ガウスの2次形式論とクロネッカー·ウェーバーの定理についての考察

三浦 正道

新潟大学大学院自然科学研究科数理物質科学専攻

2016/02/09

修士論文について

修士論文目次

- 準備 (初等整数論, 代数的整数論, ガロア理論, ヒルベルトの理論)
- ガウスの 2 次形式論 (2 章) §1
- クロネッカー · ウェーバーの定理 (3 章) §2
- 考察と具体例 (4 章) §3
- 今後の研究について (5 章) §4

§1 (1/4)

2 元 2 次形式 $f(x,y) = ax^2 + bxy + cy^2 \quad (a,b,c \in \mathbb{Z})$ に対し,

定義

(1) $D_f := b^2 - 4ac$ を f の判別式という.
(2) $\gcd(a,b,c) = 1$ であるとき, f を原始形式という.
(3) f が $n \in \mathbb{Z}$ を原始的に表現する
$\overset{\text{def}}{\iff} \exists (x,y) \in \mathbb{Z}^2$ s.t. $\gcd(x,y) = 1,\ f(x,y) = n.$

2 つの 2 元 2 次形式 f, g に対し, 同値関係を導入する.

定義

$$f \sim g \overset{\text{def}}{\iff} \exists \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \text{ s.t. } g(x,y) = f\left(\begin{pmatrix} x & y \end{pmatrix} {}^t \begin{pmatrix} p & q \\ r & s \end{pmatrix} \right).$$

- $f \sim g \Longrightarrow D_f = D_g$.
- f : 原始形式かつ $f \sim g \Longrightarrow g$: 原始形式.

§1 (2/4)

- D : $D \equiv 0, 1 \pmod 4$ となる整数.
- $f(x, y) = a_1x^2 + b_1xy + c_1y^2$, $g(x, y) = a_2x^2 + b_2xy + c_2y^2$: 判別式 D をもつ 2 元 2 次形式

定義

$\gcd(a_1, a_2, \frac{b_1+b_2}{2}) = 1$ を満たすと仮定する.
演算 $\circ$ を, 次のように定義する:

$$(f \circ g)(x, y) := a_3x^2 + b_3xy + c_3y^2.$$

ただし, $a_3 = a_1a_2$, b_3 は a_i, b_i, c_i から求められる整数, $c_3 = \frac{b_3^2-D}{4a_3}$ である.

§1 (3/4)

- $P_D := \{f(x,y) = ax^2 + bxy + cy^2 \mid \gcd(a,b,c) = 1, D_f = D\}$. ($D$: $D \equiv 0, 1 \pmod 4$ となる整数)
- $P_D/\sim$ は有限アーベル群をなす.

単位元は,

$$e = \begin{cases} x^2 - \frac{D}{4}y^2 & (D \equiv 0 \pmod 4) \\ x^2 + xy + \frac{1-D}{4}y^2 & (D \equiv 1 \pmod 4) \end{cases}$$

である.
$f(x,y) = ax^2 + bxy + cy^2$ に対する逆元は,

$$f^{-1}(x,y) = ax^2 - bxy + cy^2$$

である.

§1 (4/4)

- F : $\mathbb{Q}$ 上の 2 次体.

定理

2 次体 F の整数環 $\mathfrak{O}_F$ のイデアルは, 2 元 2 次形式と対応している.

$$\begin{array}{ccc} \mathfrak{O}_F & & P_{\Delta_F} \\ \cup & & \Cup \\ \mathfrak{a} & \longmapsto & f_{\mathfrak{a}} \\ \mathfrak{a}_f & \longleftarrow\!\shortmid & f \end{array}$$

- $Cl_F^+ \simeq P_{\Delta_F}/\sim$.

