Dirichlet の単数定理の Siegel による証明

MATHEMATICS.PDF

平成 18 年 12 月 1 日

目 次

1 はじめに

n を正の整数とする. K を n 次代数体とし, O_K を K の整数環とする.

K の元 α が K の単数であるとは, $\alpha \in O_K$ であって, ある $\beta \in O_K$ が存在して $\alpha\beta = 1$ が成り立つことである. K の単数の全体 $O_K^\times$ は $K^\times$ の部分群になる. そのため, $O_K^\times$ は K の単数群と呼ばれる.

Dirichlet[1]の単数定理とは, $O_K^\times$ の構造に関する定理である.

K から $\mathbb{Q}$ の代数的閉包 $\overline{\mathbb{Q}}$ の中への同型写像のことを K の共役写像という. K の共役写像は n 個ある.

σ を K の共役写像とする. $\sigma(K)$ が $\mathbb{R}$ に含まれるとき, σ は実であるといい, そうでないとき, σ は虚であるという.

K の共役写像 σ に対して,

$$\overline{\sigma} : K \longrightarrow \overline{\mathbb{Q}}, \quad \alpha \longmapsto \overline{\sigma(\alpha)}$$

もまた共役写像である. σ が実のときは $\sigma = \overline{\sigma}$, 虚のときは $\sigma \neq \overline{\sigma}$ である. 実共役写像の個数を r_1, 虚共役写像の個数を $2r_2$ とするとき, $n = r_1 + 2r_2$ が成り立つ.

[1]カタカナ表記は「ディリクレ」.

共役写像に番号をつけて, σ_1, σ_2, …, σ_{r_1} は実共役写像, σ_{r_1+1}, …, σ_n は虚共役写像であり, $\sigma_{r_1+r_2+i} = \overline{\sigma_{r_1+i}}$ $(i = 1, 2, \ldots, r_2)$ であるとする. σ_1 は K の恒等写像 id_K であるとする.

定理 1.1 (Dirichlet の単数定理)**.** K に属する 1 の根の全体を W_K とおく. W_K は有限巡回群である. $r = r_1 + r_2 - 1$ とおくと,

$$O_K^\times = W_K \times \mathbb{Z}^r$$

が成り立つ.

W_K は有限巡回群なので, その位数を q とすると, $W_K \cong \mathbb{Z}/q\mathbb{Z}$ が成り立つ. したがって,

$$O_K^\times = \mathbb{Z}/q\mathbb{Z} \oplus \mathbb{Z}^r$$

となる.

Dirichlet の単数定理を言い換えれば, K の単数 ε_1, …, $\varepsilon_r \in O_K^\times$ が存在して, 任意の K の単数 $\varepsilon \in O_K^\times$ は

$$\varepsilon = \zeta \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}, \quad \zeta \in W_K, \quad n_1, \ldots, n_r \in \mathbb{Z} \tag{1}$$

の形に一意的に表される. なお, このような性質をもつ単数の組 ε_1, …, ε_r を K の基本単数系という.

さて, Dirichlet の単数定理の証明の概略は次の通りである.

$\alpha \in K$ に対して $\alpha^{(i)} = \sigma_i(\alpha)$ とおく. そして, 群の準同型写像

$$\lambda : O_K^\times \longrightarrow \mathbb{R}^r, \quad \varepsilon \longmapsto (\log|\varepsilon^{(1)}|, \ldots, \log|\varepsilon^{(r)}|)$$

を考えると,

$$\ker \lambda = W_K$$

かつ

$$\lambda(O_K^\times) = \mathbb{Z}^r$$

である. そうすると, K の単数 ε_1, …, $\varepsilon_r \in O_K^\times$ が存在して, 任意の K の単数 $\varepsilon \in O_K^\times$ は (1) の形に一意的に表されることがいえる.

この文書で紹介する証明は, C. L. Siegel がかつて Göttingen で講義したときの方法と伝えられているものをもとにしている.

2 実行列

命題 2.1. 実数 $t \geq 1$, $u > 1$ に対して

$$t^u + 1 < (t+1)^u$$

が成り立つ.

証明. $f(t) = (t+1)^u - (t^u + 1)$ とおく. $u > 1$ より,

$$f(1) = 2^u - 2 > 0.$$

また, $t \geq 1$, $u > 1$ より,

$$\frac{d}{dt} f(t) = u\big((t+1)^{u-1} - t^{u-1}\big) > 0.$$

したがって $t \geq 1$, $u > 1$ のとき $f(t) > 0$ である. □

定理 2.2. m, n を正の整数とし, $m < n$ であるとする.

t を正の整数とする. また, $A = (a_{ij})$ を $m \times n$ 型の実行列とし,

$$a = \max_{1 \le i \le m} \sum_{j=1}^{n} |a_{ij}|$$

とおく.

このとき, $\mathbf{0}$ でない $\mathbb{Z}^n$ の元 $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ が存在して,

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix} = A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

とおくと

$$\max_{1 \le j \le n} |x_j| \le t, \tag{2}$$

$$\max_{1 \le i \le m} |y_i| \le 2at^{1-n/m} \tag{3}$$

が成り立つ.

証明. $m < n$ かつ $t \ge 1$ であるから, 命題 2.1 より,

$$t^{n/m} + 1 < (t+1)^{n/m}$$

が成り立つ. よって, ある整数 h をとって[2]

$$t^{n/m} \le h < (t+1)^{n/m} \tag{4}$$

すなわち

$$t^n \le h^m < (t+1)^n \tag{5}$$

となるようにできる.

立体[3]

$$I = \{(y_1, \ldots, y_m) \in \mathbb{R}^m \mid |y_i| \le at,\ i = 1, 2, \ldots, m\}$$

の各辺を h 個の等しい部分に分ける. そうすると, I は各辺の長さが $2at/h$ の h^m 個の部分立体に分けられる. 一方, $j = 1, 2, \ldots, n$ に対して, $x_j = 0, 1, \ldots, t$ をとることにより, $\mathbb{Z}^n$ の中に $(t+1)^n$ 個の点

$$\boldsymbol{x}_k = (x_{k,1}, \ldots, x_{k,n}), \quad k = 1, 2, \ldots, (t+1)^n$$

が存在する. これらの点 $\boldsymbol{x}_k$ に対して,

$$\begin{pmatrix} y_{k,1} \\ y_{k,2} \\ \vdots \\ y_{k,m} \end{pmatrix} = A \begin{pmatrix} x_{k,1} \\ x_{k,2} \\ \vdots \\ x_{k,n} \end{pmatrix} \tag{6}$$

[2]例えば, h として $t^{n/m} + 1$ を超えない最大の整数をとる.

[3]$m = 2$ のとき, I は辺の長さが $2at$ の正方形である. $m = 3$ のとき, I は辺の長さが $2at$ の直方体である.

とおくと, $i=1,2,\dots,m$ に対して $|y_{k,i}| \le at$ が成り立つ. よって $(y_{k,1}, y_{k,2}, \dots, y_{k,m}) \in I$ である. したがって (5) より, ある 2 つの点 $\boldsymbol{x}_{k_1}$, $\boldsymbol{x}_{k_2}$ が存在して, (6) のようにして $\boldsymbol{y}_{k_1}$, $\boldsymbol{y}_{k_2}$ を定めたとき, それらは I の同じ部分立体に入らなければならない.

