

3, 4, 5 次体に於る類数の可除性の問題

東大 理学部 市村 文男

類数の可除性の問題とは、何らかの付帯条件を満たす代数体のなかで、類数が与えられた数で割れるものをたく士ん(無限個)構成しようという問題である。既に次の場合でこの問題はとがれている。

- (i) 虚二次体 (Nagel [2], 黒田 [1], 山本 [6])
- (ii) 実二次体 (山本 [6])
- (iii) 3次ガロア体 (内田 [4])

筆者は、山本 [6], 内田 [4] で用いられた方法を応用して次の事実を証明した。

定理 1 (1) 判別式負の 3 次体のなかで類数が与えられた奇数 (resp. 2) で割れるものが無数に存在する。

定理 2 (2) 判別式正の 3 次非ガロア体のなかで類数が与えられた奇数 (resp. 2) で割れるものが無数に存在する。

定理 3 次の条件を満たす 4 次体が無数に存在する。

- ① \mathbb{Q} 上の Galois closure の Galois 群は 4 次対称群に同型。
(従って、特に、2 次体を含まない。)
- ② 実素点は 2 つ、虚素点は 1 つ。
- ③ 類数は与えられた素数で割れる。

定理 4 次の条件を満たす 5 次体が無数に存在する。

- ① \mathbb{Q} 上の Galois closure の Galois 群は 5 次対称群に同型。
- ② 実素点は 3 つ、虚素点は 1 つ。
- ③ 類数は与えられた素数で割れる。

以下、上の定理の説明をするが、証明は最も簡単な定理 1 のみにし、他はいくつかの補題をのべるにとどめる。

記号の約束 p, l を相異なる素数、 a を p と素な有理整数とする時、 $\left(\frac{a}{p}\right)_l = 1$ で a が $\text{mod. } p$ で l 乗剰余な事を表し、 $\left(\frac{a}{p}\right)_l \neq 1$ でそうでない事を表す。又、有理整数 a, b に対して、 (a, b) で a と b の最大公約数を表す。

§1 判別式負の 3 次体

正の整数 a に対して、 $f(x) = x^3 + ax + 1$ とおけば、これは \mathbb{Q} 上既約で、 $d(f) = -(27 + 4a^3) < 0$ となる。 α を $f(x) = 0$ の一根とし、 $K = k_a = \mathbb{Q}(\alpha)$ とおく。これは判別式負の 3 次体となる。

我々はこの様な K 達のなかで可除性の問題を考えていく。

補題1 H を与えられた自然数とする。 a は 3 と素で、更にある整数 b が存在して $a = b^H$ と仮定する。この時、 $(\alpha+1) = \alpha^H$ とする K の ideal \mathcal{O} が存在する。

$\therefore N_{K/\mathbb{Q}}(\alpha+1) = +a = +b^H$ であるが、 $(a, 3) = 1$ 故 $\alpha+1$ はその共役達と互いに素である。この事から、補題1が得られる。 //

以下、上の ideal \mathcal{O} の位数を問題にしていく。

E を K の全単数群、 E_1 を -1 と α の生成するその部分群とする。
 K は判別式負の 3 次体であるから、 $[E: E_1]$ は有限であるが、
 更に、

補題2 l を与えられた素数とする。 $a \equiv 5 \pmod{17}$ とする。
 次の満たす素数 p が存在すれば、 $[E: E_1]$ は l と素である。

① $p \mid f(-2) = -(2a+7)$

② $\left(\frac{2}{p}\right)_l \neq 1$

③ $\left(\frac{-1}{p}\right)_l = 1$

\therefore 先ず、①と $a \equiv 5 \pmod{17}$ である事から、 p 上の K の 1 次の素 ideal \mathcal{P} で $\alpha+2$ を含むものが存在する。さて、補題を示すには、 K は ± 1 以外に 1 の巾根を含まないので、任意の単数 ε に対して、 " $\varepsilon^l = \pm \alpha^d, d \in \mathbb{Z} \implies d \equiv 0 \pmod{l}$ " を示せば十分。
 上の式を $\text{mod. } \mathcal{P}$ で見ると、 $\varepsilon^l \equiv \pm (-2)^d \pmod{\mathcal{P}}$ となるが、この事と条件②,③から直ちに $d \equiv 0 \pmod{l}$ が得られる。 //

命題 1. $a \not\equiv 0 \pmod{3}$, $a \not\equiv 3 \pmod{5}$, $a \not\equiv 5 \pmod{17}$ とする。
 H を与えられた自然数. $\exists b \in \mathbb{Z}$ s.t. $a = b^H$ と仮定する. この時,
 補題 1 により, $(\alpha+1) = \alpha^H$ となる K の ideal α が存在するが,
 α の位数は次の条件下で H である。

$\exists p_1, p_2$: 素数 s.t.

