d|a + bm$ なので，a, b は互いに素とする.

Dirichlet の算術級数定理:
$p = a + bm\ (m \in \mathbb{Z})$ という形の素数は無限個ある.

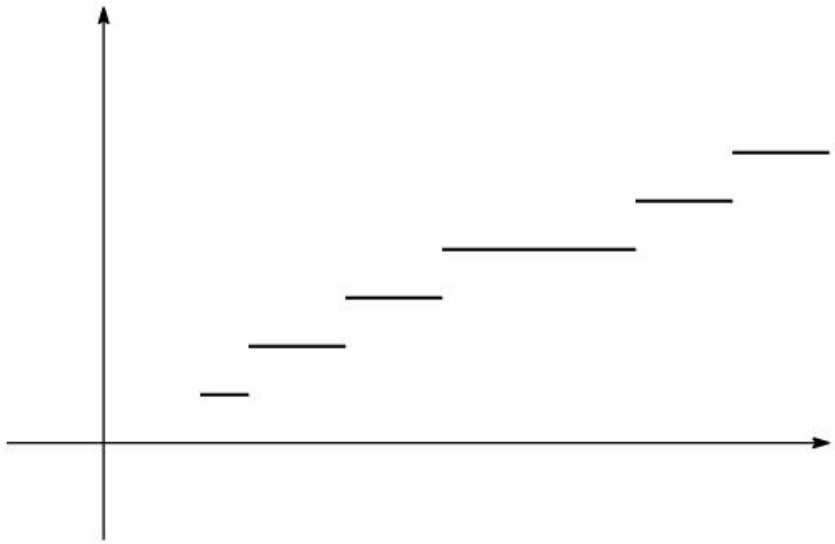
この定理の証明には微分，積分を使う.

解析的整数論

微分，積分のような解析を使って整数論を研究する分野のことを**解析的整数論**という.

$\pi(x) = x$ 以下の素数の個数.

$$\pi(3) = 2,\ \pi(4.5) = 2,\ \pi(10) = 4,\ \pi(20) = 8$$



解析的整数論

素数定理: $\displaystyle\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$

この定理は 100 年以上前に証明されたが，その証明には Riemann **のゼータ関数** というものを使う.

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$$

とおいてこれを Riemann のゼータ関数という. $s > 1$ なら右側は収束する.

解析的整数論

実は $\zeta(s)$ は $s = 1$ を除く全ての**複素数 s の関数**として拡張することができる.

Riemann **予想**: s の実数部が $[0, 1]$ にあるとき、
$\zeta(s) = 0$ になるのは s の実数部が $\frac{1}{2}$ であるときに限る.

この問題はクレイ社が出した 100 万ドルの懸賞金つきの 7 つの問題のうちの一つ (ただし問題はずっと前からある.)

代数体

定義: 最高次の係数が 1 の整数係数多項式の根を**代数的整数**という.

例: 1. $(\sqrt{-1})^2 + 1 = 0$ なので，$\sqrt{-1}$ は代数的整数.
2. $\sqrt[3]{2}$
3. $x^3 + x^2 - 2x - 1$ の根 (実は $2\cos 2\pi/7$)
4. $1/\sqrt{2}$ は No.

定義: $\mathbb{C}$ の部分集合で 0 で割る以外の加減乗除ができ，$\mathbb{Q}$ 上有限次元ベクトル空間であるものを**代数体**という.

代数体

代数体の例

1. $\mathbb{Q}(\sqrt{-1}) = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\}$
2. $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{15})$ など同様
3. $\mathbb{Q}(\sqrt[3]{2}) = \{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4} \mid a_0, a_1, a_2 \in \mathbb{Q}\}$
4. p 素数, $\zeta = \exp(2\pi\sqrt{-1}/p)$

$$\mathbb{Q}(\zeta) = \{a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \mid a_0, \ldots, a_{p-2} \in \mathbb{Q}\}$$

ζ は $i = 1, \ldots, p-1$ なら $\zeta^i \neq 1$, $\zeta^p = 1$ という性質を満たす.

代数体の整数環

定義: K が代数体なら K に含まれる代数的整数の集合を $\mathcal{O}_K$ と書き，K の**代数的整数環**という.

例: $\mathbb{Q}(\sqrt{-1})$ の代数的整数環は

$$\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}.$$

問題: $\mathcal{O}_K$ で素因数分解が一意的にできるか?

