Title	On discriminants and Galois groups
Sub Title	
Author	Komatsu, Kenzo
Publisher	慶應義塾大学理工学部
Publication year	1992
Jtitle	Keio Science and Technology Reports Vol.45, No.2 (1992. 3) ,p.23- 27
JaLC DOI	
Abstract	
Notes	
Genre	Departmental Bulletin Paper
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO50001004-00450002-0023

KEIO SCIENCE AND TECHNOLOGY REPORTS
VOL 45, NO. 2, pp. 23-27, 1992, ISSN: 02864215

ON DISCRIMINANTS AND GALOIS GROUPS

by

Kenzo KOMATSU

Department of Mathematics
Faculty of Science and Technology, Keio University
Hiyoshi, Yokohama 223, Japan

(Received March 27, 1992)

§ 1. Introduction

Let $a_1, a_2, \ldots, a_n$ $(n>1)$ be rational integers such that

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

is irreducible over the rational number field $\boldsymbol{Q}$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ denote the roots of $f(x)=0$. Then the Galois group G of $f(x)=0$ over $\boldsymbol{Q}$ is a transitive permutation group on the set $\{1, 2, \ldots, n\}$. We denote by $D(f)$ the discriminant of $f(x)=0$:

$$D(f)=\prod_{i<j}(\alpha_i-\alpha_j)^2=\begin{vmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ & & \cdots & \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{vmatrix}^2 . \tag{1.1}$$

The discriminant $D(f)$ is a rational integer. The following result is well-known: *The Galois group G contains an odd permutation if and only if $D(f)$ is not a square.*

In the present paper we discuss a certain factorization (§ 2) of the discriminant $D(f)$ (cf. [7]):

$$D(f)=\pm D^{(1)}D^{(2)} . \tag{1.2}$$

Both $D^{(1)}$ and $D^{(2)}$ have some interesting properties. For example: If $D^{(2)}$ is not a square, G contains a transposition (Theorem 2). If $D^{(1)}=2^t$ $(0\leq t\leq n-1)$, then G is the symmetric group S_n (Theorem 6). We shall state our theorems in § 2, prove them in § 3, and give some examples in § 4.

§ 2. Main results

Let $a_1, a_2, \ldots, a_n$ $(n>1)$ be rational integers such that

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

is irreducible over $\boldsymbol{Q}$, and let $\alpha_1, \alpha_2, \dots, \alpha_n$ be the roots of $f(x)=0$. Let G denote the Galois group of $f(x)=0$ over $\boldsymbol{Q}$; G is regarded as a transitive permutation group on the set $\{1, 2, \dots, n\}$. For any $\xi \in \boldsymbol{Q}(\alpha_1)$, let $N(\xi)$ denote its norm in $\boldsymbol{Q}(\alpha_1)$. Now let

$$\delta = f'(\alpha_1)\,, \qquad D = N(\delta)\,,$$

$$\frac{D}{\delta} = x_0 + x_1\alpha_1 + \cdots + x_{n-1}\alpha_1^{n-1}\,, \quad x_i \in \boldsymbol{Z}\,, \tag{2.1}$$

where $\boldsymbol{Z}$ denotes the ring of rational integers ([2], Theorem 1). Let D^* denote the greatest common divisor of $x_0, x_1, \cdots, x_{n-1}$:

$$D^* = (x_0, x_1, \dots, x_{n-1})\,. \tag{2.2}$$

For any prime number p and any $A \in \boldsymbol{Z}$, let A_p denote the largest integer M such that A is divisible by p^M. Define $D^{(1)}$ and $D^{(2)}$ by

$$D^{(1)} = \prod_{p \mid D^*} p^{D_p}\,, \qquad D^{(2)} = \frac{|D|}{D^{(1)}}\,. \tag{2.3}$$

Then, clearly,

$$|D(f)| = |D| = D^{(1)}D^{(2)}\,, \qquad (D^{(1)}, D^{(2)}) = 1\,, \qquad D^{(1)} > 0\,, \qquad D^{(2)} > 0\,, \tag{2.4}$$

where $D(f)$ denotes the discriminant (§ 1) of $f(x)=0$. We call $D^{(1)}$ (resp. $D^{(2)}$) *the first* (resp. *second*) *factor of the discriminant of* $f(x)=0$. Both $D^{(1)}$ and $D^{(2)}$ are independent of the choice of α_1. Finally, let d denote the discriminant of $\boldsymbol{Q}(\alpha_1)$.