$\boldsymbol{x} = (x_1, \dots, x_n) = \boldsymbol{x}_{k_1} - \boldsymbol{x}_{k_2}$ とおき, $\boldsymbol{x}$ に対して (6) のようにして $\boldsymbol{y} = (y_1, \dots, y_m)$ を定める. すると, $j=1,2,\dots,n$ に対して

$$|x_j| = |x_{k_1,j} - x_{k_2,j}| \le t$$

となっている. また,

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix} = A \begin{pmatrix} x_{k_1,1} - x_{k_2,1} \\ x_{k_1,2} - x_{k_2,2} \\ \vdots \\ x_{k_1,n} - x_{k_2,n} \end{pmatrix} = A \begin{pmatrix} x_{k_1,1} \\ x_{k_1,2} \\ \vdots \\ x_{k_1,n} \end{pmatrix} - A \begin{pmatrix} x_{k_2,1} \\ x_{k_2,2} \\ \vdots \\ x_{k_2,n} \end{pmatrix} = \begin{pmatrix} y_{k_1,1} - y_{k_2,1} \\ y_{k_1,2} - y_{k_2,2} \\ \vdots \\ y_{k_1,m} - y_{k_2,m} \end{pmatrix}$$

であるから, $i=1,2,\dots,m$ に対して

$$|y_i| = |y_{k_1,i} - y_{k_2,i}| \le \frac{2at}{h}$$

が成り立つ. 一方, (4) より,

$$\frac{2at}{h} \le 2at^{1-n/m}$$

である. ゆえに $i=1,2,\dots,m$ に対して

$$|y_i| \le 2at^{1-n/m}$$

が成り立つ. □

定理 2.3. $A = (a_{ij})$ は r 次の実正方行列で, 次の条件を満たすとする.

$$a_{ii} > 0 \quad (i = 1, \dots, r), \tag{7}$$

$$a_{ij} \le 0 \quad (i \ne j), \tag{8}$$

$$\sum_{j=1}^{r} a_{ij} > 0 \quad (i = 1, \dots, r). \tag{9}$$

このとき, $\det A \ne 0$ である.

証明. もし仮に $\det A = 0$ とすると, ある $\mathbf{0}$ でない列ベクトル

$$\boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{pmatrix}$$

が存在して, $A\boldsymbol{x} = \mathbf{0}$ でなければならない. $\boldsymbol{x}$ の成分のうち, 絶対値において最大のものを x_s とすると, $x_s \ne 0$ であり,

$$\sum_{j=1}^{r} a_{sj} x_j = 0$$

より

$$\begin{aligned} a_{ss} = |a_{ss}| &= \left| \sum_{\substack{1\le j\le r\\ j\neq s}} \frac{a_{sj}x_j}{x_s} \right| \\ &\le \sum_{\substack{1\le j\le r\\ j\neq s}} |a_{sj}| \frac{|x_j|}{|x_s|} \\ &\le \sum_{\substack{1\le j\le r\\ j\neq s}} |a_{sj}| = -\sum_{\substack{1\le j\le r\\ j\neq s}} a_{sj}. \end{aligned}$$

よって

$$\sum_{j=1}^{r} a_{sj} \le 0$$

となる．これは (9) に矛盾する． □

3 離散的部分群

m を正の整数とする．

$\mathbb{R}^m$ の部分集合 S が離散的であるとは, 任意の正の実数 C に対して

$$\#\left\{ (x_1, x_2, \ldots, x_n) \in S \;\middle|\; \max_{1\le j\le m} |x_j| \le C \right\} < \infty$$

が成り立つときにいう．明らかに, S が離散的であるとき, S の任意の部分集合もまた離散的である．特に, S が離散的であるとき, S の有界部分集合は有限集合である．

命題 3.1. $\mathbb{R}$ の任意の離散的部分群 Γ は, ある $\gamma \in \Gamma$ によって

$$\Gamma = \mathbb{Z}\gamma$$

と書ける．

証明. $\Gamma = \{0\}$ のとき, $\gamma = 0$ とすればよい．

$\Gamma \neq \{0\}$ と仮定すると, ある $\gamma_1 \in \Gamma$ が存在して $|\gamma_1| > 0$ である．$C = |\gamma_1|$ とおくと, Γ が離散的であることから, $|x| \le C$ であるような $x \in \Gamma$ は有限個しかない．よって, $0 < |x| \le C$ を満たす $x \in \Gamma$ の中で最小のものが存在する．それを γ とおく．

$\mathbb{Z}\gamma$ が Γ の部分群であることは明らかである．よって, $\Gamma \subseteq \mathbb{Z}\gamma$ を示せば, $\Gamma = \mathbb{Z}\gamma$ がいえて証明が完了する．

任意の $x \in \Gamma$ に対して,

$$q_0 = \max\left\{ q \in \mathbb{Z} \;\middle|\; q > 0,\ |x| \le q|\gamma| \right\}$$

が存在する[4]．そして,

$$0 \le q_0|\gamma| - |x| < |\gamma|$$

が成り立つ[5]．一方,

$$q_0|\gamma| - |x| \in \Gamma$$

[4] アルキメデスの原理と自然数の整列性からこのような q_0 の存在が保証される．

[5] もし $|\gamma| \le q_0|\gamma| - |x|$ なら $|x| \le (q_0 - 1)|\gamma|$ となって q_0 の最小性に反する．

である[6]. よって, γ の最小性から, $q_0|\gamma| - |x| = 0$ でなければならない. ゆえに $|x| \in \mathbb{Z}\gamma$. したがって $x = \pm|x| \in \mathbb{Z}\gamma$ となり, $\Gamma \subseteq \mathbb{Z}\gamma$ がいえる. □

命題 3.2. Γ を $\mathbb{R}^m$ の離散的部分群とし, $\Gamma \neq \{\mathbf{0}\}$ であるとする. このとき, ある $\gamma \in \Gamma$ が存在して

$$\mathbb{R}\gamma \cap \Gamma = \mathbb{Z}\gamma, \quad \gamma \neq \mathbf{0}$$

が成り立つ.

証明. $\mathbf{0}$ でない元 $\gamma_0 \in \Gamma$ を 1 つとり,

$$M = \{u\gamma_0 \in \mathbb{R}^m \mid 0 < u \leq 1\}$$

とおくと, M は有界集合である. Γ は離散的だから,

$$\Gamma \cap M = \{u\gamma_0 \in \Gamma \mid 0 < u \leq 1\}$$

は有限集合である. また, 少なくとも $\gamma_0 \in \Gamma \cap M$ なので, $\Gamma \cap M$ は空でない. よって,

$$\{u \in \mathbb{R} \mid u\gamma_0 \in \Gamma,\, 0 < u \leq 1\}$$

もまた空でな有限集合なので, 最小元をもつ. それを u_0 とおく. また, $\gamma = u_0\gamma_0$ とおく.

$\alpha \in \Gamma \cap \mathbb{R}\gamma$ とすると, $\alpha = u\gamma$, $u \in \mathbb{R}$ と表される. u を超えない最大の整数を l とすれば,

$$\Gamma \ni \alpha - l\gamma = (u - l)\gamma = (u - l)u_0\gamma_0.$$

一方, $0 \leq u - l < 1$ だから,

$$0 \leq (u - l)u_0 < u_0.$$

である. u_0 の最小性から, $u - l = 0$ でなければならない. ゆえに $\alpha = l\gamma \in \mathbb{Z}\gamma$. したがって $\Gamma \cap \mathbb{R}\gamma \subseteq \mathbb{Z}\gamma$. 逆の包含関係は明らか. □

Γ を $\mathbb{R}^m$ の離散的部分群とし, γ を $\mathbf{0}$ でない Γ の元とする. $\boldsymbol{b}_2$, $\boldsymbol{b}_3$, …, $\boldsymbol{b}_m$ を, γ, $\boldsymbol{b}_2$, $\boldsymbol{b}_3$, …, $\boldsymbol{b}_m$ が $\mathbb{R}^m$ の $\mathbb{R}$ 上の基底となっているような $\mathbb{R}^m$ の元とする. このとき, $m \geq 2$ に対して, 写像 $L_\gamma : \mathbb{R}^m \to \mathbb{R}^{m-1}$ を

$$L_\gamma(x_1\gamma + x_2\boldsymbol{b}_2 + \cdots + x_m\boldsymbol{b}_m) = (x_2, x_3, \ldots, x_m)$$

によって定める. L_γ は明らかに $\mathbb{R}$ 上の線型写像である.

命題 3.3. $\mathbf{0}$ でない任意の $\gamma \in \Gamma$ に対して, $\ker L_\gamma = \mathbb{R}\gamma$ が成り立つ.

