TOKYO J. MATH.
VOL. 14, NO. 1, 1991

Square-Free Discriminants and Affect-Free Equations

Kenzo KOMATSU

Keio University

§1. Square-free discriminants.

Unramified A_n-extensions of quadratic number fields are discussed by Uchida [5], [6] and Yamamoto [10]. Their results are closely related to the fact that there are infinitely many algebraic number fields K of degree n $(n>1)$ with the following properties:

1. The Galois group of $\bar{K}/\boldsymbol{Q}$ is the symmetric group S_n, where $\bar{K}$ denotes the Galois closure of $K/\boldsymbol{Q}$.
2. The discriminant of K is square-free.

It is the purpose of the present paper to discuss square-free discriminants and affect-free (affektlos) equations. We begin by proving the following theorem. The Galois closure of $K/\boldsymbol{Q}$ means the minimal Galois extension of $\boldsymbol{Q}$ which contains K.

THEOREM 1. *Let K denote an algebraic number field of degree n $(n\geq 1)$ and let $\bar{K}$ denote the Galois closure of $K/\boldsymbol{Q}$. Suppose that the discriminant d of K is square-free. Then we have*:

1. *The Galois group of $\bar{K}/\boldsymbol{Q}$ is the symmetric group S_n.*
2. *The Galois group of $\bar{K}/\boldsymbol{Q}(\sqrt{d})$ is the alternating group A_n.*
3. *Every prime ideal is unramified in $\bar{K}/\boldsymbol{Q}(\sqrt{d})$.*

PROOF. We may assume that $n>1$. Let G denote the Galois group of $\bar{K}/\boldsymbol{Q}$. Then G is a transitive permutation group on $\{1, 2, \cdots, n\}$. 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 d_F denote the discriminant of F. Then d is divisible by d_F^m, where $m=[K:F]$ ([1], Satz 39). Since $m>1$, by Minkowski's theorem we see that d cannot be square-free. This implies that G is primitive ([9], Theorem 7.4). Let p denote a prime number which divides d; by hypothesis d is exactly divisible by p. Then (van der Waerden [7]) the prime ideal decomposition of p (in K) is of the form

Received April 24, 1990

$$p=\mathfrak{p}_0^2\mathfrak{p}_1\cdots\mathfrak{p}_s\,,\quad N(\mathfrak{p}_0)=p\,.$$

Let $\mathfrak{P}$ be a prime ideal in $\bar{K}$ which divides p. Then the inertia group of $\mathfrak{P}$ contains a transposition ([7], Satz I). Hence $G=S_n$ ([9], Theorem 13.3). Since the ramification index of $\mathfrak{P}$ with respect to $\bar{K}/Q$ is equal to 2 ([7], Satz I), $\mathfrak{P}$ is unramified in $\bar{K}/Q(\sqrt{d})$. Every prime number which ramifies in $\bar{K}$ also ramifies in K ([7]). This proves the assertion (3). The assertion (2) follows from the fact that $Q(\sqrt{d})$ is the fixed field of A_n.

From Theorem 1 and a result of [2] we obtain the following theorem.

THEOREM 2. *Let $a_0, a_1, \cdots, a_{n-1}$ $(n>1)$ be rational integers such that*

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

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

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

Suppose that

$$(D, x_0, x_1, \cdots, x_{n-1})=1\,.$$

Then the discriminant of $Q(\alpha)$ is square-free, and the Galois group of $f(x)=0$ over Q is the symmetric group S_n.

PROOF. Every prime factor p of the discriminant d of $Q(\alpha)$ is also a prime factor of D. Therefore there exists a number i such that x_i is not divisible by p. By Theorem 1 of [2] we see that d is not divisible by p^2. Hence d is square-free, and the Galois group of $f(x)=0$ is S_n (Thoerem 1).

§2. Examples.

In [8] Wegner proved that the Galois group over Q of the equation

$$f(x)=x^p+ax+b=0$$

of prime degree $p>3$ is the symmetric group S_p if $f(x)$ is irreducible and if $(a, b)=(p, a)=(p-1, b)=1$. We generalize Wegner's result as follows:

THEOREM 3. *Let n $(n>1)$, a, b be rational integers such that $f(x)=x^n+ax+b$ is irreducible over Q. If $((n-1)a, nb)=1$, then the Galois group of $f(x)=0$ over Q is the symmetric group S_n, and the discriminant of $Q(\alpha)$ is square-free, where α denotes a root of $f(x)=0$.*

PROOF. The result follows immediately from Theorem 2 and [2] (Theorem 2).