定理 (クロネッカー・ウェーバーの定理)

有理数体 $\mathbb{Q}$ 上のアーベル体は円分体に含まれる.

$$\begin{array}{l} \mathbb{Q}(\zeta_n) \quad \exists n \in \mathbb{N} \\ \Big| \\ K \\ \Big| \qquad \mathrm{Gal}(K/\mathbb{Q}) : \text{アーベル群} \\ \mathbb{Q} \end{array}$$

§3 (1/2)

$F = \mathbb{Q}(\sqrt{-5})$ を考える. この 2 次体に対応する 2 元 2 次形式は,

$$x^2 + 5y^2, 2x^2 + 2xy + 3y^2$$

の 2 つである. 特に, 単位元 $x^2 + 5y^2$ が原始的に表現する奇素数について,

$$x^2 + 5y^2 = p \Longleftrightarrow p \equiv 1, 9 \pmod{20}$$

である.

§3 (2/2)

体の拡大:

$$F = \mathbb{Q}(\sqrt{-5})$$
$$\Big|$$
$$\mathbb{Q}$$

§3 (2/2)

体の拡大:

$$\begin{array}{ll} \mathbb{Q}(\sqrt{-5},\sqrt{-1}) & F \text{ のヒルベルト類体} \\ \Big| & \\ F=\mathbb{Q}(\sqrt{-5}) & \\ \Big| & \\ \mathbb{Q} & \end{array}$$

§3 (2/2)

体の拡大:

$\mathbb{Q}(\zeta_{20})$ クロネッカー・ウェーバー

|

$\mathbb{Q}(\sqrt{-5}, \sqrt{-1})$ F のヒルベルト類体

|

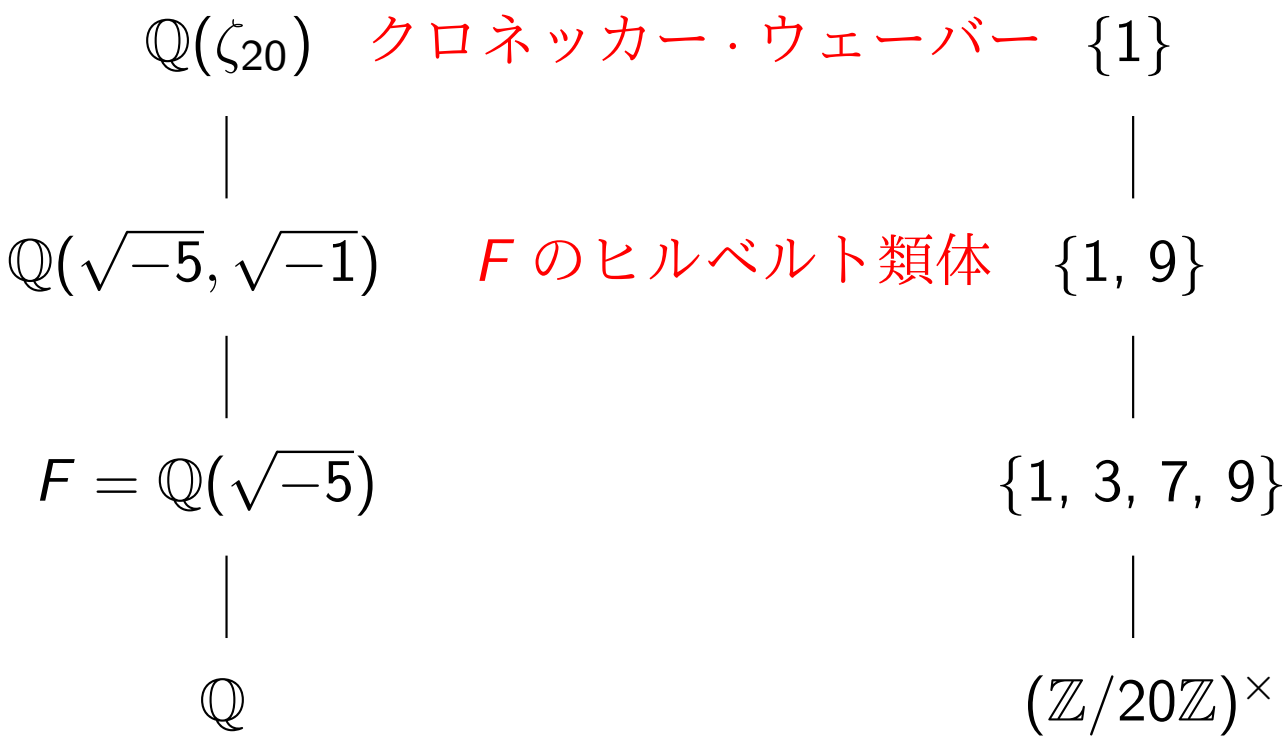
$F = \mathbb{Q}(\sqrt{-5})$

|

$\mathbb{Q}$

§3 (2/2)