証明. $\alpha \in \ker L_\gamma$ とし, ある $x_1, x_2, \ldots, x_m \in \mathbb{R}$ によって

$$\alpha = x_1\gamma + x_2\boldsymbol{b}_2 + \cdots + x_m\boldsymbol{b}_m$$

と表したとする. このとき

$$(x_2, \ldots, x_n) = L_\gamma(\alpha) = \mathbf{0}.$$

すなわち,

$$x_2 = \cdots = x_r = 0.$$

ゆえに $\alpha = x_1\gamma \in \mathbb{R}\gamma$. したがって $\ker L_\gamma \subseteq \mathbb{R}\gamma$. 逆の包含関係は明らかである. □

[6] x, $\gamma \in \Gamma$ のとき, $-x$, $-\gamma \in \Gamma$ だから, $|x|$, $|\gamma| \in \Gamma$. また, $q_0|\gamma| = |\gamma| + \cdots + |\gamma|$（$q_0$ 個の和）.

命題 3.4. $\mathbf{0}$ でない任意の $\gamma \in \Gamma$ に対して, $\Gamma' = L_\gamma(\Gamma)$ は $\mathbb{R}^{m-1}$ の離散的部分群である.

証明. L_γ は線型写像なので, 特に $\mathbb{R}^m$ から $\mathbb{R}^{m-1}$ への群の準同型写像である. よって, Γ' は $\mathbb{R}^{m-1}$ の部分群である.

C を正の実数とする. また, $(x_2, x_3, \ldots, x_m) \in \Gamma'$ とし,

$$\max_{2 \le j \le m} |x_j| \le C \tag{10}$$

であるとする. $\Gamma' = L(\Gamma)$ だから, ある $x_1 \in \mathbb{R}$ が存在して

$$x_1\gamma + x_2\boldsymbol{b}_2 + \cdots + x_m\boldsymbol{b}_m \in \Gamma.$$

x_1 を超えない最大の整数を l_1 とすると, $\gamma \in \Gamma$ なので, $l_1\gamma \in \Gamma$. よって

$$\begin{aligned}&(x_1 - l_1)\gamma + x_2\boldsymbol{b}_2 + \cdots + x_m\boldsymbol{b}_m \\ &\quad = (x_1\gamma + x_2\boldsymbol{b}_2 + \cdots + x_m\boldsymbol{b}_m) - l_1\gamma \in \Gamma.\end{aligned}$$

しかも, $0 \le x_1 - l_1 < 1$ であり, $(x_1 - l_1)\gamma + x_2\boldsymbol{b}_2 + \cdots + x_m\boldsymbol{b}_m$ の L_γ による像は $(x_2, \ldots, x_m)$ である.

したがって, (10) を満たす $(x_2, \ldots, x_m) \in \Gamma'$ の個数は,

$$x_1\gamma + x_2\boldsymbol{b}_2 + \cdots + x_m\boldsymbol{b}_m, \quad 0 \le x_1 < 1 \tag{11}$$

なる形の Γ の元の個数以下である.

一方, γ, $\boldsymbol{b}_2$, $\boldsymbol{b}_3$, …, $\boldsymbol{b}_m$ の各成分の絶対値の最大値を C' とすれば, (11) の形の元を $(y_1, y_2, \ldots, y_m)$ で表すとき,

$$\max_{1 \le j \le m} |y_j| \le C' + (m-1)CC'$$

である. 右辺の $C' + (m-1)CC'$ は $(x_2, \ldots, x_m) \in \Gamma'$ には依存しない定数であり, Γ は離散的だから, (11) の形の元は有限個しかない. ゆえに (10) を満たす $(x_2, \ldots, x_m) \in \Gamma'$ の個数は有限である. したがって Γ' は離散的である. □

定理 3.5. $\mathbb{R}^m$ の任意の離散的部分群 Γ に対して, ある γ_1, γ_2, …, $\gamma_r \in \Gamma$ が存在して

$$\Gamma = \mathbb{Z}\gamma_1 \oplus \cdots \oplus \mathbb{Z}\gamma_r, \quad r \le m$$

が成り立つ.

証明. $\Gamma = \{\mathbf{0}\}$ のときは明らかなので, $\Gamma \ne \{\mathbf{0}\}$ であると仮定する.

m に関する数学的帰納法により証明する. $m = 1$ のときは, まさに命題 3.1 である.

$m \ge 2$ とし, $\mathbb{R}^{m-1}$ の任意の離散的部分群に対して定理が成り立つと仮定する. 命題 3.2 より,

$$\mathbb{R}\gamma_1 \cap \Gamma = \mathbb{Z}\gamma_1, \quad \gamma_1 \ne \mathbf{0}$$

を満たす $\gamma_1 \in \Gamma$ が存在する.

$L = L_{\gamma_1}$, $\Gamma' = L(\Gamma)$ とおく. 命題 3.4 より, Γ' は $\mathbb{R}^{m-1}$ の離散的部分群である. よって帰納法の仮定により, ある γ_2', …, $\gamma_r' \in \Gamma'$ が存在して

$$\Gamma' = \mathbb{Z}\gamma_2' \oplus \cdots \oplus \mathbb{Z}\gamma_r', \quad r \le m$$

が成り立つ. また, $\Gamma' = L(\Gamma)$ なので, ある $\gamma_2, \ldots, \gamma_r \in \Gamma$ が存在して

$$L(\gamma_j) = r'_j \quad (j = 2, \ldots, r)$$

となる.

$n_1, n_2, \ldots, n_r \in \mathbb{Z}$ とし, $n_1\gamma_1 + \cdots + n_r\gamma_r = \mathbf{0}$ と仮定する. このとき,

$$n_2\gamma'_2 + \cdots + n_r\gamma'_r = L(n_1\gamma_1 + \cdots + n_r\gamma_r) = \mathbf{0}.$$

$\gamma'_2, \ldots, \gamma'_r$ は Γ' の $\mathbb{Z}$ 上の基底だから, $n_2 = \cdots = n_r = 0$. さらに, $\gamma_1 \neq \mathbf{0}$ だから $n_1 = 0$ でなければならない. したがって $\gamma_1, \gamma_2, \ldots, \gamma_r$ は $\mathbb{Z}$ 上 1 次独立である.

$\alpha \in \Gamma$ とすると, $L(\alpha) \in \Gamma'$ より, ある $n_2, \ldots, n_r \in \mathbb{Z}$ が存在して

$$L(\alpha) = n_2\gamma'_2 + \cdots + n_r\gamma'_r = L(n_2\gamma_2 + \cdots + n_r\gamma_r)$$

となる. よって

$$L\big(\alpha - (n_2\gamma_2 + \cdots + n_r\gamma_r)\big) = \mathbf{0}.$$

ゆえに

$$\alpha - (n_2\gamma_2 + \cdots + n_r\gamma_r) \in \ker L \cap \Gamma.$$

一方, 命題 3.3 より $\ker L = \mathbb{R}\gamma_1$ だから,

$$\ker L \cap \Gamma = \mathbb{R}\gamma_1 \cap \Gamma = \mathbb{Z}\gamma_1.$$

よって, ある $n_1 \in \mathbb{Z}$ が存在して

$$\alpha - (n_2\gamma_2 + \cdots + n_r\gamma_r) = n_1\gamma_1.$$

ゆえに

$$\alpha = n_1\gamma_1 + n_2\gamma_2 + \cdots + n_r\gamma_r.$$

したがって Γ のすべての元は $\gamma_1, \gamma_2, \ldots, \gamma_r$ によって $\mathbb{Z}$ 上生成される.

以上より, $\mathbb{R}^m$ の任意の離散的部分群に対しても定理が成り立つとが示された. □

4 共役 (1)

n を正の整数とする. K を n 次代数体とし, O_K を K の整数環とする.

K から $\mathbb{Q}$ の代数的閉包 $\overline{\mathbb{Q}}$ の中への同型写像のことを K の共役写像という. K の共役写像は n 個ある.

σ を K の共役写像とする. $\sigma(K)$ が $\mathbb{R}$ に含まれるとき, σ は実であるといい, そうでないとき, σ は虚であるという.