Then we have

Theorem 1. *For any prime factor p of $D^{(2)}$,*

$$d_p = \begin{cases} 1 & \text{when } (D^{(2)})_p \text{ is odd}\,, \\ 0 & \text{when } (D^{(2)})_p \text{ is even}\,. \end{cases}$$

Theorem 2. *If $D^{(2)}$ is not a square, G contains a transposition.*

Theorem 3. *If $D^{(2)}$ is a square, then $(d, D^{(2)})=1$ and $d \mid D^{(1)}$.*

Theorem 4. *If F is a proper subfield of $\boldsymbol{Q}(\alpha_1)$, then the discriminant d_F of F satisfies*

$$(d_F, D^{(2)}) = 1\,, \qquad d_F^m \mid D^{(1)}\,,$$

where $m = [\boldsymbol{Q}(\alpha_1) : F]$.

Theorem 5. *If $D^{(2)}$ is not a square and if $\boldsymbol{Q}$ is the only proper subfield of $\boldsymbol{Q}(\alpha_1)$, then G is the symmetric group S_n.*

Theorem 6. *If $D^{(1)} = 2^t$ $(0 \le t \le n-1)$, then $G = S_n$.*

Theorem 7. *Suppose that the following three conditions are satisfied:*

1. *$n = l$ is an odd prime;*

2. $(l, D^{(1)})=1$;

3. *every prime factor of* $D^{(1)}$ *is either completely ramified or unramified in* $\boldsymbol{Q}(\alpha_1)/\boldsymbol{Q}$.

Then $G=S_l$ *if and only if* $D^{(2)}$ *is not a square. If* $D^{(2)}$ *is a square, then* G *is a simple group, and every prime ideal is unramified in* $\boldsymbol{Q}(\alpha_1, \ldots, \alpha_l)/\boldsymbol{Q}(\alpha_1)$.

§ 3. Proof

1. Theorem 1 follows from the definition of $D^{(2)}$ and [2] (Theorem 1). Since $D^{(2)}>0$, $D^{(2)}$ is a square if and only if $(D^{(2)})_p$ is even for every prime number p. Hence, if $D^{(2)}$ is not a square, then $d_p=1$ for some p (Theorem 1). Therefore Theorem 2 follows from van der Waerden's theorem [8] (cf. [7], Theorem 1). Since $D(f)$ is divisible by d, Theorem 3 follows from Theorem 1 and (2.4).

2. Let F be a proper subfield of $\boldsymbol{Q}(\alpha_1)$. Then

$$m=[\boldsymbol{Q}(\alpha_1):\ F]>1\ . \tag{3.1}$$

It is well-known ([1], Satz 39) that d is divisible by d_F^m. Hence, Theorem 4 follows from Theorem 1, (3.1) and (2.4). Theorem 5 follows from Theorem 2, since the Galois group G is primitive if and only if $\boldsymbol{Q}$ is the only proper subfield of $\boldsymbol{Q}(\alpha_1)$ ([9], Theorem 7.4 and Theorem 13.3).

3. Now we prove Theorem 6. Suppose that $D^{(1)}=2^t$, where $0\leq t\leq n-1$. Then $D^{(2)}$ is not a square. In fact, if $D^{(2)}$ is a square, then from Theorem 3 we obtain

$$|d|\leq D^{(1)}\leq 2^{n-1}\ .$$

On the other hand, we have $|d|>2^{n-1}$ ([6], Lemma 1). A contradiction proves that $D^{(2)}$ is not a square. Hence G contains a transposition (Theorem 2). Now we prove that G is primitive. Suppose that $\boldsymbol{Q}(\alpha_1)$ has a subfield F such that

$$\boldsymbol{Q}\subset F\subset \boldsymbol{Q}(\alpha_1)\ ,\qquad F\neq \boldsymbol{Q}\ ,\qquad F\neq \boldsymbol{Q}(\alpha_1)\ .$$

Let d_F denote the discriminant of F, and let

$$m=[\boldsymbol{Q}(\alpha_1):\ F]\ ,\qquad k=[F:\ \boldsymbol{Q}]\ .$$

Since $D^{(1)}$ is a power of 2, it follows from Theorem 4 that $|d_F|$ is also a power of 2: $|d_F|=2^s$. Since $k>1$, we obtain $s\geq k$ ([6], Lemma 1). Theorem 4 implies that $D^{(1)}$ is divisible by $2^{km}=2^n$. A contradiction shows that G is primitive ([9], Theorem 7.4). Hence $G=S_n$ ([9], Theorem 13.3).