ガロア対応:


$\mathbb{Q}(\zeta_{20})$
クロネッカー・ウェーバー
$\{1\}$
$\mathbb{Q}(\sqrt{-5}, \sqrt{-1})$
F のヒルベルト類体
$\{1, 9\}$
$F = \mathbb{Q}(\sqrt{-5})$
$\{1, 3, 7, 9\}$
$\mathbb{Q}$
$(\mathbb{Z}/20\mathbb{Z})^\times$

§4 (1/10)

課題

3 次体のイデアルは 2 次体と同じように対応できるのか？

予想

3 次体 F の整数環 $\mathfrak{O}_F$ のイデアルは, 2 元 3 次形式と対応している (？)

$$\begin{array}{ccc} \mathfrak{O}_F & & P_{\Delta_F} \\ \cup & & \Psi \\ \mathfrak{a} & \longleftrightarrow & ax^3+bx^2y+cxy^2+dy^3 \end{array}$$

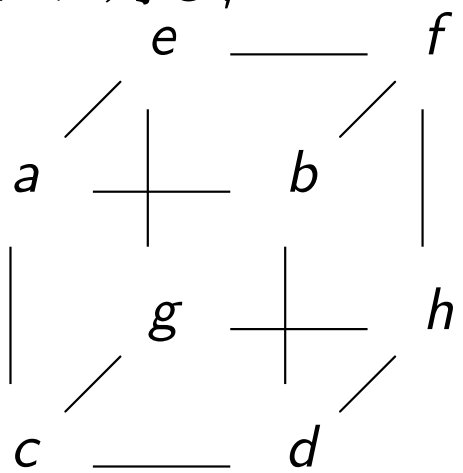
§4 (2/10)

マンジュル・バルガヴァは以下の論文を元に, フィールズ賞を受賞した.

- M. Bhargava, *Higher composition laws I: A new view on Gauss composition, and quadratic generations*, Ann. of Math. (2) **159** (2004), 217–250.
- M. Bhargava, *Higher Composition laws II: On cubic analogues of Gauss composition*, Ann. of Math. (2) **159** (2004), 865–886.
- M. Bhargava, *Higher Composition laws III: The parametrization of quartic rings*, Ann. of Math. (2) **159** (2004), 1329–1360.

§4 (3/10)

$A = (a, b, c, d, e, f, g, h) \in \mathbb{Z}^8$ に対し,



を考える. 次の 6 つの行列

$$M_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad N_1 = \begin{pmatrix} e & f \\ g & h \end{pmatrix},$$

$$M_2 = \begin{pmatrix} a & c \\ e & g \end{pmatrix}, \quad N_2 = \begin{pmatrix} b & d \\ f & h \end{pmatrix},$$

$$M_3 = \begin{pmatrix} a & e \\ b & f \end{pmatrix}, \quad N_3 = \begin{pmatrix} c & g \\ d & h \end{pmatrix}$$

とする.

§4 (4/10)

- 3 つの 2 元 2 次形式 $Q_i^A(x,y) := -\det(M_i x - N_i y)$. $(i = 1,2,3)$
- 2 元 2 次形式での同値関係を立方体に拡張できる. その同値関係を $\sim'$ をする.

定理

$D_{Q_1^A} = D_{Q_2^A} = D_{Q_3^A}$.