K の共役写像 σ に対して,

$$\overline{\sigma} : K \longrightarrow \overline{\mathbb{Q}}, \quad \alpha \longmapsto \overline{\sigma(\alpha)}$$

もまた共役写像である. σ が実のときは $\sigma = \overline{\sigma}$, 虚のときは $\sigma \neq \overline{\sigma}$ である. 実共役写像の個数を r_1, 虚共役写像の個数を $2r_2$ とするとき, $n = r_1 + 2r_2$ が成り立つ.

共役写像に番号をつけて, $\sigma_1, \sigma_2, \ldots, \sigma_{r_1}$ は実共役写像, $\sigma_{r_1+1}, \ldots, \sigma_n$ は虚共役写像であり, $\sigma_{r_1+r_2+i} = \overline{\sigma_{r_1+i}}$ $(i = 1, 2, \ldots, r_2)$ であるとする. σ_1 は K の恒等写像 id_K であるとする.

$\alpha \in K$ に対して $\alpha^{(i)} = \sigma_i(\alpha)$ とおく. $\sigma_1 = \mathrm{id}_K$ としたので, $\alpha^{(1)} = \alpha$ である.

$K/\mathbb{Q}$ のノルムを N で表すことにすると, 任意の $\alpha \in K$ に対して $N(\alpha) = \alpha^{(1)}\alpha^{(2)} \cdots \alpha^{(n)}$ が成り立つ.

命題 4.1. O_K の 0 でない任意の元 α に対して, $N(\alpha)/\alpha \in O_K$.

証明. $N(\alpha) = \alpha^{(1)}\alpha^{(2)}\cdots\alpha^{(n)}$ であり, α の各共役元はすべて代数的整数だから[7],

$$\frac{N(\alpha)}{\alpha} = \alpha^{(2)}\cdots\alpha^{(n)}$$

もまた代数的整数である. さらに, $N(\alpha) \in \mathbb{Z}$ だから, $N(\alpha)/\alpha \in K$ である. O_K は代数的整数の全体 $\overline{\mathbb{Z}}$ と K との共通部分であるから, $N(\alpha)/\alpha \in O_K$. □

定理 4.2. $u \in O_K$ が K の単数であるための必要十分条件は, $|N(u)| = 1$ となることである.

証明. u を K の単数とすれば, ある $v \in O_K$ が存在して $uv = 1$ となる. よって

$$N(u)N(v) = N(uv) = N(1) = 1.$$

$u, v \in O_K$ だから, $N(u), N(v) \in \mathbb{Z}$. したがって $N(u) = \pm 1$.

逆に, $u \in O_K$ かつ $|N(u)| = 1$ ならば, $u \neq 0$ であり[8],

$$u\,\frac{N(u)}{u} = N(u) = \pm 1.$$

u は 0 でない O_K の元なので, 命題 4.1 より, $N(u)/u$ もまた O_K の元である. したがって u は K の単数である. □

命題 4.3. 任意の正の整数 a $(\in \mathbb{Z})$ に対して, $|O_K/aO_K| \leq a^n$.

証明. $\omega_1, \ldots, \omega_n$ を O_K の整数基とする:

$$O_K = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n.$$

また,

$$A = \{r_1\omega_1 + \cdots + r_n\omega_n \mid 0 \leq r_j < a,\ 1 \leq j \leq n\}$$

とおく. このとき, $|A| = a^n$ である.

一方, 任意の $\alpha \in O_K$ に対して, ある $\beta \in A$ が存在して $\alpha \equiv \beta \pmod{a}$ となる. したがって a を法とする同値類は高々 a^n 個である. □

O_K の 2 つの元 α, β が同伴であるとは, ある単数 $\varepsilon \in O_K^\times$ が存在して, $\alpha = \varepsilon\beta$ と書けるときにいう. 同伴であるという関係が O_K における同値関係であることはすぐにわかる.

命題 4.4. O_K の 0 でない 2 つの元 α, β が同伴であるための必要十分条件は, $\alpha\beta^{-1}$ と $\beta\alpha^{-1}$ がともに O_K に属することである.

証明. α, β が同伴ならば, ある単数 $\varepsilon \in O_K^\times$ が存在して, $\alpha = \varepsilon\beta$ と書ける. よって $\alpha\beta^{-1} = \varepsilon \in O_K$, $\beta\alpha^{-1} = \varepsilon^{-1} \in O_K$.

逆に, $\alpha\beta^{-1}$ と $\beta\alpha^{-1}$ がともに O_K に属するとき, ある $\gamma, \delta \in O_K$ が存在して $\alpha\beta^{-1} = \gamma$, $\beta\alpha^{-1} = \delta$ となる. このとき

$$\alpha = \gamma\beta = \gamma\delta\alpha.$$

よって

$$\alpha(1 - \gamma\delta) = 0.$$

$\alpha \neq 0$ だから, $\gamma\delta = 1$. よって γ, δ は K の単数である. したがって α, β は同伴である. □

[7] α は代数的整数だから, ある $\mathbb{Z}$ 係数の単多項式 $f(x)$ の根である: $f(\alpha) = 0$. このとき, 各共役元 $\alpha^{(i)} = \sigma(\alpha)$ に対して $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$ が成り立つ. したがって $\alpha^{(i)}$ もまた代数的整数である.

[8] もし仮に $u = 0$ ならば $N(u) = 0$.

定理 4.5. 任意の正の整数 $a \in \mathbb{Z}$ に対して, $|N(\alpha)| = a$ となるような O_K の元 α は同伴を除いて有限個しかない.

証明. 命題 4.3 より, a を法とする同値類は有限個しかない. したがって, 同じ同値類に属する任意の $\alpha, \beta \in O_K$ に対して, $N(\alpha) = N(\beta) = a$ ならば α と β が同伴であることを示せば十分である.

$a > 0$ なので, α, β はともに 0 ではない. また, ある $\gamma \in O_K$ が存在して

$$\alpha - \beta = a\gamma$$

が成り立つ. 命題 4.1 より,

$$\alpha\beta^{-1} = 1 \pm \frac{N(\beta)}{\beta}\,\gamma \in O_K,$$
$$\beta\alpha^{-1} = 1 \pm \frac{N(\alpha)}{\alpha}\,\gamma \in O_K.$$

命題 4.4 より α と β とは同伴である. □

定理 4.6. 任意の実数 $c > 0$ に対して, $\alpha \in O_K$ で

$$|\alpha^{(i)}| \le c, \quad i = 1, 2, \ldots, n$$

を満たすものは有限個しかない.

証明. $\omega_1, \ldots, \omega_n$ を O_K の整数基とする:

$$O_K = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n.$$

O_K の任意の元 α は, ある $x_1, \ldots, x_n \in \mathbb{Z}$ によって

$$\alpha = x_1\omega_1 + \cdots + x_n\omega_n$$

と表される. このとき, 共役写像の準同型性によって,

$$\begin{aligned}
\alpha^{(1)} &= x_1\omega_1^{(1)} + \cdots + x_n\omega_n^{(1)} \\
\alpha^{(2)} &= x_1\omega_1^{(2)} + \cdots + x_n\omega_n^{(2)} \\
&\cdots\cdots \\
\alpha^{(n)} &= x_1\omega_1^{(n)} + \cdots + x_n\omega_n^{(n)}
\end{aligned}$$

となる.

$$P = \begin{pmatrix} \omega_1^{(1)} & \omega_2^{(1)} & \cdots & \omega_n^{(1)} \\ \omega_1^{(2)} & \omega_2^{(2)} & \cdots & \omega_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1^{(n)} & \omega_2^{(n)} & \cdots & \omega_n^{(n)} \end{pmatrix}, \quad \boldsymbol{\alpha} = \begin{pmatrix} \alpha^{(1)} \\ \alpha^{(2)} \\ \vdots \\ \alpha^{(n)} \end{pmatrix}, \quad \boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

とおくと,

$$\boldsymbol{\alpha} = P\boldsymbol{x}$$

となる. P は正則行列なので, 逆行列 P^{-1} が存在して,

$$\boldsymbol{x} = P^{-1}\boldsymbol{\alpha}$$

となる. $P^{-1}=(p_{ij})$ とおき,

$$c_1=\max_{\substack{1\le i\le n\\ 1\le j\le n}}|p_{ij}|$$

とおく. このとき, $i=1,2,\dots,n$ に対して

$$\begin{aligned}|x_i|&=|p_{i1}\alpha^{(1)}+\cdots+p_{in}\alpha^{(n)}|\\&=|p_{i1}||\alpha^{(1)}|+\cdots+|p_{in}||\alpha^{(n)}|\\&\le nc_1c\end{aligned}$$

となる. nc_1c は K にのみ依存する定数である. よって α は有限個しかない. □

5 共役 (2)

n を正の整数, K を n 次代数体, r_1 を K の実共役写像の個数, $2r_2$ を虚共役写像の個数とする. $r_1\ge 0$, $r_2\ge 0$, $r_1+2r_2=n>0$ なので, $r_1\ge 1$ または $r_2\ge 1$ である. よって $r_1+r_2\ge 1$ である.