- ① $p_1 | f(-2) = -(2\alpha+7)$, $p_2 | f(2) = 2\alpha+9$
 ② $\left(\frac{-1}{p_1}\right)_l = 1$, $\left(\frac{2}{p_1}\right)_l \neq 1$, $\forall l = \text{素数} | H$
 ③ $\left(\frac{-1}{p_2}\right)_l = 1$, $\left(\frac{3}{p_2}\right)_l \neq 1$, " .

∴ 先ず、補題 2 の証明中で示した様に、 p_1 上の K の 1 次の素 ideal \mathfrak{p}_1 で $\alpha+2$ を含むものがある。同様に、①より、 p_2 上の K の 1 次の素 ideal \mathfrak{p}_2 で $\alpha-2$ を含むものがある。

この命題を示すには、 H を割る任意の素数 l に対して、 $(\alpha+1)$ が単項 ideal の l 乗ではない事を示せばよい。そこで、 $(\alpha+1) = (\beta)^l$ と仮定する。すると、補題 2 より、 $[E:K]$ は l と素だから、 $\alpha+1 = \pm \alpha^l \varepsilon^l \beta^l$ — ④, $\exists A \in \mathbb{Z}, \exists \varepsilon \in E$ となる。
 ④ を $\text{mod. } \mathfrak{p}_1$ で見ると、②より $A \equiv 0 \pmod{l}$ を得る。従って、 $\alpha+1 \in \pm K^{\times l}$ であるが、これを $\text{mod. } \mathfrak{p}_2$ で見ると、③に反する。 //

次に、命題 1 の条件を満たす a を構成するが、そのためには次の補題が必要である。

H を与えられた自然数とし、

$\zeta = \begin{cases} 1 \text{ の原始 } H \text{ 乗根} & \text{----- } H \text{ が奇数, 又は偶数で } 4 \nmid H \text{ の時.} \\ 1 \text{ の原始 } 2H \text{ 乗根} & \text{----- } H \text{ が偶数で } 4 \nmid H \text{ の時.} \end{cases}$

とし、 $k = \mathbb{Q}(\zeta)$ とおく。又、 $H = \prod p_i^{h_i}$ と素因数分解した時、 $\tilde{H} = \prod p_i'$ とする。

補題3 H が奇数又は2の時、 $k(\sqrt[H]{\zeta})$, $k(\sqrt[\tilde{H}]{2})$ はそれぞれ k の H 次, \tilde{H} 次の巡回拡大であり、両者は k 上独立である。

補題4 H が奇数又は2の時、 $k(\sqrt[H]{\frac{\zeta}{2}})$, $k(\sqrt[\tilde{H}]{3})$ はそれぞれ k の H 次, \tilde{H} 次の巡回拡大であり、両者は k 上独立である。

注意: 補題3は一般の H に対しては必ずしも成り立たない。

例えば、 $H=8$ の時、 $k \ni \sqrt[8]{\zeta} = \sqrt{2}$ となり、又 $H=14$ の時は、

$k(\sqrt[14]{\frac{\zeta}{2}}) = k(\sqrt{2})$ となる。定理1(1)で、“..... 与えられた任意の整数で割れる.....” ではなく、“..... 奇数 (resp. 2)” としてあるのは上の様な理由による。それ以外の定理でも、同様の理由で、主張が少し制限されている。以下、常に H は奇数又は2を表わすものとする。

補題3と類体論により、 k の1次の素idealで、 $k(\sqrt[H]{\zeta})$ で完全分解し、 $k(\sqrt[\tilde{H}]{2})$ で remain prime なものが無数に存在する。それらの内で、2, 3, 5, 7, 17, H と素なものを選びお₁ とする。同様に k の1次の素idealで $k(\sqrt[H]{\frac{\zeta}{2}})$ で完全分解し、 $k(\sqrt[\tilde{H}]{3})$ で remain prime なものが無数に存在するが、それらの内で、2, 3, 5, 7, 17, H , $N \neq 6$ お₁ と素なものを選びお₂ とする。お₁, お₂ を、そ