$\mathbb{Z}[\sqrt{-1}]$ では Yes.
$\mathbb{Z}[\sqrt{-5}]$ では No.

素因数分解の一意性

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

2, 3 はそれ以上分解できない数.

$$2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$$

なら絶対値の 2 乗をとり

$$4 = (a^2 + 5b^2)(c^2 + 5d^2)$$

$$\Rightarrow b = d = 0,\ 4 = a^2c^2$$

$$a = \pm 1 \text{ または } c = \pm 1$$

$3, 1 \pm \sqrt{-5}$ も同様.

素因数分解の一意性

$\mathcal{O}_K$ で素因数分解の一意性がどれだけ成り立たないかを表す量がある → **類数**. 定義は「分数イデアルのなす群を単項イデアルのなす部分群で割った剰余群の位数」
類数が $1 \Rightarrow \mathcal{O}_K$ で素因数分解の一意性が成り立つ.

例: 1. $\mathbb{Q}$ の類数は 1
2. $\mathbb{Q}(\sqrt{-1})$ の類数は 1
3. $\mathbb{Q}(\sqrt{-5})$ の類数は 2
4. $\mathbb{Q}(\sqrt[3]{2})$ の類数は 1

類数 1 の代数体が無限個あるかどうかは未解決問題

素因数分解の重要性

- 暗号理論で有名な RSA 暗号は大きい整数 (600 桁くらい) n の素因数分解の困難さに依存する.
- 整数 n の素数判定を $(\log n)^{19}$ 時間で行うアルゴリズム (AKS アルゴリズム) が発見された. しかしそれほどは速くない.
- 確率論的アルゴリズムだが,「数体ふるい法」で 200 桁くらいの整数が素因数分解されたことがある.

不定方定式 $y^2 = x^3 - x$ の整数解
(有理数解はもう少し難)

定理: $y^2 = x^3 - x$ の整数解は $(\pm 1, 0), (0, 0)$ だけ.

証明:

$$x^3 - x = x(x+1)(x-1)$$

$x, x+1$ は互いに素
$x, x-1$ は互いに素
$x+1, x-1$ は 2 以外の公約数を持たない.

$$(*) \Rightarrow \begin{cases} x = t^2, \\ x+1 = s^2, \\ x-1 = u^2 \end{cases} \text{ または } \begin{cases} x = t^2, \\ x+1 = 2s^2, \\ x-1 = 2u^2 \end{cases}$$

$y^2 = x^3 - x$

後者だけ考える.

$$t^2 + 1 = 2s^2,\ t^2 - 1 = 2u^2$$

$$\Rightarrow s^2 = u^2 + 1$$

$$\Rightarrow (s - u)(s + u) = 1$$

$$\Rightarrow s - u = s + u = 1$$

または $s - u = s + u = -1$.

どちらの場合も $u = 0, t^2 = 1$. よって,

$$(x, y) = (1, 0). \qquad \text{(証明終)}$$

(*) で素因数分解の一意性を使った.

フェルマー予想の第一の場合

フェルマー予想の第一の場合は素因数分解の一意性を同じような状況で使う例.
フェルマー予想はワイルスにより証明されたが，古典的にはクンマーにより次の定理が基本

定理: p 奇素数 $\zeta = e^{2\pi\sqrt{-1}/p}$, $K = \mathbb{Q}(\zeta)$ の類数が p で割れないとする. このとき，

$$x^p + y^p = z^p$$

の整数解 (x, y, z) で $xyz \neq 0$ であり, x, y, z が p で割れないものはない.

フェルマー予想の第一の場合

ただし

$$\mathbb{Q}(\zeta) = \{a_0 + a_1\zeta + \cdots + a_{p-2} \mid a_0, \ldots, a_{p-2} \in \mathbb{Q}\},$$
$$\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + \cdots + a_{p-2} \mid a_0, \ldots, a_{p-2} \in \mathbb{Z}\}.$$

$K = \mathbb{Q}(\zeta)$ なら $O_K = \mathbb{Z}[\zeta]$
(x, y, z) 定理の条件を満たすとする.

$$\prod_{i=0}^{p-1}(x + \zeta^i y) = z^p$$

フェルマー予想の第一の場合

$\mathbb{Z}[\zeta]$ では素因数分解の一意性は成り立たないが，仮定を使うと，素因数分解の一意性が成り立つ場合と同様の考察で $i \neq j$ なら $x + \zeta^i y, x + \zeta^j y$ が互いに素で

$$x + \zeta^i y = \text{逆数を持つ数} \times p \text{ 乗数}$$

となり，これを出発点として定理を証明できる.