$E=\{1,2,\dots,r_1+r_2\}$ とし, $k\in E$ に対して $\widetilde{k}$ を次のように定義する :

$$\widetilde{k}=\begin{cases}k, & 1\le k\le r_1 \text{ のとき},\\ k+r_2, & r_1<k\le r_1+r_2 \text{ のとき}.\end{cases}$$

E の部分集合 S に対して,

$$\widetilde{S}=\{\widetilde{k}\mid k\in S\}$$

とおく.

以下, この節では $r_1+r_2\ge 2$ と仮定する. つまり, E は 2 つ以上の元をもつとする. X, Y を E の部分集合とし,

$$E=X\cup Y,\quad X\cap Y=\emptyset,\quad X\ne\emptyset,\quad Y\ne\emptyset$$

であるとする. このとき,

$$\{1,2,\dots,n\}=(X\cup\widetilde{X})\cup(Y\cup\widetilde{Y}),\quad (X\cup\widetilde{X})\cap(Y\cup\widetilde{Y})=\emptyset \tag{12}$$

が成り立つ.

$X\cup\widetilde{X}$ の元の個数を m とする. $X\ne\emptyset$ なので, $m\ge 1$ である. $n=r_1+2r_2$ より,

$$X\cup\widetilde{X}\subseteq\{1,2,\dots,n\}.$$

また, $Y\ne\emptyset$ より,

$$X\cup\widetilde{X}\ne\{1,2,\dots,n\}.$$

したがって $m<n$ である.

定理 5.1. *K のみに依存する正の実数 c が存在して, 任意の整数 $t>1$ に対して, O_K の 0 でない元 α が存在して,*

$$\begin{aligned}&c^{1-n}t^{1-n/m}\le|\alpha^{(k)}|\le c\,t^{1-n/m}\quad(k\in X),\\&c^{1-n}t\le|\alpha^{(l)}|\le ct\quad(l\in Y),\end{aligned}$$

が成り立つ.

証明. $k_1, \ldots, k_u$ を X の元で $\widetilde{k_i} = k_i$ となるもの, $l_1, \ldots, l_v$ を X の元で $\widetilde{l_i} = l_i$ となるものとする. このとき, $m = u + 2v$ である.

$\omega_1, \omega_2, \ldots, \omega_n$ を O_K の整数基とする. $m \times n$ 型の行列 $A = (a_{ij})$ を, $j = 1, 2, \ldots, n$ に対して

$$\begin{aligned} a_{ij} &= \omega_j^{(k_i)} \quad (i = 1, 2, \ldots, u), \\ a_{u+i,j} &= \operatorname{Re} \omega_j^{(l_i)} \quad (i = 1, 2, \ldots, v), \\ a_{u+v+i,j} &= \operatorname{Im} \omega_j^{(l_i)} \quad (i = 1, 2, \ldots, v) \end{aligned}$$

で定義する. $m < n$ なので, 定理 2.2 より,

$$\begin{aligned} \boldsymbol{x} &= (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n, \\ \boldsymbol{y} &= (y_1, y_2, \ldots, y_m) \in \mathbb{R}^m \end{aligned}$$

が存在して, $\boldsymbol{x} \neq \boldsymbol{0}$ であり,

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix} = A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

および

$$\begin{aligned} \max_{1 \leq j \leq n} |x_j| &\leq t, \\ \max_{1 \leq i \leq m} |y_i| &\leq 2at^{1-n/m} \end{aligned}$$

が成り立つ.

$$\alpha = \sum_{j=1}^{n} x_j \omega_j$$

とおくと, α は 0 でない O_K の元である. このとき, $i = 1, 2, \ldots, u$ に対して

$$|\alpha^{(k_i)}| = \left| \sum_{j=1}^{n} x_j \omega_j^{(k_i)} \right| = \left| \sum_{j=1}^{n} a_{ij} x_j \right| = |y_i| \leq 2at^{1-n/m}$$

および, $i = 1, 2, \ldots, v$ に対して

$$\begin{aligned} |\alpha^{(l_i)}| &\leq \left| \sum_{j=1}^{n} x_j \operatorname{Re} \omega_j^{(l_i)} \right| + \left| \sum_{j=1}^{n} x_j \operatorname{Im} \omega_j^{(l_i)} \right| \\ &= \left| \sum_{j=1}^{n} a_{u+i,j} x_j \right| + \left| \sum_{j=1}^{n} a_{u+v+i,j} x_j \right| \\ &= |y_{u+i}| + |y_{u+v+i}| \\ &\leq 4at^{1-n/m} \end{aligned}$$

が成り立つ. さらに, $\alpha^{(\widetilde{l_i})}$ は $\alpha^{(l_i)}$ の複素共役なので, $|\alpha^{(l_i)}| = |\alpha^{(\widetilde{l_i})}|$ である. ゆえに, 任意の $k \in X \cup \widetilde{X}$ に対して

$$|\alpha^{(k)}| \leq 4at^{1-n/m}$$

が成り立つ.

次に,

$$c_1 = \max_{1\le i\le n} \sum_{j=1}^{n} |\omega_j^{(i)}|$$

とおくと, $j = 1, 2, \ldots, n$ に対して $|x_j| \le t$ だから, 任意の $l \in Y \cup \widetilde{Y}$ に対して,

$$|\alpha^{(l)}| = \left| \sum_{j=1}^{n} x_j \omega_j^{(l)} \right| \le c_1 t$$

となる.

$$c = \max\{4a, c_1\}$$

とおくと,

$$|\alpha^{(k)}| \le c\, t^{1-n/m} \quad (k \in X \cup \widetilde{X}), \tag{13}$$

$$|\alpha^{(l)}| \le c\, t \quad (l \in Y \cup \widetilde{Y}) \tag{14}$$

が得られる.

α は 0 でない代数的整数なので, $|N(\alpha)| \ge 1$ である[9].

任意の $k \in X$ に対して, (12), (13), (14) より

$$\begin{aligned} 1 \le |N(\alpha)| &= \prod_{i\in X\cup\widetilde{X}} |\alpha^{(i)}| \prod_{j\in Y\cup\widetilde{Y}} |\alpha^{(j)}| \\ &\le |\alpha^{(k)}| \left(c^{1-n/m}\right)^{m-1} (ct)^{n-m} \\ &= |\alpha^{(k)}| c^{n-1} t^{n/m-1} \end{aligned}$$

が成り立つ. よって

$$c^{1-n} t^{1-n/m} \le |\alpha^{(k)}|$$

が得られる.