- Q_1^A, Q_2^A, Q_3^A の判別式を立方体 A の判別式という.
- $C_D := \{A \in \mathbb{Z}^8 \mid Q_i^A \in P_D\}$. $(D : D \equiv 0,1 \pmod 4$ となる整数$)$

§4 (5/10)

- D : $D \equiv 0, 1 \pmod 4$ となる整数.
- $\exists A_0 \in C_D$ s.t. $Q_1^{A_0} = Q_2^{A_0} = Q_3^{A_0}$.
- $Q_{\mathrm{id},D} := Q_i^{A_0}$. $(i = 1, 2, 3)$

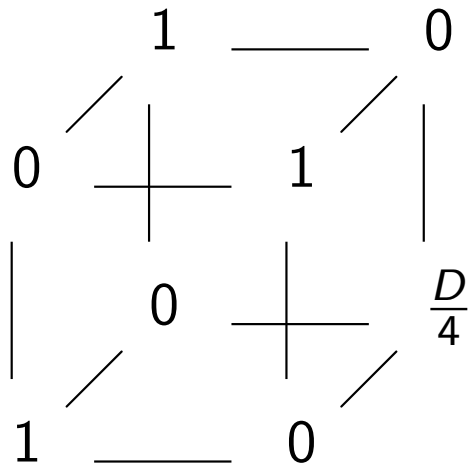
定理 (バルガヴァ, 2004, Theorem 1)

$P_D/\sim$ に対し, 以下の 3 つの条件を満たすような群の演算 $\cdot$ が一意に存在する:
(1) $\overline{Q_{\mathrm{id},D}}$ は単位元である;
(2) $\overline{Q_1^A} \cdot \overline{Q_2^A} \cdot \overline{Q_3^A} = \overline{Q_{\mathrm{id},D}}$; $(\forall A \in C_D)$
(3) $\overline{Q_1} \cdot \overline{Q_2} \cdot \overline{Q_3} = \overline{Q_{\mathrm{id},D}}$ となる Q_1, Q_2, Q_3 に対し,

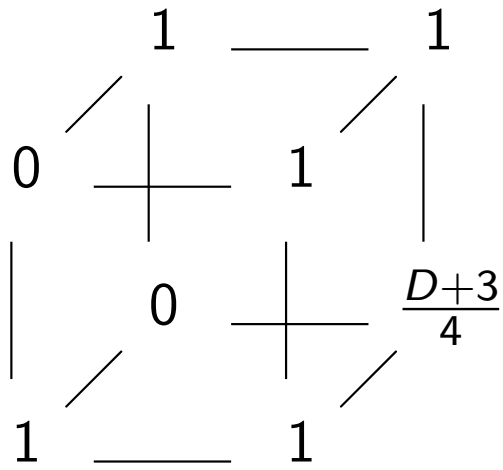
$$\exists 1 \overline{A} \in C_D/\sim \text{ s.t. } \overline{Q_1^A} = \overline{Q_1}, \overline{Q_2^A} = \overline{Q_2}, \overline{Q_3^A} = \overline{Q_3}.$$

