TOKYO J. MATH.
VOL. 16, NO. 1, 1993

On Certain Affect-Free Equations

Kenzo KOMATSU

Keio University

§1. Affect-free equations.

What is the *simplest* affect-free equation (§5) of given degree n? Although many affect-free equations are known, simple examples are rare (cf. [5], [6]). Perhaps one of the simplest examples is the equation

$$x^n - x - 1 = 0 , \tag{1.1}$$

which is affect-free for every $n > 1$ ([4], Theorem 4). Another possible answer to our question is the equation

$$x^n + 2x + 2 = 0 , \tag{1.2}$$

which is also affect-free for every $n > 1$ (§4).

The equation (1.2) is much different from (1.1). For example, it is obvious that the left-hand side of (1.2) is irreducible; it is not at all obvious that the left-hand side of (1.1) is irreducible (Selmer [7]). Let α denote a root of (1.2), and let β denote a root of (1.1). Then the prime number 2 is completely ramified (§5) in $\boldsymbol{Q}(\alpha)$, whereas no prime numbers are completely ramified in $\boldsymbol{Q}(\beta)$ if $n > 2$. The discriminant of $\boldsymbol{Q}(\beta)$ is square-free ([4], Theorem 3), whereas the discriminant of $\boldsymbol{Q}(\alpha)$ is not square-free. Therefore, Theorem 1 of our previous paper [4] is not applicable to the equation (1.2).

The main purpose of the present paper is to prove the following theorem.

THEOREM 1. *Let $a_0, a_1, \cdots, a_{n-1}$ $(n > 1)$ be integers such that*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

is irreducible over $\boldsymbol{Q}$. Let α be a root of $f(x) = 0$, and let $K = \boldsymbol{Q}(\alpha)$, $\delta = f'(\alpha)$, $D = \mathrm{norm}\,\delta$ (in K). Let $x_0, x_1, \cdots, x_{n-1}$ be integers such that

$$D/\delta = x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1} .$$

Suppose that the following three conditions are satisfied.

Received March 5, 1991

1. $(D, x_0, x_1, \cdots, x_{n-1})$ *is a power of* 2.
2. *The prime number* 2 *is completely ramified in K.*
3. *D is not divisible by* 2^{n+1}.

Then the equation $f(x)=0$ *is affect-free.*

§2. Lemmas.

To prove our theorem, we require the following lemma.

LEMMA 1. *Let d denote the discriminant of an algebraic number field of degree n.*
1. *If* $n \geq 3$, *then* $|d| > 2^n$.
2. *If* $n \geq 2$, *then* $|d| > 2^{n-1}$.

PROOF. It is well-known ([1], §18) that

$$|d| > \left(\frac{\pi}{4}\right)^n \left(\frac{n^n}{n!}\right)^2 .$$

By Stirling's formula, we see that

$$\frac{n^n}{n!} > \frac{e^n}{\sqrt{2\pi n}} e^{-1/12n} .$$

Hence we obtain

$$|d| > \left(\frac{\pi}{4}\right)^n \frac{e^{2n-1/6n}}{2\pi n} . \tag{2.1}$$

Now let $(x>0)$

$$g(x) = x \log \frac{\pi}{4} + \left(2x - \frac{1}{6x}\right) - \log(2\pi x) - x \log 2. \tag{2.2}$$

Then

$$g'(x) = \log \frac{\pi}{4} + 2 + \frac{1}{6x^2} - \frac{1}{x} - \log 2 = (\log \pi - \log 8 + 2) - \frac{1}{x} + \frac{1}{6x^2} .$$

Since

$$\log \pi - \log 8 + 2 > 1 ,$$

we see that $g'(x) > 0$ for every $x \geq 1$.

On the other hand,

$$g(3) > 0.1 > 0 .$$

Hence $g(n) > 0$ for every $n \geq 3$. From (2.1) and (2.2) we obtain $|d| > 2^n$ for every $n \geq 3$.

The second assertion is now obvious, since $|d|\geq 3$ for $n=2$.

We also require the following result (van der Waerden [8]).

LEMMA 2. *Let $f(x)$ be an irreducible polynomial of degree n with rational coefficients, and let α be a root of $f(x)=0$. Let G denote the Galois group of $f(x)=0$ over $\boldsymbol{Q}$. G is a transitive permutation group on $\{1, 2, \cdots, n\}$. If there exists a prime number p such that the discriminant d of $\boldsymbol{Q}(\alpha)$ is exactly divisible by p (i.e. $p|d, p^2\nmid d$), then G contains a transposition.*

§3. Proof of Theorem 1.

Now we prove Theorem 1. We may suppose that $n\geq 3$. Let d denote the discriminant of K. Then by the conditions 2 and 3, we see that d is exactly divisible by 2^{n-1} or 2^n, since D is divisible by d. If p is an odd prime factor of d, then D is divisible by p, and so $p\nmid x_i$ for some i; this implies that d is exactly divisible by p ([2], Theorem 1). Hence $|d|$ is of the form

$$|d|=2^{n-1}b \quad \text{or} \quad 2^n b\,, \tag{3.1}$$

where b is a square-free odd integer. Clearly $b\neq 1$ (Lemma 1). Hence there exists an odd prime p such that d is exactly divisible by p. The Galois group G of $f(x)=0$ over $\boldsymbol{Q}$ is a transitive permutation group on $\{1, 2, \cdots, n\}$. It follows from Lemma 2 that G contains a transposition.

