数理解析研究所講究録
第589巻 1986年 112-122

多項式 x^n+ax^l+b のガロア群について

立教大 理 長田弘幸 (Hiroyuki Osada)

$f(x)=x^n+ax+b$ とし、K を $\mathbb{Q}$ 上 $f(x)$ の分解体とするとき、任意の n に対して $a,b\in\mathbb{Z}$ を適当にとれば、$Gal(K/\mathbb{Q})\simeq S_n$ となることが[8],[16]で示された。また、p を素数とするとき、x^p+ax^2+b, $x^p+ax^l\pm1$ の $\mathbb{Q}$ 上のガロア群 G が $G\simeq S_p$ になるための条件が[3]で示された。ここでは、一般的な三項式 x^n+ax^l+b の $\mathbb{Q}$ 上のガロア群 G が $G\simeq S_n$ になるための条件を示す。また、この結果から Williams — 内山の予想の証明が得られる。

ここで、Williams — 内山の予想について説明する。

$f(x)=x^n+x+a$, p を素数とするとき $f(x)$ を $\bmod p$ で既約にするような最小の正整数 a を

$a_n(p)$ とし、$a_n = \lim_{p\to\infty} \inf a_n(p)$ とするとき、

$$\begin{cases} (1) & n=2 \text{ or } n\not\equiv 2 \pmod 3 \Rightarrow a_n = 1 \\ (2) & n\equiv 2 \pmod 3,\ n=\text{even}>2 \Rightarrow a_n = 2 \\ (3) & n\equiv 2 \pmod 3,\ n=\text{odd} \Rightarrow a_n = 3 \end{cases}$$

が成り立つ。これがWilliams—内山の予想である。この予想は $n=2,3$ のとき、正しいことが[13]で示され、$n=4,6,9$ 及び任意の素数のとき、正しいことが[9]で示された。また、$n\leq 20$ 及びいくつかの n の値に対して正しいことが[2], [8]で示された。ここでは任意の n に対して、この予想が正しいことを証明する。

定理1　$f(x)=x^n+ax^l+b \in \mathbb{Z}[x]$, $a=a_0c^n$, $b=b_0^l c^n$, とし、K を $\mathbb{Q}$ 上 $f(x)$ の分解体とするとき、次の条件を満せば、$G=\mathrm{Gal}(K/\mathbb{Q}) \simeq S_n$ となる。

(1)　$f(x)$ は $\mathbb{Q}$ 上既約

(2)　$(a_0c(n-l)l,\ nb_0)=1$

$D(f)$ を $f(x)$ の判別式とすると、条件(2)より、$D(f) = (-1)^{\frac{n(n-1)}{2}} \cdot b_0^{l(l-1)} \cdot c^{n(n-1)} \cdot D_0(f)$ となる。ここで、$D_0(f) = n^n b_0^{l(n-l)} + (-1)^{n-1} l^l (n-l)^{n-l} a_0^n c^{nl}$。

補題1　p を素数，$\mathfrak{p}$ を K の素 ideal とし、$\mathfrak{p} | p$ とする。そのとき、$p | D_0(f)$ ならば、$\mathbb{Q}$ 上 $\mathfrak{p}$ の惰性群は互換から生成される位数2の群となる。

補題2　p を素数とする。そのとき $p | b$ ならば p は K で不分岐となる。(c.f. [5])。

補題3　互換から生成された群 H が、n 文字上可移ならば、$H \cong S_n$ となる。

定理1の証明　p を素数とし、$\mathfrak{p}$ を K の素 ideal とし、$\mathfrak{p} | p$ とする。もし $p | D_0(f)$ ならば、補題1より、$\mathbb{Q}$ 上 $\mathfrak{p}$ の惰性群は互換から生成される位数2の群となる。もし、$p | b$ ならば、補題2より、p は K で不分岐となる。従って、全ての惰性群から生成される群を H とす

ると．Minkowskiの定理から、$H=G=Gal(K/\mathbb{Q})$となる。従って条件(1)からGは互換から生成される群で可移となるから．補題3より．$G\simeq S_m$となる。