それぞれ、 $\mathfrak{p}_1, \mathfrak{p}_2$ の $\mathbb{K}(\sqrt[4]{\frac{p}{2}})$, $\mathbb{K}(\sqrt[4]{\frac{q}{2}})$ に於る素因子とする。又、 $\mathfrak{p}_i = \mathfrak{p}_i \cap \mathbb{Q}$ とする。 $\mathfrak{p}_1, \mathfrak{p}_2$ は作り方から1次の素idealで2と素であるから、

$$b_1 \equiv \sqrt[4]{\frac{p}{2}} \pmod{\mathfrak{p}_1}, \quad b_2 \equiv \sqrt[4]{\frac{q}{2}} \pmod{\mathfrak{p}_2}$$

となる有理整数 b_1, b_2 が存在する。次に、有理整数 b を次の様に定める。

$$b \equiv b_i \pmod{\mathfrak{p}_i} \quad i=1, 2$$

$$b \equiv 1 \pmod{3 \cdot 5 \cdot 17}$$

$$b > 0$$

3, 5, 17, $\mathfrak{p}_1, \mathfrak{p}_2$ の内どの2つも互いに素であるから、上の様な b は確かに存在する。そこで、 $a = b^H$ とすれば、これは命題1の条件をすべて満たしている。従って、判別式負の3次体で類数が H で割れるものが(少なくともひとつは)存在する。

更に、

補題5. $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ を $\mathfrak{p}_1, \mathfrak{p}_2, 3, 5, 17$ と素な素数とする。この時、判別式負の3次体で類数が H で割れ、 $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ は remain prime でないものが存在する。

∵ 上の a を構成する段階で、 $b \equiv 0 \pmod{\mathfrak{p}_j}$, $1 \leq j \leq m$, とする様に b を選べばよい。 //

補題6 F を m 次体とし、その \mathbb{Q} 上の Galois closure の Galois 群は m 次対称群になるものとする。この時、 F/\mathbb{Q} で

remain prime な素数が無数に存在する。

∵ Tschebotareff の密度定理より直ちに出る。 //

この2つの補題によつて、判別式負の3次体で類数がH (= 奇数又は2)で割れるものが無数に存在する事がわかる。

§2 判別式正の3次非ガロア体

命題2 正の整数 a に対して、 α を $X^3 - a^2X + 1 = 0$ の一解とし、

$K = K_a = \mathbb{Q}(\alpha)$ とおく。すると、 K は判別式正の3次非ガロア

体となる。 $a \not\equiv 0 \pmod{3}$, $a^2 \not\equiv 2 \pmod{5}$, $a \not\equiv 4 \pmod{11}$, $2a^2 \not\equiv 7$

$\pmod{17}$, $a \not\equiv 250 \pmod{997}$ とする。H を与えられた自然数

とし、ある整数 b に対して $a^2 = b^H$ となることを仮定する。

この時、 $(\alpha+1) = \alpha^H$ となる K の ideal \mathcal{O} が存在するが、 \mathcal{O} の位数

は次の条件下で H となる。

∃ p_1, p_2, p_3, p_4, p_5 : 素数 s.t.

$$\textcircled{1} \quad p_1 | 4a-3, \quad p_2 | 2a+3, \quad p_3 | f(1) = -(a^2-2), \quad p_4 | f(-2) = 2a^2-7,$$

$$p_5 | f(2) = -(2a^2-9)$$

$$\textcircled{2} \quad \left(\frac{-1}{p_i}\right)_\ell = 1 \quad \forall i, \quad \forall \ell = \text{素数} | H$$

$$\textcircled{3} \quad \left(\frac{2}{p_1}\right)_\ell = \left(\frac{2}{p_2}\right)_\ell = \left(\frac{2}{p_4}\right)_\ell \neq 1 \quad \forall \ell \text{ "}$$

$$\textcircled{4} \quad \left(\frac{2}{p_3}\right)_\ell = 1, \quad \left(\frac{a+1}{p_3}\right)_\ell \neq 1 \quad \forall \ell \text{ "}$$

$$\textcircled{5} \quad \left(\frac{3}{p_5}\right)_\ell \neq 1 \quad \forall \ell \text{ "}$$

