Title	On discriminants and certain matrices
Sub Title	
Author	Komatsu, Kenzo
Publisher	慶應義塾大学理工学部
Publication year	1996
Jtitle	Keio Science and Technology Reports Vol.49, No.1 (1996.) ,p.1- 11
JaLC DOI	
Abstract	
Notes	
Genre	Departmental Bulletin Paper
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO50001004-00490001-0001

KEIO SCIENCE AND TECHNOLOGY REPORTS
VOL. 49, NO. 1, pp. 1–11

ON DISCRIMINANTS AND CERTAIN MATRICES

by

Kenzo KOMATSU

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

(Received February 28, 1996)

0. Introduction

Let K be an algebraic number field of degree $n > 1$, and let α be an integer of K. In this paper we discuss the $n \times n$ matrix $C(\alpha) = (\ Tr\ (\alpha^{(i-1)+(j-1)})\ )$ and its minors. Certain minors of $C(\alpha)$ are closely related to the ramification of primes in $K/\boldsymbol{Q}$. For example: If the greatest common divisor of all the minors of order $(n-1)$ of the matrix $C(\alpha)$ is equal to 1, then the discriminant of K is square-free, and K has a very simple and explicit integral basis (§4). Therefore it seems important to study $C(\alpha)$ and its minors in relation to the discriminant and the ring of integers of K. In this paper we prove two theorems on the minors of order $(n-1)$, together with a few elementary results on the minors of order $i \leq n-1$.

1. The matrix $C(\alpha)$ and its minors of order $n-1$.

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

Theorem 1. *Let K be an algebraic number field of degree $n > 1$. Let p be a prime number, and let $k \in \boldsymbol{Z}$, $k > 0$. Suppose that the discriminant of K is divisible by p^{2k}. Then, for any integer α of K, every minor of order $(n-1)$ of the $n \times n$ matrix*

$$C(\alpha) = \begin{pmatrix} Tr(1) & Tr(\alpha) & \dots & Tr(\alpha^{n-1}) \\ Tr(\alpha) & Tr(\alpha^2) & \dots & Tr(\alpha^n) \\ & & \dots & \\ Tr(\alpha^{n-1}) & Tr(\alpha^n) & \dots & Tr(\alpha^{2n-2}) \end{pmatrix}$$

is divisible by p^k, where $Tr(\xi)$ means the trace of ξ in $K/\boldsymbol{Q}$.

Proof. Let $\alpha^{(1)}, \cdots, \alpha^{(n)}$ denote the conjugates of α in $K/\boldsymbol{Q}$. Then

(1.1)

$$C(\alpha) = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha^{(1)} & \alpha^{(2)} & \dots & \alpha^{(n)} \\ & & \dots & \\ \alpha^{(1)n-1} & \alpha^{(2)n-1} & \dots & \alpha^{(n)n-1} \end{pmatrix} \begin{pmatrix} 1 & \alpha^{(1)} & \dots & \alpha^{(1)n-1} \\ 1 & \alpha^{(2)} & \dots & \alpha^{(2)n-1} \\ & & \dots & \\ 1 & \alpha^{(n)} & \dots & \alpha^{(n)n-1} \end{pmatrix}.$$

Suppose first that $K \neq \boldsymbol{Q}(\alpha)$. If $n > 2$, then

$$\text{rank}\begin{pmatrix} 1 & \alpha^{(1)} & \dots & \alpha^{(1)n-1} \\ & & \dots & \\ 1 & \alpha^{(n)} & \dots & \alpha^{(n)n-1} \end{pmatrix} \leq \frac{n}{2} < n-1. \tag{1.2}$$

By (1.1) we see that $\text{rank}C(\alpha) < n-1$; every minor of order $(n-1)$ is equal to 0. If $n = 2$, then $\alpha \in \boldsymbol{Z}$, $k = 1$ and $p = 2$; every entry of the matrix $C(\alpha)$ is divisible by $p^k = 2$. In any case, every minor of order $n-1$ of the matrix $C(\alpha)$ is divisible by p^k.

From now on, we assume that $K = \boldsymbol{Q}(\alpha)$. Let

$$\begin{aligned} f(x) &= (x-\alpha^{(1)})(x-\alpha^{(2)})\cdots(x-\alpha^{(n)}) \\ &= x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n. \end{aligned} \tag{1.3}$$

Then the coefficients a_i are rational integers, and $f(x)$ is irreducible over $\boldsymbol{Q}$.

