

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、 $\text{Gal}(K/\mathbb{Q}) \cong S_n$ 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 , $x^p+ax^l \pm 1$ の $\mathbb{Q}$ 上のガロア群 G が $G \cong S_p$ 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 $G \cong S_n$ 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 $\text{mod } p$ で既約にするような最小の正整数 a を

$a_n(p)$ とし, $a_n = \lim_{p \rightarrow \infty} \inf a_n(p)$ 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 $f(x) = x^n + ax^2 + b \in \mathbb{Z}[x]$, $a = a_0 c^n$, $b = b_0 c^m$, とし, K を $\mathbb{Q}$ 上 $f(x)$ の分解体とすると, 次の条件を満たせば, $G = \text{Gal}(K/\mathbb{Q}) \cong S_n$ となる。

(1) $f(x)$ は $\mathbb{Q}$ 上既約

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

$D(f)$ を $f(x)$ の判別式とすると、条件 (2) より、
 $D(f) = (-1)^{\frac{n(n-1)}{2}} \cdot b_0^{l(l-1)} \cdot c^{m(m-1)} \cdot D_0(f)$ となる。こ
 こで、 $D_0(f) = n^n b_0^{l(m-l)} + (-1)^{m-1} l^l (m-l)^{m-l} \alpha_0^m c^{ml}$ 。

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
 $\mathfrak{p}$ の慣性群は自明な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 $\mathfrak{p}$ の慣性群は自明な互換から生
 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、全ての慣性群から生成される群を H とす

ると、Minkowskiの定理から、 $H = G = \text{Gal}(K/\mathbb{Q})$ 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、 $G \cong S_m$ 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 $\mathfrak{p}$ の慣性群を T とすると、 $K/\mathbb{Q}(\sqrt{D(f)})$ における $\mathfrak{p}$ の慣性群は $A_m \cap T$ となる。 T は自明な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 $f(x) = x^m + ax + b \in \mathbb{Z}[x]$, $a = a_0 c^m$,
 $b = b_0 c^m$, とするとき、次の条件を満たせば、
 $\text{Gal}(K/\mathbb{Q}) \cong S_m$ となる。

- (1) $f(x)$ は $\mathbb{Q}$ 上既約
 (2) $(a_0c(n-1), mb_0) = 1$

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 の条件を満たし、 $K/\mathbb{Q}(\sqrt{D(f)})$ 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 $f_1(x) = x^m - x - 1$ ($m \geq 2$),
 $f_2(x) = x^m + x + 1$ $m \not\equiv 2 \pmod{3}$ 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 $x^n - x - 1$ ($n \geq 2$) 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,

$f(x) = x^n + a_1 x^{n-1} + \dots + a_{n-1} x \pm P \in \mathbb{Z}[x]$ とするとき, 次の条件を満たせば, $f(x)$ は $\mathbb{Q}$ 上既約となる。

$$(1) \quad 1 + |a_1| + |a_2| + \dots + |a_{n-1}| < P$$

or

(2) $1 + |a_1| + |a_2| + \dots + |a_{n-1}| = P$ となり, $f(x)$ は 1 の n 乗根をもたない。

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、 $G \cong S_n$ 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、

$G \cong S_n$ 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 $f(x) = x^m + ax^2 + b \in \mathbb{Z}[x]$,

$a = a_0 c^m$, $b = b_0 c^m$, とするとき、次の条件を

満たせば、 $\text{Gal}(K/\mathbb{Q}) \cong S_m$ となる。

(1) $f(x)$ は $\mathbb{Q}$ 上既約

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

さらに、 $K/\mathbb{Q}(\sqrt{D(f)})$ は不分岐 A_m 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 の定理 2 の条件を満し、 $K/\mathbb{Q}(\sqrt{D(f)})$
は、不分裂 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 $f(x) = x^n + ax^l + b \in \mathbb{Z}[x]$,
 $a = a_0 c^n$, $b = b_0 c^m$ とし、 $l = p$ の $2p$ (p は素数)
とするとき、次の条件を満せば、 $\text{Gal}(K/\mathbb{Q}) \simeq S_n$
となる。

- (1) $f(x)$ は $\mathbb{Q}$ 上既約
- (2) $(a_0 c^{(n-l)l}, m b_0) = 1$
- (3) $\sqrt{|D_0(f)|} \notin \mathbb{Q}$
- (4) $8 \nmid b$ for some prime number 8

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) は必要ない。 $l=3, 4, 6$ のとき、条件 (4) は必要ない。

例 $f(x) = x^5 + x^3 + 5$ とする。 $f(x)$ は定理 3 の条件を満たし、 $f(x)$ の $\mathbb{Q}$ 上のガロア群 G は $G \subseteq S_5$ 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 gegebenen 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 $x^m + ax^l + b$., 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 $x^m + ax + b$ 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.

[1] B.L. Van der Weerden: *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.