立方体 A_0 を

$D \equiv 0 \pmod 4$



$D \equiv 1 \pmod 4$

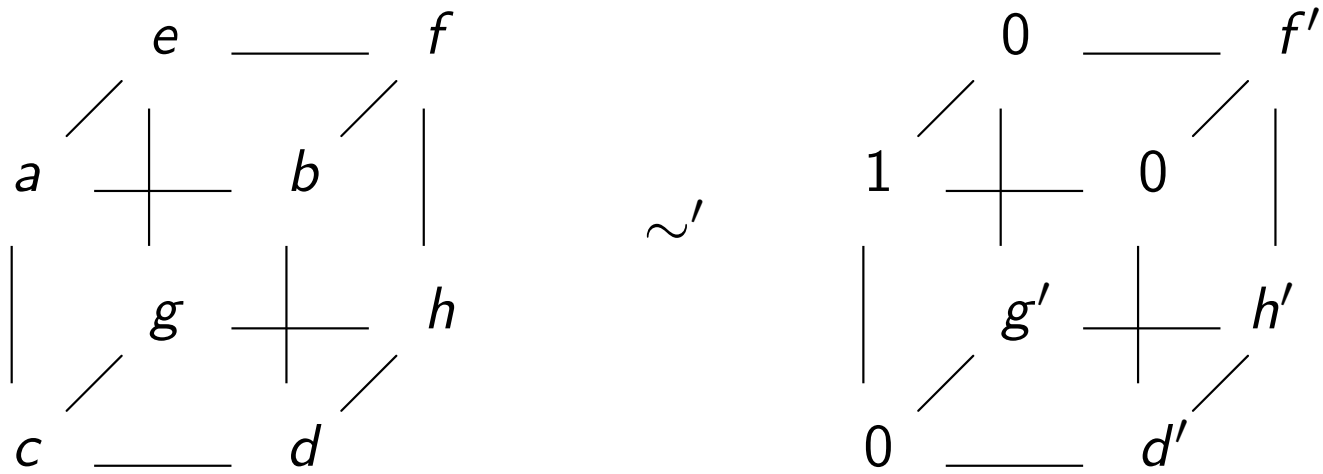


とする. これらを判別式 D の基本立方体という.

- $D \equiv 0 \pmod 4$ のとき, $Q_1^{A_0} = Q_2^{A_0} = Q_3^{A_0} = x^2 - \frac{D}{4}y^2$.
- $D \equiv 1 \pmod 4$ のとき, $Q_1^{A_0} = Q_2^{A_0} = Q_3^{A_0} = x^2 + xy + \frac{1-D}{4}y^2$.

§4 (7/10)

- $A = (a, b, c, d, e, f, g, h) \in C_D$.



- $\overline{Q_1^A} = -d'x^2 + h'xy + f'g'y^2, \overline{Q_2^A} = -g'x^2 + h'xy + d'f'y^2,$
  $\overline{Q_3^A} = -f'x^2 + h'xy + d'g'y^2.$
- $\overline{Q_1^A} \circ \overline{Q_2^A} = d'g'x^2 + h'xy - f'y^2 \sim -f'x^2 - h'xy + d'g'y^2 = \overline{Q_3^A}^{-1}.$
- $\overline{Q_1^A} \circ \overline{Q_2^A} \circ \overline{Q_3^A} = \overline{e}.$

- D : $D \equiv 0, 1 \pmod 4$ となる整数.
- $A_{\mathrm{id},D}$: 判別式 D の基本立方体.

定理 (バルガヴァ, 2004, Theorem 2)

集合 $C_D/\sim'$ に対し, 以下の 2 つの条件を満たすような群の演算が一意に存在する:
(1) $\overline{A_{\mathrm{id},D}}$ は単位元である;
(2) $i = 1, 2, 3$ に対し, $\overline{A} \mapsto \overline{Q_i^A}$ という写像は, $P_D/\sim$ への群準同型写像である.

- $\overline{A}, \overline{B} \in C_D/\sim'$.
- $\overline{Q_1^A} \circ \overline{Q_2^A} \circ \overline{Q_3^A} = \overline{Q_1^B} \circ \overline{Q_2^B} \circ \overline{Q_3^B} = \overline{e}$. (Theorem 1 (2) より)

$\overline{Q_i} = \overline{Q_i^A} \circ \overline{Q_i^B}$ とする. $(i = 1, 2, 3)$

- $\overline{Q_1} \circ \overline{Q_2} \circ \overline{Q_3} = \overline{e}$.
- $\exists 1 \overline{C} \in C_D/\sim'$ s.t. $\overline{Q_i^C} = \overline{Q_i}$. $(i = 1, 2, 3)$ (Theorem 1 (3) より)

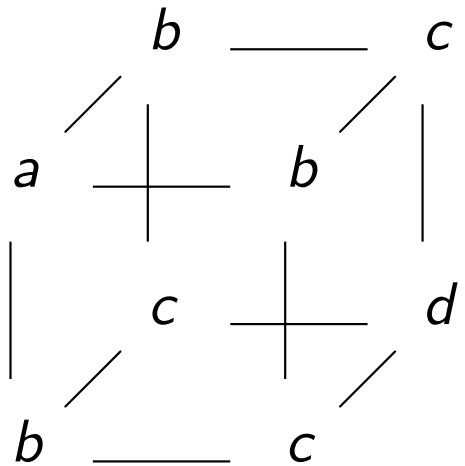
このとき, $\overline{A} \circ \overline{B} := \overline{C}$ と定義する.

§4 (10/10)

疑問

2 つの 2 元 3 次形式 f, g に対し,

$$f \circ g = \ ?$$



という形の立方体で考える.