系1　$K/\mathbb{Q}(\sqrt{D(f)})$は不分岐$A_m$拡大（全ての有限素点）となる。

証明　$\mathfrak{P}$をKの素idealとし．$K/\mathbb{Q}$における$\mathfrak{P}$の惰性群をTとすると．$K/\mathbb{Q}(\sqrt{D(f)})$における$\mathfrak{P}$の惰性群は$A_m\cap T$となる。Tは自明か互換から生成される位数2の群だから．$A_m\cap T=\{1\}$となる。

定理1において．$l=1$とするとき．次の系が得られる。

系2　$f(x)=x^m+ax+b\in\mathbb{Z}[x]$，$a=a_0c^m$，$b=b_0c^m$，とするとき．次の条件を満せば．$Gal(K/\mathbb{Q})\simeq S_m$となる。

(1) $f(x)$ は $\mathbb{Q}$ 上既約

(2) $(a_0 c(n-1), n b_0) = 1$

さらに、$K/\mathbb{Q}(\sqrt{D(f)})$ は不分岐 A_n 拡大（全ての有限素点）となる。

注　Nart からの私信によって、系2はすでに Nart－Vila [6] によって示されていることを、知った。

例　$f(x) = x^5 + 3x + 1$ とする。そのとき、$f(x)$ は系2の条件を満し、$K/\mathbb{Q}(\sqrt{D(f)})$ は不分岐 A_n 拡大（全ての有限素点）となる。また、$D(f) = 65333$ となり、$\mathbb{Q}(\sqrt{65333})$ の広義の類数は1となる。(c.f. [12])。

補題4　$f_1(x) = x^n - x - 1$ $(n \geq 2)$,
$f_2(x) = x^n + x + 1$　$n \not\equiv 2 \pmod 3$ とするとき、
$f_1(x)$, $f_2(x)$ は $\mathbb{Q}$ 上既約になる。(c.f. [7])。

系2と補題4から、次の系を得る。

系3　x^n-x-1 $(n\geqq 2)$ の $\mathbb{Q}$ 上のガロア群 G は、$G\cong S_n$ となる。

補題5　p を素数、
$f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x\pm p\in\mathbb{Z}[x]$ とするとき、次の条件を満せば、$f(x)$ は $\mathbb{Q}$ 上既約となる。

(1)　$1+|a_1|+|a_2|+\cdots+|a_{n-1}|<p$

or

(2)　$1+|a_1|+|a_2|+\cdots+|a_{n-1}|=p$ となり、$f(x)$ は1の中根をもたない。

Williams—内山の予想の証明

最初に、(1) $n=2$ or $n\not\equiv 2\pmod 3$ $\Rightarrow$ $a_n=1$ を証明する。　$n=2$ のとき、x^2+x+1 は $\mathbb{Q}$ 上既約だから、x^2+x+1 の $\mathbb{Q}$ 上のガロア群 G は、$G\cong S_2$ となる。　$n\not\equiv 2\pmod 3$ のとき、系2と補題4より、x^n+x+1 の $\mathbb{Q}$ 上のガロア群 G は、$G\cong S_n$ となる。従って、$n=2$ or $n\not\equiv 2\pmod 3$ のとき、x^n+x+1 の $\mathbb{Q}$ 上のガロア群

Gは、$G \subset S_n$ となり、Gは n-cycle を含む。
従って、Čebotarev の密度定理[1]より、$a_n = 1$
となり、(1) を得る。

次に、(2) $n \equiv 2 \pmod 3$, $n = \text{even} > 2 \Rightarrow a_n = 2$,
(3) $n \equiv 2 \pmod 3$, $n = \text{odd} \Rightarrow a_n = 3$, を証明
する。 $f_1(x) = x^n + x + 2$ $(n = \text{even} \geq 2)$,
$f_2(x) = x^n + x + 3$ $(n \geq 2)$, とするとき、補題5
より、$f_1(x)$, $f_2(x)$ は $\mathbb{Q}$ 上既約になる。従って、
系2から、$f_1(x)$, $f_2(x)$ の $\mathbb{Q}$ 上のガロア群 G は、
$G \subset S_n$ となり、G は n-cycle を含むから、
Čebotarev の密度定理より、(2), (3) を得る。

定理1と同様にして、次の定理が得られる。

定理2 $f(x) = x^n + ax^2 + b \in \mathbb{Z}[x]$,
$a = a_0 c^n$, $b = b_0 c^n$, とするとき、次の条件を
満せば、$\mathrm{Gal}(K/\mathbb{Q}) \subset S_n$ となる。