注意: K の単数群の rank は2であるが、 α と $\beta = \alpha + a$ が独立

な単数である。

この命題の条件を満たす a を構成するための補題は、簡単ではあるが、数が多いため省略する。

§3 4次体の場合

命題3 a を正の整数とし、更に、 $a \not\equiv 0 \pmod{2}$, $a^3 \equiv 1 \pmod{7}$, $2a^3 \equiv -15 \pmod{3^r \cdot 5^4 + 4^6}$, $3a^3 \equiv 80 \pmod{80^4 + 3 \cdot 4^4}$ を満たし、 a は十分大きいとする。 α を $X^4 + a^3X - 1 = 0$ の一根とし、 $K = \mathbb{Q}(\alpha)$ とおく。 K は定理3の条件①, ②を満たす4次体である。 l を与えられた素数とする。 $l \neq 3$ の場合は、ある整数 b に対して、 $a = b^l$ と仮定する。この時、 $(\alpha+1) = \sigma^l$ とする K の ideal σ が存在するが、 σ の位数は次の条件下で l である。

$\exists p_1, p_2, p_3$: 素数 s.t.

$$\textcircled{1} \quad p_1 | f(2) = 2a^3 + 15, \quad p_2 | f(2), \quad p_3 | f(-3) = -(3a^3 - 80)$$

$$\textcircled{2} \quad \left(\frac{-1}{p_i}\right)_l = 1 \quad 1 \leq i \leq 3$$

$$\textcircled{3} \quad \left(\frac{3}{p_1}\right)_l = \left(\frac{2}{p_1}\right)_l = 1, \quad \left(\frac{a+2}{p_1}\right)_l \neq 1$$

$$\textcircled{4} \quad \left(\frac{3}{p_2}\right)_l = 1, \quad \left(\frac{2}{p_2}\right)_l \neq 1$$

$$\textcircled{5} \quad \left(\frac{-2}{p_3}\right)_l \neq 1.$$

注意: K の単数群の rank は 2 であるが、 α と $\beta = \alpha + a$ はその単数で、 a が十分大きければ両者は独立である。

この命題の条件を満たす a を構成するために、次の2つの補

題が必要である。

素数 l に対して、

$$\zeta = \begin{cases} 1 \text{ の原始 } 3l \text{ 乗根} & \dots\dots l \neq 2, 3 \text{ の時.} \\ 1 \text{ の原始 } 12 \text{ 乗根} & \dots\dots l = 2 \text{ の時.} \\ 1 \text{ の原始 } 3 \text{ 乗根} & \dots\dots l = 3 \text{ の時} \end{cases}$$

と置く。 $k = \mathbb{Q}(\zeta)$, $F = k(\sqrt[3]{\frac{15}{2}})$ と置く。

補題 7 $L_1 = F(\sqrt[3]{\frac{15}{2}}, \sqrt[3]{3})$, $L_2 = F(\sqrt[3]{2})$, $L_3 = F(\sqrt[3]{\sqrt[3]{\frac{15}{2}} + 2})$ と置く。

L_2, L_3 は F 上の l 次巡回拡大であり, L_1, L_2, L_3 は F と独立である。

$$\text{即ち } [L_1 \cdot L_2 \cdot L_3 : F] = [L_1 : F] \cdot [L_2 : F] \cdot [L_3 : F].$$

(この補題の証明は複雑であり、 $2 \cdot (\sqrt[3]{\frac{15}{2}} + 2)^3$ が $\mathbb{Q}(\sqrt[3]{\frac{15}{2}})$ の基本単数である事を用いる。)

$$\text{補題 8 } L' = \begin{cases} k(\sqrt[3]{\frac{80}{3}}) & \dots\dots l \neq 3 \text{ の時.} \\ k(\sqrt[3]{-\frac{80}{3}}) & \dots\dots l = 3 \text{ の時.} \end{cases}, \quad L'' = k(\sqrt[3]{2})$$

と置く。 L'' は k の l 次巡回拡大であり, L' と L'' は k 上独立である。

§ 4 5 次体の場合

命題 4 a を正の整数とする。 $a \not\equiv 0 \pmod{2}$, $a \equiv 0 \pmod{3}$, $a \not\equiv 0 \pmod{5}$, $2a^4 \not\equiv 33 \pmod{2^3 \cdot 3^3 \cdot 5^5}$ で a は十分大きいと仮定する。 α を $X^5 - a^4 X - 1 = 0$ の一根とし、 $K = k_a = \mathbb{Q}(\alpha)$ と置く。

