数理解析研究所講究録
440巻 1981年 179-190

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さん(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かれている。

(i) 虚2次体 (Nagel[2], 黒田[1], 山本[6])

(ii) 実2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.

180

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 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わす。又、有理整数 a, b に対して、(a,b) で a と b の最大公約数を表わす。

§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Kα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。αは3と素で、更にある整数bが存在して $\alpha = b^H$ と仮定する。この時、$(\alpha+1) = \mathfrak{A}^H$ となるKのidealAが存在する。

∵　$N_{K/\mathbb{Q}}(\alpha+1) = +a = +b^H$ 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idealA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。$a \not\equiv 5 \pmod{17}$ とする。次を満たす素数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 $\left(\frac{-1}{p}\right)_l = 1$.

∵　先ず、①とaの条件からpがKの1次の素idealP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、"$\varepsilon^l = \pm\alpha^A,\ A \in \mathbb{Z} \Longrightarrow A \equiv 0 \pmod{l}$" を示せば十分。上の式をmod.Pで見ると、$\varepsilon^l \equiv \pm(-2)^A \pmod{P}$ となるが、この事と条件②,③から直ちに $A \equiv 0 \pmod{l}$ が得られる。 //

182

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、$(\alpha+1) = \mathfrak{A}^H$ となる k の ideal $\mathfrak{A}$ が存在するが、$\mathfrak{A}$ の位数は次の条件下で H である。

$\exists p_1, p_2$: 素数 s.t.

① $p_1 \mid f(-2) = -(2a+17)$, $p_2 \mid f(2) = 2a+9$

② $\left(\frac{-1}{p_1}\right)_\ell = 1$, $\left(\frac{2}{p_1}\right)_\ell \not\equiv 1$, $\forall \ell =$素数$\mid H$

③ $\left(\frac{-1}{p_2}\right)_\ell = 1$, $\left(\frac{3}{p_2}\right)_\ell \not\equiv 1$, 〃 .

∵ 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 乗では無い事を示せばよい。そこで、$(\alpha+1) = (\beta)^\ell$ と仮定する。すると、補題2より、$[E:E_1]$ は ℓ と素だから、$\alpha+1 = \pm \alpha^\lambda \varepsilon^\ell \beta^\ell$ —— ⊛ , $\exists \lambda \in \mathbb{Z}$, $\exists \varepsilon \in E$ となる。
⊛ を $\bmod \mathfrak{p}_1$ で見ると、②より $\lambda \equiv 0 \pmod \ell$ を得る。従って、$\alpha+1 \in \pm K^{\times \ell}$ であるが、これを $\bmod \mathfrak{p}_2$ 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、

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

とし、$k = \mathbb{Q}(\zeta)$ とおく。又、$H = \prod_j \mathfrak{l}_j^{n_j}$ と素因数分解された時、$\tilde{H} = \prod \mathfrak{l}_j'$ とする。

補題3　H が奇数又は2の時、$k(\sqrt[H]{\frac{\pi}{2}})$, $k(\sqrt[\tilde{H}]{2})$ 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、$k(\sqrt[H]{\frac{\pi}{2}})$, $k(\sqrt[\tilde{H}]{3})$ 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たたない。例えば、$H=8$ の時、$k \ni \sqrt[8]{2} = \sqrt{2}$ となり、又 $H = 14$ の時は、$k(\sqrt{\frac{\pi}{2}}) = k(\sqrt{2})$ 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、$k(\sqrt[H]{\frac{\pi}{2}})$ 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 と素なものをひとつ選び $\mathfrak{p}$ とする。同様に k の1次の素 ideal で $k(\sqrt[H]{\frac{\pi}{2}})$ 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, $N\mathfrak{p}$ と素なものを選び $\mathfrak{p}_1$ とする。$\mathfrak{p}, \mathfrak{p}_1$ を、そ

それぞれ、$\mathfrak{P}_1, \mathfrak{P}_2$ の $k(\sqrt[H]{\frac{\pi}{2}})$, $k(\sqrt[H]{-\frac{\pi}{2}})$ に於る素因子とする。又、$P_i = \mathfrak{P}_i \cap \mathbb{Q}$ とする。$\mathfrak{P}_1, \mathfrak{P}_2$ は作り方から1次の素idealで之と素であるから、

$b_1 \equiv \sqrt[H]{\frac{\pi}{2}} \pmod{\mathfrak{P}_1}$, $b_2 \equiv \sqrt[H]{-\frac{\pi}{2}} \pmod{\mathfrak{P}_2}$

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。

$b \equiv b_i \pmod{P_i}$ $i=1,2$

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

$b > 0$

3, 5, 17, P_1, 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、$a = b^H$ とおけば、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. $g_1, \cdots, g_m$ を $P_1, P_2, 3, 5, 17$ 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、$g_1, \cdots, g_m$ は remain prime ではないものが存在する。