(1) $f(x)$ は $\mathbb{Q}$ 上既約

(2) $(a_0 c^{(n-2)2}, n b_0) = 1$

さらに、$K/\mathbb{Q}(\sqrt{D(f)})$ は不分岐 A_n 拡大(全

ての有限素点）となる。　ここで、$D(f) = (-1)^{\frac{n(n-1)}{2}} \cdot b_0 \cdot C^{n(n-1)} \cdot [n^n b_0^{n-2} + (-1)^{n-1} 4 \cdot (n-2)^{n-2} \cdot a_0^n C^{2n}]$。

例　$f(x) = x^5 + 2x^2 + 1$ とする。$f(x)$ は、定理1 or 定理2 の条件を満し、$K/\mathbb{Q}(\sqrt{D(f)})$ は、不分岐 A_5 拡大（全ての有限素点）となる。また、$D(f) = 6581$ より、$\mathbb{Q}(\sqrt{6581})$ の狭義の類数は1となる。（c.f. [12]）。

さらに、条件を加えると、次の定理が得られる。

定理3　$f(x) = x^n + ax^l + b \in \mathbb{Z}[x]$, $a = a_0 C^n$, $b = b_0 C^n$ とし、$l = p$ or $2p$ (pは素数) とするとき、次の条件を満せば、$Gal(K/\mathbb{Q}) \simeq S_n$ となる。

(1)　$f(x)$ は $\mathbb{Q}$ 上既約

(2)　$(a_0 c^{(n-l)l}, n b_0) = 1$

(3)　$\sqrt{|D_0(f)|} \notin \mathbb{Q}$

(4)　$q \| b$ for some prime number q

ここで． $D_0(f) = D(f) \cdot (-1)^{\frac{n(n-1)}{2}} / b_0^{l-1} C^{n(n-1)}$ 。

注　　定理２より． $l=2$ のとき．条件(3),(4)は必要なし。　$l=3, 4, 6$ のとき．条件(4)は必要なし。

例　$f(x) = x^5 + x^3 + 5$ とする。　$f(x)$ は定理３の条件を満し．$f(x)$ の $\mathbb{Q}$ 上のガロア群 G は．$G \subset S_5$ となる。　$D(f) = 5^2 \cdot D_0(f)$ となり．$D_0(f) = 78233$ は素数となる。

参考文献

[1] N.Čebotarev : Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gagebenen Substitutionsklasse gehören., Math. Ann. 95 (1926), 191−228.

[2] B.C. Mortimer and K.S. Williams : Note on a paper of S. Uchiyama., Canada. Math. Bull. 17 (1974), 289−293.

[3] K. Ohta : On unramified Galois extensions of quadratic number fields (in Japanese)., Sûgaku 24 (1972), 119-120.

[4] H. Osada : The Galois groups of the polynomials $x^n + ax^l + b$., to appear.

[5] P.Llorente, E. Nart and N.Vila : Discriminants of number fields defined by trinomials., Acta Arith. 43 (1984), 367-373.

[6] E. Nart and N. Vila : Equations of the type $x^n + ax + b$ with absolute Galois groups S_n ., Rev. Univ. Santander. No.2, II (1979), 821-825.

[7] E.S. Selmer : On the irreducibility of certain trinomials., Math. Scand. 4 (1956), 287-302.

[8] K. Uchida : Unramified extensions of quadratic number field II., Tôhoku. Math. J. 22 (1970), 220-224.

[9] S. Uchiyama : On a conjecture of K.S. Williams., Proc. Japan Acad. 46 (1970), 755-757.

[10] S. Uchiyama and S. Hitotumatu : On the irreducibility of certain polynomials (in Japanese)., R.I.M.S. Kokyuroku. 155 (1972), 14-30.

[11] B.L. Van der Wearden: Moderne Algebra., Vol. I, Ungar, New York, 1949.

[12] H. Wada: A table of ideal class numbers of real quadratic fields (in Japanese)., Sophia Kokyuroku in Math. 10(1981).

[13] K.S. Williams: On two conjectures of Chowla., Canad. Math. Bull. 12(1969), 545-565.

[16] Y. Yamamoto: On unramified Galois extensions of quadratic number fields., Osaka. J. Math. 7(1970), 57-76.