Now we show that G is primitive. Suppose that K has a subfield F such that

$$\boldsymbol{Q}\subset F\subset K\,, \quad F\neq \boldsymbol{Q}\,, \quad F\neq K\,.$$

Let $[F:\boldsymbol{Q}]=k$, $[K:F]=m$. Then

$$k\geq 2\,, \quad m\geq 2\,, \quad n=km\,. \tag{3.2}$$

Let d_F denote the discriminant of F. Then d is divisible by d_F^m ([1], Satz 39).

Hence, by (3.1) and (3.2), we see that $|d_F|$ ia a power of 2. Since the prime number 2 is completely ramified in K, it is also completely ramified in F. If k is odd, then $|d_F|=2^{k-1}$. This is impossible (Lemma 1), since $k\geq 2$. Hence k is even. Let $\mathfrak{D}_F$, $\mathfrak{D}_K$, $\mathfrak{D}_{K/F}$ denote the differents of F, K, K/F, respectively. Let $\mathfrak{p}$ (resp. $\mathfrak{P}$) denote the prime ideal in F (resp. K) such that

$$2=\mathfrak{p}^k\,, \qquad \mathfrak{p}=\mathfrak{P}^m\,.$$

Then $\mathfrak{D}_F$ is divisible by $\mathfrak{p}^k$, since k is even; $\mathfrak{D}_{K/F}$ is divisible by $\mathfrak{P}^{m-1}$. Since

$$\mathfrak{D}_K=\mathfrak{D}_F\mathfrak{D}_{K/F}\,,$$

$\mathfrak{D}_K$ is divisible by

$$\mathfrak{p}^k\mathfrak{P}^{m-1}=\mathfrak{P}^{mk+m-1}=\mathfrak{P}^{n+m-1}\,.$$

Hence d is divisible by 2^{n+m-1}. This is a contradiction, since

$$n+m-1 \geq n+2-1=n+1\,.$$

Hence G is primitive ([9], Theorem 7.4).

We have already proved that G contains a transposition. Hence $G=S_n$ ([9], Theorem 13.3).

§4. Examples.

THEOREM 2. *Let n, a, b be integers which satisfy the following conditions*:

(i) $n>1$;

(ii) $(a, n)=1$;

(iii) *b is odd*, $(b, n-1)=1$, $(a, b)=1$.

Then the equation

$$x^n+2ax+2b=0$$

is affect-free.

PROOF. Let α be a root of

$$f(x)=x^n+2ax+2b=0\,,$$

and let $K=Q(\alpha)$. Since b is odd, $f(x)$ is irreducible. It is easily seen that 2 is completely ramified in K ([3], Lemma 4). Now let

$$\delta=f'(\alpha)\,,\quad D=\operatorname{norm}\delta\,,\quad D/\delta=x_0+x_1\alpha+\cdots+x_{n-1}\alpha^{n-1}\,.$$

Then ([2], Theorem 2)

$$D=(-1)^{n-1}(n-1)^{n-1}(2a)^n+n^n(2b)^{n-1}=2^{n-1}D_0\,, \tag{4.1}$$

where

$$D_0=(-1)^{n-1}2(n-1)^{n-1}a^n+n^nb^{n-1}\,.$$

If n is odd, D_0 is odd; if n is even, $D_0/2$ is odd. Hence D is not divisible by 2^{n+1}. Now let p be a prime factor of $(D, x_0, \cdots, x_{n-1})$. Then $p|x_0$, and so $p|2(n-1)a$ ([2], Theorem 2). Since $p|D$, by (4.1) we see that $p|2nb$. Hence $p=2$. Therefore $(D, x_0, \cdots, x_{n-1})$ is a power of 2. Hence the result follows from Theorem 1.

THEOREM 3. *The following equations are all affect-free for every $n>1$*:

$$x^n+2x+2=0\,,\qquad x^n+2x-2=0\,,$$

$$x^n-2x+2=0\,,\qquad x^n-2x-2=0\,.$$

PROOF. The result follows immediately from Theorem 2.

§5. Notation and terminology.

As usual, $\boldsymbol{Q}$ denotes the field of rational numbers. An *affect-free equation* means an equation $f(x)=0$ with the following properties: (i) $f(x)$ is an irreducible polynomial of degree n with rational coefficients; (ii) the Galois group of $f(x)=0$ over $\boldsymbol{Q}$ is isomorphic to the symmetric group S_n. An *integer* always means a rational integer. A prime number p is said to be *completely ramified* in an algebraic number field K of degree n, if $p=\mathfrak{p}^n$ with a prime ideal $\mathfrak{p}$ in K.

References

[1] D. Hilbert, Die Theorie der algebraischen Zahlkörper, Jahrsber. Deutsch. Math.-Verein., **4** (1897), 175–546.

[2] K. Komatsu, Integral bases in algebraic number fields, J. Reine Angew. Math., **278/279** (1975), 137–144.

[3] K. Komatsu, Discriminants of certain algebraic number fields, J. Reine Angew. Math., **285** (1976), 114–125.

[4] K. Komatsu, Square-free discriminants and affect-free equations, Tokyo J. Math., **14** (1991), 57–60.

[5] I. Schur, Gleichungen ohne Affekt, Sitzungsber. Berlin. Akad., (1930), 443–449.

[6] I. Schur, Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome, J. Reine Angew. Math., **165** (1931), 52–58.

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

[8] B. L. van der Waerden, Die Zerlegungs- und Trägheitsgruppe als Permutationsgruppen, Math. Ann., **111** (1935), 731–733.

[9] H. Wielandt, *Finite Permutation Groups*, Academic Press, 1964.

Present Address:
Department of Mathematics, Faculty of Science and Technology, Keio University
Hiyoshi, Kohoku-ku, Yokohama 223, Japan