また, 任意の $l \in Y$ に対して, (12), (13), (14) より

$$\begin{aligned} 1 \le |N(\alpha)| &= \prod_{i\in X\cup\widetilde{X}} |\alpha^{(i)}| \prod_{j\in Y\cup\widetilde{Y}} |\alpha^{(j)}| \\ &\le \left(ct^{1-n/m}\right)^{m} |\alpha^{(l)}| (ct)^{n-m-1} \\ &= |\alpha^{(l)}| c^{n-1} t^{-1} \end{aligned}$$

が成り立つ. よって

$$c^{1-n} t \le |\alpha^{(l)}|$$

が得られる. □

定理 5.2. *K のみに依存する正の実数 c が存在して, 次が成り立つような 0 でない O_K の元の列 (α_ν) が存在する :*

$$|\alpha_\nu^{(k)}| > |\alpha_{\nu+1}^{(k)}| \quad (k \in X),$$
$$|\alpha_\nu^{(l)}| < |\alpha_{\nu+1}^{(l)}| \quad (l \in Y)$$

かつ

$$|N(\alpha_\nu)| \le c^n.$$

[9] α が 0 でなければ $N(\alpha) \ne 0$ である. また, α が代数的整数ならば $N(\alpha) \in \mathbb{Z}$ である. ゆえに $|N(\alpha)| \ge 1$ である.

証明. c を定理 5.1 における, K のみに依存する正の実数とする.

$M > c^n$ かつ $M^{n/m-1} > c^n$ を満たす正の整数 M をとる[10]. $t_1 > 1$ なる整数 t_1 を任意に 1 つとる. また, 帰納的に $t_{\nu+1} = Mt_\nu$ と定義する.

$M \geq 1$ より各 ν について $t_\nu > 1$ である. よって, 各 ν に対して, O_K の 0 でない元 α_ν が存在して,

$$\begin{aligned} &c^{1-n}t_\nu^{1-n/m} \leq |\alpha_\nu^{(k)}| \leq c\,t_\nu^{1-n/m} \quad (k \in X), \\ &c^{1-n}t_\nu \leq |\alpha_\nu^{(l)}| \leq c\,t_\nu \quad (l \in Y), \end{aligned}$$

が成り立つ. このとき,

$$\begin{aligned} |\alpha_{\nu+1}^{(k)}| &\leq c\,t_{\nu+1}^{1-n/m} = c\,(Mt_\nu)^{1-n/m} \\ &< c^{1-n}t_\nu^{1-n/m} \leq |\alpha_\nu^{(k)}| \end{aligned}$$

かつ

$$\begin{aligned} |\alpha_{\nu+1}^{(l)}| &\geq c\,t_{\nu+1} = c^{1-n}Mt_\nu \\ &> ct_\nu \geq |\alpha_\nu^{(l)}|. \end{aligned}$$

最後に,

$$\begin{aligned} |N(\alpha_\nu)| &= \prod_{i \in X \cup \widetilde{X}} |\alpha^{(i)}| \prod_{j \in Y \cup \widetilde{Y}} |\alpha^{(j)}| \\ &\leq \left(c\,t_\nu^{1-n/m}\right)^m (c\,t_\nu)^{n-m} = c^n. \end{aligned}$$

□

定理 5.3. *K の単数 ε が存在して,*

$$\begin{aligned} &|\varepsilon^{(k)}| < 1 \quad (k \in X), \\ &|\varepsilon^{(l)}| > 1 \quad (l \in Y) \end{aligned}$$

が成り立つ.

証明. 定理 5.2 より, 0 でない O_K の元の列 (α_ν) が存在して

$$\begin{aligned} &|\alpha_\nu^{(k)}| > |\alpha_{\nu+1}^{(k)}| \quad (k \in X), \\ &|\alpha_\nu^{(l)}| < |\alpha_{\nu+1}^{(l)}| \quad (l \in Y) \end{aligned}$$

かつ

$$|N(\alpha_\nu)| \leq c^n.$$

一方, 定理 4.5 より, $|N(\alpha)| \leq c^n$ であるような $\alpha \in O_K$ は同伴を除いて有限個しかない. したがって, K の単数 ε と番号 μ, ν が存在して $\alpha_\mu = \varepsilon\alpha_\nu$, $\mu > \nu$ となる. よって, $j \in X$ のとき

$$|\varepsilon^{(j)}| = \frac{|\alpha_\mu^{(j)}|}{|\alpha_\nu^{(j)}|} < 1$$

であり, $j \in Y$ のとき

$$|\varepsilon^{(j)}| = \frac{|\alpha_\mu^{(j)}|}{|\alpha_\nu^{(j)}|} > 1$$

である. □

[10] 言い換えれば, M として, c^n, $c^{mn/(n-m)}$ のどちらよりも大きな整数をとる.

6　単数定理の証明 (1)

n を正の整数, K を n 次代数体, r_1 を K の実共役写像の個数, $2r_2$ を K の虚共役写像の個数とする. このとき $n = r_1 + 2r_2$ が成り立つ.

$r = r_1 + r_2 - 1$ とおく. $r \geq 0$ である[11]. $r \geq 1$ のとき, 写像 $\lambda : O_K^\times \to \mathbb{R}^r$ を

$$\lambda(\varepsilon) = (\log|\varepsilon^{(1)}|, \ldots, \log|\varepsilon^{(r)}|)$$

によって定義する. log の性質から, λ が群の準同型写像であることは明らかである.

K に属する 1 の根の全体を W_K とおく. W_K は乗法に関して群をなす.

$$\begin{aligned}\zeta \in W_K &\iff \zeta \in K \text{ かつ, ある正の整数 } t \text{ が存在して } \zeta^t = 1\\ &\iff \zeta \in O_K^\times \text{ かつ, ある正の整数 } t \text{ が存在して } \zeta^t = 1\\ &\iff \zeta \text{ は } O_K^\times \text{ の有限位数の元}\end{aligned}$$

であるから, W_K は $O_K^\times$ の有限位数の元の全体と一致する.

定理 6.1. *W_K は有限巡回群である.*

証明. $\zeta \in W_K$ とすると, ある正の整数 t が存在して $\zeta^t = 1$ が成り立つ. よって,

$$|\zeta^{(i)}|^t = 1 \quad (i = 1, 2, \ldots, n).$$

$|\zeta^{(i)}|$ は正の実数だから,

$$|\zeta^{(i)}| = 1 \quad (i = 1, 2, \ldots, n)$$

でなければならない. 定理 4.6 より, $|\alpha^{(i)}| \leq 1$ を満たす $\alpha \in O_K$ は有限個しかない. ゆえに, W_K は有限群である. 一般に, 体 F の乗法群 $F^\times$ の有限部分群は巡回群である. W_K は $K^\times$ の有限部分群なので, 巡回群である. □

定理 6.2. *$r \geq 1$ のとき, $\ker\lambda = W_K$.*

証明. $r \geq 1$ のとき, $r_1 \geq 1$ または $r_2 \geq 1$ である.

$\varepsilon \in \ker\lambda$ とする. $i = 1, 2, \ldots, r$ に対して,

$$\log|\varepsilon^{(i)}| = 0,$$

すなわち

$$|\varepsilon^{(i)}| = 1$$

が成り立つ.

$r_2 > 0$ のとき, $j = 1, 2, \ldots, r_2$ に対して

$$|\varepsilon^{(r_1+r_2+j)}| = |\varepsilon^{(r_1+j)}|$$

である[12]. よって, $i = r_1 + r_2$, n を除いて[13]は $|\varepsilon^{(i)}| = 1$ であることがいえる. ところが, このことと定理 4.2 より

$$1 = |N(\varepsilon)| = \prod_{i=1}^{n} |\varepsilon^{(i)}| = |\varepsilon^{(r_1+r_2)}||\varepsilon^{(n)}| = |\varepsilon^{(r_1+r_2)}|^2 = |\varepsilon^{(n)}|^2$$

[11] もし仮に $r < 0$ ならば, $r_1 \geq 0$, $r_2 \geq 0$ より $r_1 = r_2 = 0$ でなければならない. ところが, これは $r_1 + 2r_2 = n > 0$ に反する.

[12] $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$ となるように, あらかじめ K の共役写像に番号づけをしたのであった. ここで, $\overline{\sigma}$ は σ の像の複素共役によって定まる写像を表している.

[13] $n = r_1 + 2r_2$ であることに注意せよ.

であるから, $|\varepsilon^{(r_1+r_2)}| = |\varepsilon^{(n)}| = 1$ が成り立つ. したがって, すべての $i = 1, 2, \ldots, n$ に対して $|\varepsilon^{(i)}| = 1$ が成り立つ.