4. Now we prove Theorem 7. Suppose that the conditions of Theorem 7 are satisfied. Since l is a prime, $G=S_l$ if $D^{(2)}$ is not a square (Theorem 5). Suppose that $D^{(2)}$ is a square. Then, by Theorem 3, $(d, D^{(2)})=1$ and $d|D^{(1)}$. Hence $(l, d)=1$, and every prime factor of d is completely ramified in $\boldsymbol{Q}(\alpha_1)/\boldsymbol{Q}$. It follows from Theorem 4 of [3] that every prime ideal is unramified in $\boldsymbol{Q}(\alpha_1, \ldots, \alpha_l)/\boldsymbol{Q}(\alpha_1)$, and G is a simple group. Since $l>2$, $G\neq S_l$. This completes the proof.

§ 4. Examples

1. Suppose that

$$f(x)=x^n+Ax+B \quad (A, B\in \boldsymbol{Z},\ n>2)$$

is irreducible. Then ([2], Theorem 2)

$$x_0=(-1)^{n-1}(n-1)^{n-1}A^{n-1}\ ,$$
$$x_i=(-1)^i(n-1)^{i-1}n^{n-i}A^{i-1}B^{n-1-i} \quad (1\le i\le n-1)\ .$$

For every prime number p, we obtain

$$p|D^* \Leftrightarrow p|((n-1)A, nB)\ , \tag{4.1}$$

since $n>2$. Hence the first factor of the discriminant of $f(x)=0$ is given by

$$D^{(1)}=\prod_{p|((n-1)A,nB)} p^{D_p}\ . \tag{4.2}$$

In particular, if $((n-1)A, nB)=1$, then $D^{(1)}=1$, and so $G=S_n$ (Theorem 6). See [4], Theorem 3.

Another special case is treated in [5]:

$$n=l\ , \qquad A=B=a\ ,$$

where l ($l>3$) is a prime number such that $(l, a)=1$. We have ([2], Theorem 2)

$$D=a^{l-1}\{(l-1)^{l-1}a+l^l\}\ .$$

From (4.2) we obtain

$$D^{(1)}=a^{l-1}\ , \qquad D^{(2)}=|(l-1)^{l-1}a+l^l|\ .$$

Every prime factor of a is either completely ramified or unramified in $\boldsymbol{Q}(\alpha_1)$ ([3], p. 125). Since $(l, D^{(1)})=1$, it follows from Theorem 7 that $G=S_l$ if and only if $D^{(2)}$ is not a square. If $D^{(2)}$ is a square, then G is a simple group, and every prime ideal is unramified in $\boldsymbol{Q}(\alpha_1, \dots, \alpha_l)/\boldsymbol{Q}(\alpha_1)$. See [5], Theorem 1 and Theorem 2.

2. Consider now the case

$$f(x)=x^n-x^{n-1}-\cdots-x-1\ ,$$

which we discussed in [6]. We see that D^* is a power of 2 ([6], § 5). If n is even, then D is odd, and so $D^{(1)}=1$. Suppose that n is odd. Then D is exactly divisible by 2^{n-1} ([6], Lemma 2), and so $D^{(1)}=2^{n-1}$ or 1. In any case we have $D^{(1)}=2^t$, where $t=0$ or $t=n-1$. Hence $G=S_n$ (Theorem 6).

3. The converse of Theorem 2 is false. A simple example is

$$f(x)=x^3-5\cdot 34x-5^2\cdot 34\ .$$

The discriminant of $f(x)=0$ is

$$D(f)=-4(-5\cdot 34)^3-27(-5^2\cdot 34)^2$$
$$=5^3\cdot 34^2=2^2 5^3 17^2 .$$

From (4.2) we obtain

$$D^{(1)}=D(f)\,, \qquad D^{(2)}=1\,.$$

Since $D(f)$ is not a square, we have $G=S_3$. Therefore G contains a transposition, but $D^{(2)}=1^2$ is a square.

References

[1] D. Hilbert, Die Theorie der algebraischen Zahlkörper, Jahresber. 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] K. Komatsu, On the Galois group of $x^p+ax+a=0$, Tokyo J. Math., **14** (1991), 227–229.
[6] K. Komatsu, On the Galois group of $x^n-x^{n-1}-x^{n-2}-\cdots-x-1=0$, Keio Science and Technology Reports, **44** (1991), 1–6.
[7] K. Komatsu, On the Galois group of $x^p+p^t b(x+1)=0$, to appear.
[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.