類数が関係するその他の不定方定式

1. $p = x^2 - dy^2$

$\mathbb{Q}(\sqrt{d})$ の類数と $d \equiv a^2 \mod p$ となるかが関係

2. $3x^3 + 4y^3 + 5z^3 = 0$

セルマーの例　$\mathbb{Q}(\sqrt[3]{6})$ の類数が 1 であることが使われる.

類数の計算法

- 「ミンコフスキーの定理」を使って，原理的には計算できる. (コンピューターにより計算可能)
- $\mathbb{Q}(\sqrt{d})$ の場合には，ガウスによる 2 次形式の理論で計算できる.
- $\mathbb{Q}(\sqrt{d})$ の場合には,「ディリクレの類数公式を」使うこともできる. これは解析的な方法. → 最近は「p 進」の公式も調べられる.

2次形式と類数

$$f_x(u,v) = x_0u^2 + x_1uv + x_2v^2 \ (x_0, x_1, x_2 \in \mathbb{Z})$$

という形の多項式を**整数係数2変数2次形式**という
$D = x_1^2 - 4x_0x_1$ はその**判別式**という.
簡単のため $d < 0$ を 4 で割った余りは $2, 3$ と仮定.
$D = 4d$.

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \middle| \begin{array}{l} \alpha, \beta, \gamma, \delta \in \mathbb{Z} \\ \alpha\delta - \beta\gamma = 1 \end{array} \right\}$$

例えば $\begin{pmatrix} 2 & 3 \\ -1 & -1 \end{pmatrix}$ は $\mathrm{SL}_2(\mathbb{Z})$ の元.

2次形式とガウス

$\mathrm{SL}_2(\mathbb{Z})$ の元は2次形式の集合に

$$f_x \mapsto f_x(au + cv, bu + dv)$$

という変数変換を引き起こす.

定義: 2次形式は x_0, x_1, x_2 の最大公約数が 1 のとき，**原始的**という.

例: $2u^2 + 6uv - 4v^2$ は原始的でない.
$u^2 - 3v^2$ は原始的.

$F_{\mathrm{pr}}(D)$ 判別式 $D = 4d$ の原始的な2次形式の集合.

2 次形式とガウス

定理 (ガウス): $\mathbb{Z}[\sqrt{d}]$ **の類数は** $\#\mathrm{SL}_2(\mathbb{Z})\backslash F_{\mathrm{pr}}(D)$.

類数が 2 次形式により解釈できた.

密度定理

類数は $\mathbb{Z}[\sqrt{d}]$ ではなく $\mathbb{Q}(\sqrt{d})$ に対して定まる数.

$$D = \begin{cases} d & d \equiv 1 \mod 4, \\ 4d & d \equiv 2, 3 \mod 4 \end{cases}$$

$\mathbb{Q}(\sqrt{D})$ の類数 h_D とすると，解析的な考察が可能.

定理: $\sum_{0<-D<X} h_D \sim CX^{\frac{3}{2}}$

$$C = \frac{\pi}{18} \prod_p (1 - p^{-2} - p^{-3} + p^{-4})$$

これはもともとはガウス予想 ($D = m^2 D'$ の曖昧さあり)

密度定理

Lipschutz 1865 $D < 0$ の場合
Siegel 1944 n 変数, $D > 0$ 含む
Goldfeld–Hoffstein 1985 曖昧さなし
早坂–雪江 2008 (n 変数曖昧さなし)

類数の計算

$b^2 - 4ac = D < 0$ とする. ($D > 0$ の場合も考察可能.)

定義 $f(x,y) = ax^2 + bxy + cy^2$ が**簡約**であるとは

(i) $c > a \geqq b > -a$ または

(ii) $c = a \geqq b \geqq 0$.