これは定理 4 の条件 ①, ② を満たす 5 次体である。 l を与えら

水た素数とする。 $l \neq 2$ の場合は、ある整数 b に対して、
 $a = b^l$ と仮定する。すると、 $(a-1) = \alpha^l$ となる K の ideal α が存在するが、 α の位数は次の条件下で l となる。

$\exists p_1, p_2, p_3, p_4$ 素数 s.t.

$$\textcircled{1} \quad p_i | f(-2) = 2a^4 - 33, \quad 1 \leq i \leq 4$$

$$\textcircled{2} \quad \left(\frac{-1}{p_i}\right)_l = 1, \quad 1 \leq i \leq 4$$

$$\textcircled{3} \quad \left(\frac{-3}{p_1}\right)_l = \left(\frac{-2}{p_1}\right)_l = \left(\frac{a-2}{p_1}\right)_l = 1, \quad \left(\frac{a+2}{p_1}\right)_l \neq 1$$

$$\textcircled{4} \quad \left(\frac{-3}{p_2}\right)_l = \left(\frac{-2}{p_2}\right)_l = 1, \quad \left(\frac{a-2}{p_2}\right)_l \neq 1$$

$$\textcircled{5} \quad \left(\frac{-3}{p_3}\right)_l = 1, \quad \left(\frac{-2}{p_3}\right)_l \neq 1$$

$$\textcircled{6} \quad \left(\frac{-3}{p_4}\right)_l \neq 1.$$

注意: K の単数群の rank は 3 である。 $\alpha, \beta = \alpha + a, \gamma = \alpha - a$ は、

K の単数で a が十分大きければ、この 3 つは独立になる。

この命題の条件を満たす a を構成するには次の補題が必要である。

素数 l に対して、

$$\zeta = \begin{cases} 1 \text{ の原始 } 4l \text{ 乗根} & \dots\dots l \neq 2 \text{ の時} \\ 1 \text{ の原始 } 4 \text{ 乗根} & \dots\dots l = 2 \text{ の時} \end{cases}$$

とする。 $K = \mathbb{Q}(\zeta)$, $F = K(\sqrt[l]{33})$ とする。 $\sqrt[l]{33}$ はひとつ固定する。

$$\text{補題 9} \quad L_1 = F(\sqrt[l]{33}), \quad L_2 = F(\sqrt[l]{-3}), \quad L_3 = F(\sqrt[l]{2}), \quad L_4 = F(\sqrt[l]{\sqrt[l]{33} + 2})$$

$L_5 = F(\sqrt[l]{\sqrt[l]{33} - 2})$ とする。この時、 L_2, L_3, L_4 は F の l 次巡回拡大であり、 $L_1 \sim L_5$ は F と独立である。 i.e. $[L_1 \cdot L_2 \cdot L_3 \cdot L_4 \cdot L_5 : F]$

$$= \prod_{i=1}^5 [L_i : F] \quad \text{となる。}$$

(この補題の証明は非常に複雑である。その証明のなかで、 $(\sqrt[4]{\frac{33}{2}} - 2) \cdot (\sqrt[4]{\frac{33}{2}} + 2)^{-1}$, $2(\sqrt{\frac{33}{2}} - 4)^2$ が $\mathbb{Q}(\sqrt[4]{\frac{33}{2}})$ の基本単数系である事を用いる。)

より高次の場合、これまでと同じ様に、 $x^m \pm a^{m-1}x \pm 1 = 0$ という方程式で定義される体のなかで可除性の問題が解かれる事が期待される。しかし、 m が大きいと独立な単数をすべてみつけ出すのがきつめて困難である。

参考文献

- [1] S. Kuroda : On the class number of imaginary quadratic number fields. Proc. Japan Acad. 40 (1964), p365~367
- [2] T. Nagel : Über die Klassenzahl imaginär-quadratischer Zahlkörper. Abh. Math. Sem. Univ. Hamburg 1 (1922), p140~150
- [3] H. J. Stender : Eine Formel für Grundeinheiten in reinen algebraischen Zahlkörpern dritten, vierten und sechsten Grades. J. Number theory 7 (1975), p235~249
- [4] K. Uchida : Class numbers of cubic cyclic fields. J. Math. Soc. Japan 26 (1974) p447~452
- [5] H. Wada : A table of fundamental units of purely cubic fields.

190

Proc. Japan Acad. 46 (1970), p1135~1140

[6] Y. Yamamoto : On unramified Galois extensions of quadratic number fields, Part I. Osaka J. Math. 7 (1970), p57~67