$r_2 = 0$ のとき, $r = r_1 - 1 = n - 1$ であるから, $i = 1, 2, \ldots, n-1$ に対して $|\varepsilon^{(i)}| = 1$ が成り立つ. ところが, このことと定理 4.2 より

$$1 = |N(\varepsilon)| = \prod_{i=1}^{n} |\varepsilon^{(i)}| = |\varepsilon^{(n)}|.$$

したがって, すべての $i = 1, 2, \ldots, n$ に対して $|\varepsilon^{(i)}| = 1$ が成り立つ.

定理 4.6 より, $|\alpha^{(i)}| \leq 1$ を満たす $\alpha \in O_K$ は有限個しかない. ゆえに, $\ker\lambda$ は有限群である. したがって, $\ker\lambda$ の元はすべて有限位数である. W_K は $O_K^\times$ の有限位数の元の全体であるから, $\ker\lambda \subseteq W_K$.

逆に, $u \in W_K$ とすると, ある正の整数 t が存在して $u^t = 1$ が成り立つ. よって, すべての $i = 1, 2, \ldots, n$ に対して

$$|u^{(i)}|^t = 1.$$

$|u^{(i)}|$ は正の実数だから,

$$|u^{(i)}| = 1$$

でなければならない. よって, $i = 1, 2, \ldots, r$ に対して

$$\log|u^{(i)}| = 0.$$

ゆえに $u \in \ker\lambda$ となる. したがって $W_K \subseteq \ker\lambda$. □

定理 6.3. *$r \geq 1$ のとき, $\lambda(O_K^\times)$ は $\mathbb{R}^r$ の離散的部分群である.*

証明. $r \geq 1$ のとき, $r_1 \geq 1$ または $r_2 \geq 1$ である.

$\lambda(O_K^\times)$ が $\mathbb{R}^r$ の加法群としての部分群であることは明らかなので, 離散的であることを示す.

正の実数 c が与えられたとする. $\varepsilon \in O_K^\times$ を,

$$\max_{1\leq j\leq r} \left|\log|\varepsilon^{(j)}|\right| \leq c$$

を満たすものとする. この条件は, $i = 1, 2, \ldots, r$ に対して

$$\left|\log|\varepsilon^{(i)}|\right| \leq c$$

すなわち

$$e^{-c} \leq |\varepsilon^{(i)}| \leq e^c$$

が成り立つことと同値である.

$r_2 > 0$ のとき, $j = 1, 2, \ldots, r_2$ に対して

$$|\varepsilon^{(r_1+r_2+j)}| = |\varepsilon^{(r_1+j)}|$$

なので, $i \neq r_1 + r_2, n$ なるすべての i に対して

$$e^{-c} \leq |\varepsilon^{(i)}| \leq e^c.$$

一方, 定理 4.2 より

$$1 = |N(\varepsilon)| = \prod_{i=1}^{n} |\varepsilon^{(i)}|$$

だから,

$$|\varepsilon^{(r_1+r_2)}||\varepsilon^{(n)}| = \prod_{\substack{1\le i\le n\\ i\neq r_1+r_2,n}} |\varepsilon^{(i)}|^{-1} < e^{(n-2)c}.$$

また, $|\varepsilon^{(r_1+r_2)}| = |\varepsilon^{(n)}|$ だから,

$$|\varepsilon^{(r_1+r_2)}|^2 = |\varepsilon^{(n)}|^2 < e^{(n-2)c}.$$

ゆえに

$$|\varepsilon^{(r_1+r_2)}| = |\varepsilon^{(n)}| < e^{(n-2)c/2}.$$

したがって, $r_2 > 0$ のとき, すべての $i = 1, 2, \ldots, n$ に対して $|\varepsilon^{(i)}| < e^c$ が成り立つ.

$r_2 = 0$ のとき, $r = r_1 - 1 = n - 1$ であるから, $i = 1, 2, \ldots, n-1$ に対して

$$e^{-c} \le |\varepsilon^{(i)}| \le e^c.$$

が成り立つ. 一方, 定理 4.2 より

$$1 = |N(\varepsilon)| = \prod_{i=1}^{n} |\varepsilon^{(i)}|$$

だから,

$$|\varepsilon^{(n)}| = \prod_{i=1}^{n-1} |\varepsilon^{(i)}|^{-1} < e^{(n-1)c}.$$

したがって, $r_2 = 0$ のとき, すべての $i = 1, 2, \ldots, n$ に対して $|\varepsilon^{(i)}| < e^c$ が成り立つ.

定理 4.6 より, すべての $i = 1, 2, \ldots, n$ に対して $|\alpha^{(i)}| < e^c$ を満たす O_K の元 α は有限個しかない. ゆえに $\lambda(O_K^\times)$ は離散的である. □

7 単数定理の証明 (2)

K の 0 でない元 α に対して,

$$l^{(i)}(\alpha) = \begin{cases} \log|\alpha^{(i)}|, & 1 \le i \le r_1 \text{ のとき,} \\ 2\log|\alpha^{(i)}|, & r_1 < i \le r_2 \text{ のとき} \end{cases}$$

とおく.

命題 7.1. 任意の $\varepsilon \in O_K^\times$ に対して

$$\sum_{i=1}^{r_1+r_2} l^{(i)}(\varepsilon) = 0$$

が成り立つ.

証明. $\alpha \in O_K$ とすると,

$$\log|N(\alpha)| = \log\prod_{i=1}^{n}|\alpha^{(i)}| = \sum_{i=1}^{n}\log|\alpha^{(i)}|.$$

一方, $j = 1, \ldots, r_2$ に対して

$$|\alpha^{(r_1+r_2+j)}| = |\alpha^{(r_1+j)}|$$

であるから,

$$\sum_{i=1}^{n} \log |\alpha^{(i)}| = \sum_{i=1}^{n} l^{(i)}(\alpha).$$

ゆえに

$$\log |N(\alpha)| = \sum_{i=1}^{n} l^{(i)}(\alpha).$$

特に, 任意の $\varepsilon \in O_K$ に対して, 定理 4.2 より $|N(\varepsilon)| = 1$ なので,

$$\sum_{i=1}^{r_1+r_2} l^{(i)}(\varepsilon) = \log |N(\varepsilon)| = 0$$

である. □

命題 7.2. $r = r_1 + r_2 - 1$ とする. $r \geq 1$ のとき, ある $\varepsilon_1, \ldots, \varepsilon_r \in O_K^\times$ が存在して, $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_r)$ は $\mathbb{R}^r$ の中で $\mathbb{R}$ 上 1 次独立である.

証明. $E = \{1, 2, \ldots, r_1 + r_2\}$ とする. 各 $i = 1, 2, \ldots, r_1 + r_2$ に対して, $Y = \{i\}$, $X = E \setminus Y$ とおく. 明らかに $E = X \cup Y$, $X \cap Y = \emptyset$, $Y \neq \emptyset$ である. $r \geq 1$ すなわち $r_1 + r_2 \geq 2$ なので, E は 2 つ以上の元をもつ. よって $X \neq \emptyset$ である. 定理 5.3 より, ある $\varepsilon_i \in O_K^\times$ が存在して,

$$|\varepsilon_i^{(i)}| > 1, \tag{15}$$

$$|\varepsilon_i^{(j)}| < 1 \quad (j \neq i) \tag{16}$$

が成り立つ.

$A = (a_{ij}) = (l^{(j)}(\varepsilon_i) \mid 1 \leq i \leq r, 1 \leq j \leq r)$ とおく. (15) より $a_{ii} > 0$ であり, (16) より $a_{ij} < 0$ $(i \neq j)$ である. さらに, 命題 7.1 と (16) より, $i = 1, 2, \ldots, r$ に対して

$$\sum_{i=1}^{r} a_{ij} = \sum_{j=1}^{r} l^{(j)}(\varepsilon_i) = -l^{(r_1+r_2)}(\varepsilon_i) > 0$$

が成り立つ. ゆえに定理 2.3 より, $\det A \neq 0$ である.