簡約なら

$$0 \leqq b \leqq a \leqq c \Rightarrow 3b^2 = 4b^2 - b^2 \leqq 4ac - b^2 = |D|$$

$$\Rightarrow |b| \leqq \sqrt{|D|/3}$$

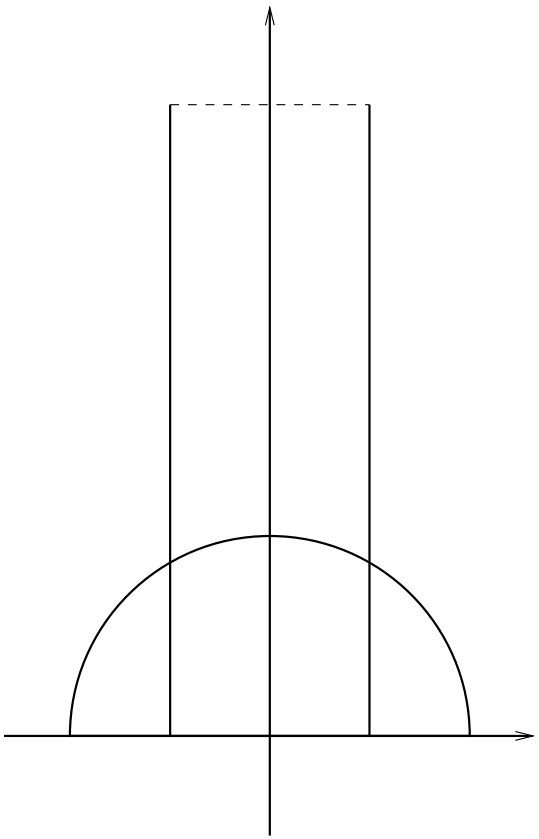
b の可能性有限個

$4ac = b^2 - D$

a, c の可能性も有限個

類数の計算

$f(x,y)$ が簡約 $\Leftrightarrow$ $(-b+\sqrt{D})/2a$ が $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ の基本領域



類数の計算

定理 $(D<0)$ 判別式 $D<0$ の簡約な f の数は $\mathbb{Q}[\sqrt{d}]$ の類数 である.

例 $d=-5$ $D=-20$

$|b| \leqq \sqrt{20/3} = 2.**$

$b = 0, \pm 1, \pm 2$

$4ac = b^2 + 20 \Rightarrow b$ は偶数

$b=0$ なら　$ac = 5$ (よって $a \neq c$)

(i) $c > a > -a \Rightarrow c = 5, a = 1$

$b = 2$ なら $ac = 6$ $(a \neq c)$

(i) $c > a \geqq 2 > -a \Rightarrow c = 3,\ a = 2$

(i) $b = -2$ はない.

$\mathbb{Q}[\sqrt{-5}]$ の類数は 2

類数の計算

$\mathbb{Q}(\sqrt{-13})$ の類数を計算してみましょう!

数論的対象のパラメータ化

$\mathbb{Q}(\sqrt{d})$ の類数を 2 次形式で計算できた理由:

2 変数 2 次形式と変数変換を考えると，

$\mathbb{Q}(\sqrt{d})$ の「乗法群」がパラメータ化ができる.

平方根のパラメータ化

$a, b \in \mathbb{Q}$ なら，$\sqrt{a}$ と $\sqrt{b}$ はいつ『整数論的』に同じか?

$$\sqrt{18} = 3\sqrt{2}$$

$a, b \in \mathbb{Q}^\times$, $a = t^2 b$ $(t \in \mathbb{Q}^\times)$ なら $\sqrt{a}$ と $\sqrt{b}$ は本質的に同じとみなす.

3次方定式のパラメータ化

3次方程式の解はいつ『同じ』か?

$$f_x(u,v) = x_0u^3 + \cdots + x_3v^3$$

$$x_0, \ldots, x_3 \in \mathbb{Q}$$

$f_x(u,1) = 0$ の一つの解を α_x.

$$\left\{a_0 + a_1\alpha_x + a_2\alpha_x^2 \mid a_0, a_1, a_2 \in \mathbb{Q}\right\}$$

という形の複素数の集合を $K(x)$.
解を選べば $K(x) = K(y)$ となるとき f_x, f_y は同じとみなす.
定理: $K(x) = K(y)$ なら，変数変換により f_x は f_y の定数倍になる.

3次方定式のパラメータ化

証明: $x_0 = 1$ 仮定, $c_0, c_1, c_2 \in \mathbb{Q}$ $\alpha_y = c_0\alpha_x^2 + c_1\alpha_x + c_2$ とする.

$$\alpha_y = \frac{A\alpha_x + B}{C\alpha_x + D}$$

となる $A, B, C, D \in \mathbb{Q}$ をみつけたい.