Selmer [4] proved that x^n-x-1 is irreducible for every $n>1$. From Theorem 3 we obtain the following theorem.

THEOREM 4. *The Galois group of*

$$x^n - x - 1 = 0$$

over Q *is the symmetric group* S_n *for every* $n > 1$.

It follows from a theorem of Perron [3] that $x^n + ax + 1$ is irreducible if $n > 1$, $a \in Z$, $|a| \geq 3$ ([4], Theorem 2). Hence we have the following theorem.

THEOREM 5. *If* n $(n > 1)$ *and* a *are rational integers such that* $|a| \geq 3$, $(n, a) = 1$, *then the Galois group of*

$$x^n + ax + 1 = 0$$

over Q *is the symmetric group* S_n.

§3. Unramified A_n-extensions of quadratic number fields: An explicit construction.

Since $x^n + ax + 1$ is irreducible for $|a| \geq 3$, it is not difficult to construct (for any integer $n > 1$) infinitely many algebraic number fields of degree n with square-free discriminants (§1). It is also possible to give an explicit construction of infinitely many quadratic number fields which have unramified A_n-extensions (cf. [6], Theorem 2): Let n $(n > 1)$ be a fixed integer. Define a_k, D_k $(k = 1, 2, \cdots)$ by

$$a_1 = n + 1\,, \qquad D_1 = (-1)^{n-1}(n-1)^{n-1}a_1^n + n^n\,,$$

$$a_k = D_1 D_2 \cdots D_{k-1}\,, \qquad D_k = (-1)^{n-1}(n-1)^{n-1}a_k^n + n^n\,.$$

Let $f_k(x) = x^n + a_k x + 1$, and let α_k be a root of $f_k(x) = 0$; let d_k denote the discriminant of the field $A_k = Q(\alpha_k)$, and let $\bar{A}_k$ denote the Galois closure of A_k over Q; let $F_k = Q(\sqrt{d_k})$. Then $f_1(x)$ is irreducible, since $|a_1| \geq 3$; D_1 is divisible by d_1, and so $|D_1| \geq |d_1| \geq 3$. By induction, we see that (for every k) $|a_k| \geq 3$, $f_k(x)$ is irreducible, and $(n, a_k) = (n, D_k) = 1$. Since D_k is the norm of $f'_k(\alpha_k)$ ([2], Theorem 2), we have $F_k = Q(\sqrt{(-1)^{n(n-1)/2}D_k})$. Clearly $i < j$ implies $(D_i, D_j) = 1$, $(d_i, d_j) = 1$, and so $A_i \neq A_j$, $F_i \neq F_j$. Since $(n, a_k) = 1$, d_k is square-free (Theorem 3). Therefore, for every k, the Galois group of $\bar{A}_k/Q$ (resp. $\bar{A}_k/F_k$) is the symmetric (resp. alternating) group of degree n, and no prime ideals are ramified in $\bar{A}_k/F_k$ (Theorem 1).

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] O. PERRON, Neue Kriterien für die Irreduzibilität algebraischer Gleichungen, J. Reine Angew. Math., **132** (1907), 288–307.

[4] E. S. SELMER, On the irreducibility of certain trinomials, Math. Scand., **4** (1956), 287–302.
[5] K. UCHIDA, Unramified extensions of quadratic number fields, I, Tôhoku Math. J., **22** (1970), 138–141.
[6] K. UCHIDA, Unramified extensions of quadratic number fields, II, Tôhoku Math. J., **22** (1970), 220–224.
[7] B. L. VAN DER WAERDEN, Die Zerlegungs- und Trägheitsgruppe als Permutationsgruppen, Math. Ann., **111** (1935), 731–733.
[8] U. WEGNER, Über trinomische Gleichungen von Primzahlgrad, Math. Ann., **111** (1935), 734–737.
[9] H. WIELANDT, Finite permutation groups, Academic Press, 1964.
[10] Y. YAMAMOTO, On unramified Galois extensions of quadratic number fields, Osaka J. Math., **7** (1970), 57–76.

Present Address:
DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCE AND TECHNOLOGY, KEIO UNIVERSITY
HIYOSHI, KOHOKU-KU, YOKOHAMA 223, JAPAN