一方,

$$\det \begin{pmatrix} \lambda(\varepsilon_1) \\ \lambda(\varepsilon_2) \\ \vdots \\ \lambda(\varepsilon_r) \end{pmatrix} = \det(\log |\varepsilon_i^{(j)}|) = \begin{cases} 2^{-(r_2-1)} \det A & r_2 \geq 1 \text{ のとき}, \\ \det A & r_2 = 0 \text{ のとき} \end{cases}$$

が成り立つことはすぐにわかる. よって, $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_r)$ は $\mathbb{R}^r$ の中で $\mathbb{R}$ 上 1 次独立である. □

定理 7.3. $r = r_1 + r_2 - 1$ とする. $r \geq 1$ のとき,

$$\lambda(O_K^\times) = \mathbb{Z}^r$$

が成り立つ.

証明. 定理 6.3 より, $\lambda(O_K^\times)$ は $\mathbb{R}^r$ の離散的部分群である. 定理 3.5 より,

$$\lambda(O_K^\times) = \mathbb{Z}^s, \quad s \leq r$$

が成り立つ. 一方, 命題 7.2 より, $\lambda(O_K^\times)$ は r 個の $\mathbb{R}$ 上 1 次独立な元をもつ. $\mathbb{Z} \subseteq \mathbb{R}$ なので, それら r 個の元は $\mathbb{Z}$ 上 1 次独立である. ゆえに $s = r$ でなければならない. □

8　単数定理の証明 (3)

命題 8.1. 虚 2 次体の単数は, 次の通りである:

(i) $\mathbb{Q}(\sqrt{-1})$ の単数は ± 1, $\pm\sqrt{-1}$ のみである.

(ii) $\mathbb{Q}(\sqrt{-3})$ の単数は ± 1, $\pm(1-\sqrt{-3})/2$, $\pm(1+\sqrt{-3})/2$ のみである.

(iii) それ以外の虚 2 次体の単数は ± 1 のみである.

証明. 一般に, 虚 2 次体は, ある square-free な正の整数 d によって $\mathbb{Q}(\sqrt{-d})$ と表される.

ε を $\mathbb{Q}(\sqrt{-d})$ の単数とするとき, $\varepsilon = a + b\sqrt{-d}$ なる $a, b \in \mathbb{Q}$ が存在する. このとき,

$$N(\varepsilon) = (a + b\sqrt{-d})(a - b\sqrt{-d}) = a^2 + b^2 d > 0$$

が成り立つ. 一方, 定理 4.2 より $|N(\varepsilon)| = 1$ である. したがって $N(\varepsilon) = 1$ である.

$b = 0$ のとき,

$$1 = N(\varepsilon) = a^2 = \varepsilon^2$$

だから, $\varepsilon = \pm 1$ である.

$b \neq 0$ のとき, ε は

$$X^2 + tX + 1, \quad t \in \mathbb{Z}$$

なる形の多項式の根である. $\varepsilon \notin \mathbb{R}$ だから, 上の多項式の判別式を考えると

$$(t-2)(t+2) = t^2 - 4 < 0.$$

よって

$$-2 < t < 2.$$

t は整数だから, $t = 0, \pm 1$ である.

ゆえに, 虚 2 次体の単数となりうる $\mathbb{C}$ の元は

$$\pm 1, \quad \pm\sqrt{-1}, \quad \pm(1-\sqrt{-3})/2, \quad \pm(1+\sqrt{-3})/2$$

のみである. そのうち, $\mathbb{Q}(\sqrt{-1})$ は ± 1, $\pm\sqrt{-1}$ のみを含む. $\mathbb{Q}(\sqrt{-3})$ は ± 1, $\pm(1-\sqrt{-3})/2$, $\pm(1+\sqrt{-3})/2$ のみを含む. それ以外の虚 2 次体は ± 1 のみを含む. □

定理 8.2 (Dirichlet の単数定理)**.** W_K は有限巡回群である. $r = r_1 + r_2 - 1$ とおくと,

$$O_K^\times = W_K \times \mathbb{Z}^r$$

が成り立つ.

証明. W_K が有限巡回群であることは定理 6.1 で示した.

$r \geq 1$ のとき, 定理 6.2, 定理 7.3 より,

$$\ker \lambda = W_K, \quad \lambda(O_K^\times) = \mathbb{Z}^r.$$

$\lambda(O_K^\times) = \mathbb{Z}^r$ より, ある $\varepsilon_1, \ldots, \varepsilon_r \in O_K^\times$ が存在して, $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_r)$ は $\lambda(O_K^\times)$ の $\mathbb{Z}$ 上の基底である.

$\varepsilon \in O_K^\times$ を任意にとると, ある n_1, …, $n_r \in \mathbb{Z}$ が存在して

$$\lambda(\varepsilon) = n_1\lambda(\varepsilon_1) + \cdots + n_r\lambda(\varepsilon_r)$$

と表される. よって

$$\lambda\left(\frac{\varepsilon}{\varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r}}\right) = \mathbf{0}.$$

$\ker\lambda = W_K$ なので,

$$\frac{\varepsilon}{\varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r}} \in W_K.$$

したがって, ある $\zeta \in W_K$ が存在して

$$\varepsilon = \zeta\varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r} \tag{17}$$

と表される. さらに, もし

$$\varepsilon = \zeta\varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r} = \zeta'\varepsilon_1^{n_1'}\cdots\varepsilon_r^{n_r'}, \quad \zeta,\zeta' \in W_K, \quad n_1,\ldots,n_r,n_1',\ldots,n_r' \in \mathbb{Z}$$

ならば,

$$\lambda(\zeta\varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r}) = \lambda(\zeta'\varepsilon_1^{n_1'}\cdots\varepsilon_r^{n_r'}).$$

$\lambda(\zeta) = \lambda(\zeta') = \mathbf{0}$ なので,

$$(n_1 - n_1')\lambda(\varepsilon_1) + \cdots + (n_r - n_r')\lambda(\varepsilon_r) = \mathbf{0}.$$

$\lambda(\varepsilon_1)$, …, $\lambda(\varepsilon_r)$ は $\mathbb{Z}$ 上 1 次独立だから,

$$n_1 = n_1', \quad \ldots, \quad n_r = n_r'$$

となる. よって $\zeta = \zeta'$ もいえる. これより ε は (17) の形に一意的に表される. したがって

$$O_K^\times = W_K \times \mathbb{Z}^r$$

が得られる.

$r = 0$ のとき, $O_K^\times = W_K$ がいえれば証明は完了する. $r = 0$ であるのは, $r_1 = 1$ かつ $r_2 = 0$ のときか, または $r_1 = 0$ かつ $r_2 = 1$ のときである. 前者は $K = \mathbb{Q}$ のときであり, 後者は K が虚 2 次体のときである.

$K = \mathbb{Q}$ のとき, $O_K = \mathbb{Z}$ だから $O_K^\times = \{\pm 1\}$ である.

K が虚 2 次体の場合, 命題 8.1 より, 次のことがわかる:

(i) $K = \mathbb{Q}(\sqrt{-1})$ のとき $O_K^\times$ は $\sqrt{-1}$ によって生成される.

(ii) $K = \mathbb{Q}(\sqrt{-3})$ のとき $O_K^\times$ は 1 の原始 6 乗根 $(1 + \sqrt{-3})/2$ によって生成される.

(iii) それ以外の虚 2 次体のときは $O_K^\times = \{\pm 1\}$ である.

$K = \mathbb{Q}$ の場合や K が虚 2 次体の場合には, $O_K^\times$ の有限位数の元の全体と $O_K^\times$ 自身とが一致する. 一方, W_K は $O_K^\times$ の有限位数の元の全体と一致する. ゆえに, $O_K^\times = W_K$ がいえる. したがって, $r = 0$ のときも定理は正しい. □

参考文献

[1] J. S. Chahal（著）, 織田進（訳）, 数論入門講義, 共立出版, 2002.

[2] 藤崎源二郎, 代数的整数論入門（上）, 裳華房, 1975.