3次方定式のパラメータ化

$C, D \in \mathbb{Q}$ なら

$$\begin{aligned}(C\alpha_x + D)\alpha_y &= (C\alpha_x + D)(c_0\alpha_x^2 + c_1\alpha_x + c_2)\\ &= Cc_0\alpha_x^3 + (Cc_1 + Dc_0)\alpha_x^2 + 1\text{次}\\ &= (Cc_1 + Dc_0 - Cc_0x_1)\alpha_x^2 + 1\text{次}\end{aligned}$$

$c_0 = 0$ なら，α_y は α_x の1次式.
$c_0 \neq 0$ なら，$Cc_1 + Dc_0 - Cc_0x_1 = 0$ となるように D を選ぶ.

3 次方定式のパラメータ化

どちらの場合も

$$\alpha_y = \frac{A\alpha_x + B}{C\alpha_x + D}$$

という形. 証明ほぼ終わり.

3 次方程式の解 (同一視はする)
$\Leftrightarrow$ {3 次式 }/変数変換

4次方定式のパラメータ化

$$f_x(u,v) = x_0u^4 + \cdots + x_4v^4$$

の場合は u, v の変数変換を考えてもうまくいかない.
$w = u^2$ とおくと，$f_x(u,1) = 0$ は

$$x_0w^2 + x_1uw + x_2u^2 + x_3u + x_4 = 0$$

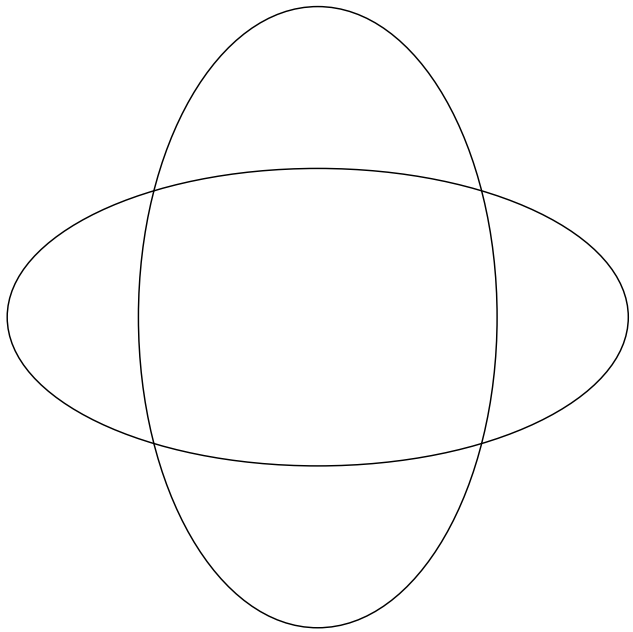
u_1, u_2, u_3 変数

$$Q_{x,1}(u_1,u_2,u_3) = \sum_{i \leqq j} x_{1,ij}u_iu_j,$$

$$Q_{x,2}(u_1,u_2,u_3) = \sum_{i \leqq j} x_{2,ij}u_iu_j$$

4次方定式のパラメータ化

として $Q_1(u_1, u_2, 1) = Q_2(u_1, u_2, 1) = 0$ を考えるのと同じ.



4 次方定式のパラメータ化

$Q_{x,1}, Q_{x,2}$ には合計 12 個の係数がある. $x = (x_{i,jk})$ は $\mathbb{Q}$ 上 12 次元のベクトル空間 V になる.

- 3 変数の変数変換
- $Q_{x,1}, Q_{x,2}$ の間の変形

定理 (Wright–雪江, 1992):
$\exists V' \subset V$, V'/変数変換 は 4 次方程式の解を本質的に表す.

Ferrari 1545 年頃: 4 次方程式の根号による解
Omar Khayyam 11 世紀後半: 4 次方程式の二つの 2 次曲線による解釈

5 次方定式のパラメータ化

5 次方程式の解も群の作用の軌道で解釈できる.

$$u^5 + \cdots + x_5 = 0$$

$$\Rightarrow (u + x_1)(u^2)^2 + (x_2u + x_3)u^2 + (x_4u + x_5) = 0$$

と解釈するところから始めて，
V 5 × 5 交代行列 の四つの組
とすると，V は 40 次元のベクトル空間.
定理 (Wright–雪江, 1992):
$^{\exists}V' \subset V$, V'/変数変換 は 5 次方程式の解を本質的に表す.

5次方定式のパラメータ化

交代行列とは

$$\begin{pmatrix} 0 & 1 & 2 \\ -1 & 0 & 3 \\ -2 & -3 & 0 \end{pmatrix}$$

(これは 3×3 の場合) といった行列.