∵ 上の a を構成する段階で、$b \equiv 0 \pmod{g_j}$, $1 \le j \le m$, となる様に b を選べばよい。 //

補題6 F を n 次体とし、その $\mathbb{Q}$ 上の galois closure の galois 群は n 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つの補題によって、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 $X^3 - a^2X + 1 = 0$ の一根とし、$K = K_a = \mathbb{Q}(\alpha)$ とおく。すると、K は判別式正の3次非ガロア体となる。$a \equiv 0 \pmod 3$, $a^2 \equiv 2 \pmod 5$, $a \equiv 4 \pmod{11}$, $2a^2 \equiv 7 \pmod{17}$, $a \equiv 250 \pmod{997}$ とする。H を与えられた自然数とし、ある整数 b に対して $a^2 = b^H$ となっていると仮定する。この時、$(\alpha+1) = \mathfrak{A}^H$ となる K の ideal $\mathfrak{A}$ が存在するが、$\mathfrak{A}$ の位数は次の条件下で H となる。

$\exists p_1, p_2, p_3, p_4, p_5$: 素数 s.t.

① $p_1 \mid 4a-3$, $p_2 \mid 2a+3$, $p_3 \mid f(1) = -(a^2-2)$, $p_4 \mid f(-2) = 2a^2 - 7$, $p_5 \mid f(2) = -(2a^2 - 9)$

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

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

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

⑤ $\left(\frac{3}{p_5}\right)_\ell \neq 1$. $\forall \ell$ 〃.

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、数が多いので省略する。

§3 4次体の場合

命題3 aを正の整数とし、更に、$a \not\equiv 0 \pmod 2$, $a^3 \equiv 1 \pmod 7$, $2a^3 \not\equiv -15 \pmod{3^7 \cdot 5^4 + 4^6}$, $3a^3 \not\equiv 80 \pmod{80^4 + 3 \cdot 4^4}$ 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、$K = k_a = \mathbb{Q}(\alpha)$ 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、$(\alpha+1) = \mathfrak{A}^l$ となるKのidealAが存在するが、A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.

① $P_1 \mid f(2) = 2a^3 + 15$, $P_2 \mid f(2)$, $P_3 \mid f(-3) = -(3a^3 - 80)$

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

③ $\left(\frac{3}{P_1}\right)_l = \left(\frac{2}{P_1}\right)_l = 1$, $\left(\frac{a+2}{P_1}\right)_l \neq 1$

④ $\left(\frac{3}{P_2}\right)_l = 1$, $\left(\frac{2}{P_2}\right)_l \neq 1$

⑤ $\left(\frac{-2}{P_3}\right)_l \neq 1$.

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、

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

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

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

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 上独立である。

i.e. $[L_1 \cdot L_2 \cdot L_3 : F] = [L_1 : F] \cdot [L_2 : F][L_3 : F]$.

（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。）

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

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

れた素数とする。$l \neq 2$ の場合は、ある整数 b に対して、$a = b^l$ と仮定する。すると、$(\alpha - 1) = \mathfrak{A}^l$ となる K の ideal $\mathfrak{A}$ が存在するが、$\mathfrak{A}$ 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.

① $P_i \mid f(-2) = 2a^4 - 33$, $1 \leq i \leq 4$

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

③ $\left(\frac{-3}{P_1}\right)_l = \left(\frac{-2}{P_1}\right)_l = \left(\frac{a-2}{P_1}\right)_l = 1$, $\left(\frac{a+2}{P_1}\right)_l \neq 1$

④ $\left(\frac{-3}{P_2}\right)_l = \left(\frac{-2}{P_2}\right)_l = 1$, $\left(\frac{a-2}{P_2}\right)_l \neq 1$

⑤ $\left(\frac{-3}{P_3}\right)_l = 1$, $\left(\frac{-2}{P_3}\right)_l \neq 1$

⑥ $\left(\frac{-3}{P_4}\right)_l \neq 1$.

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

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

とする。$k = \mathbb{Q}(\zeta)$, $F = k\left(\sqrt[4]{\frac{33}{2}}\right)$ とする。$\sqrt[4]{\frac{33}{2}}$ はひとつ固定する。

補題 9 $L_1 = F\left(\sqrt[l]{\frac{33}{2}}\right)$, $L_2 = F\left(\sqrt[l]{-3}\right)$, $L_3 = F\left(\sqrt[l]{2}\right)$, $L_4 = F\left(\sqrt[l]{\sqrt[4]{\frac{33}{2}} + 2}\right)$

$L_5 = F\left(\sqrt[l]{\sqrt[4]{\frac{33}{2}} - 2}\right)$ 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 上独立である。i.e. $[L_1 \cdot L_2 \cdot L_3 \cdot L_4 \cdot L_5 : F]$

$= \prod_{i=1}^{5} [L_i : K]$ となる。

(この補題の証明は非常に複雑である。その証明の中で、$(\sqrt[4]{\frac{33}{2}} - 2)\cdot(\sqrt[4]{\frac{33}{2}} + 2)^{-1}$, $2(\sqrt{\frac{33}{2}} - 4)^2$ 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、$x^n \pm a^{n-1}x \pm 1 = 0$ という方程式で定義される体の中で可除性の問題が解かれる事が期待される。しかし、n が大きいと独立な単数をすべてみつけ出すのがきわめて困難である。

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.

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