$K = \boldsymbol{Q}(\alpha)$ is a vector space over $\boldsymbol{Q}$. We fix its basis:$1, \alpha, \ldots, \alpha^{n-1}$. An element $\xi = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} (c_i \in \boldsymbol{Q})$ of K is then represented by a column vector $(c_0, \ldots, c_{n-1})^T$, where T denotes transposition. The linear transformation $\xi \longmapsto \alpha\xi$ is determined by the $n \times n$ matrix

$$A = (\boldsymbol{e}_2\boldsymbol{e}_3 \ldots \boldsymbol{e}_n\boldsymbol{a}_1), \tag{1.4}$$

where

$$\boldsymbol{a}_1 = (-a_n, -a_{n-1}, \ldots, -a_2, -a_1)^T; \tag{1.5}$$

$\boldsymbol{e}_j$ denotes the j-th column of the identity matrix I_n. We define $\boldsymbol{a}_2, \boldsymbol{a}_3, \ldots$ inductively:

$$\boldsymbol{a}_j = A\boldsymbol{a}_{j-1}, \tag{1.6}$$

where $j \geq 2$. Clearly,

$$\boldsymbol{a}_1 = A\boldsymbol{e}_n. \tag{1.7}$$

By induction on j, we see that

$$A^j = (\boldsymbol{e}_{j+1}\boldsymbol{e}_{j+2} \cdots \boldsymbol{e}_n\boldsymbol{a}_1 \cdots \boldsymbol{a}_j) \tag{1.8}$$

for $j = 1, 2, \ldots, n-1$.

Now let

$$g(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in \boldsymbol{Q}[x], \tag{1.9}$$

and let $\boldsymbol{g}_j$ denote the j-th column of the matrix $g(A)$:

$$g(A) = c_0I_n + c_1A + \cdots + c_{n-1}A^{n-1}, \tag{1.10}$$

$$g(A) = (\boldsymbol{g}_1\boldsymbol{g}_2 \cdots \boldsymbol{g}_n). \tag{1.11}$$

Then

$$\boldsymbol{g}_j = g(A)\boldsymbol{e}_j \tag{1.12}$$

for $j = 1, 2, \ldots, n$. The matrix $g(A)$ determines a linear transformation $\xi \longmapsto g(\alpha)\xi$. By (1.12) we see that the column vector $\boldsymbol{g}_j$ represents $g(\alpha)\alpha^{j-1}$ in K. Since

$$g(\alpha)\alpha^{j-1} = \alpha^{j-1}g(\alpha),$$

it follows from (1.9) that

$$\text{(1.13)} \qquad \boldsymbol{g}_j = A^{j-1}\begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix}$$

for $j = 1, 2, \ldots, n$. Hence

$$\text{(1.14)} \qquad \boldsymbol{g}_1 = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix}, \quad \boldsymbol{g}_j = A\boldsymbol{g}_{j-1},$$

where $2 \le j \le n$.

The eigenvalues of the matrix A are the conjugates of α in $K/\boldsymbol{Q}$; $f(x)$ is the minimum polynomial of the matrix A. For any $h(x) \in \boldsymbol{Q}[x]$, the element $h(\alpha)$ of the field K is represented by the matrix $h(A)$:

$$\text{(1.15)} \qquad h(\alpha) \longleftrightarrow h(A).$$

The norm $N(h(\alpha))$ of $h(\alpha)$ in $K/\boldsymbol{Q}$ is equal to the determinant of $h(A)$:

$$\text{(1.16)} \qquad N(h(\alpha)) = \det h(A).$$

Now let $\boldsymbol{b}_j$ denote the j-th column of the matrix $B = f'(A)$:

$$\text{(1.17)} \qquad B = f'(A) = nA^{n-1} + (n-1)a_1A^{n-2} + \cdots + a_{n-1}I_n,$$

$$\text{(1.18)} \qquad B = (\boldsymbol{b}_1\boldsymbol{b}_2 \ldots \boldsymbol{b}_n).$$

Then it follows from (1.14) that

$$\text{(1.19)} \qquad \boldsymbol{b}_1 = \begin{pmatrix} a_{n-1} \\ 2a_{n-2} \\ \vdots \\ (n-1)a_1 \\ n \end{pmatrix}, \quad \boldsymbol{b}_j = A\boldsymbol{b}_{j-1},$$

where $2 \le j \le n$.

Let D denote the norm of $\delta = f'(\alpha)$ in $K/\boldsymbol{Q}$:

$$\text{(1.20)} \qquad \delta = f'(\alpha), \quad D = N(\delta).$$

Then (1.16) gives

$$\text{(1.21)} \qquad D = \det B.$$

For $j = 1, 2, \ldots, n$, let

$$\alpha^{j-1}\delta = r_{1j} + r_{2j}\alpha + \cdots + r_{nj}\alpha^{n-1}, \tag{1.22}$$

where $r_{ij} \in \boldsymbol{Z}$. Then it follows from (1.15), (1.20) and (1.17) that

$$A^{j-1}B = r_{1j}I_n + r_{2j}A + \cdots + r_{nj}A^{n-1} \tag{1.23}$$

for $j = 1, 2, \cdots, n$. By (1.19) we see that the first column of $A^{j-1}B$ is $A^{j-1}\boldsymbol{b}_1 = \boldsymbol{b}_j$. Hence, by (1.14),

$$\boldsymbol{b}_j = (r_{1j}, r_{2j}, \ldots, r_{nj})^T. \tag{1.24}$$

Now let b_{ij} denote the (i, j)-entry of the matrix B:

$$B = \begin{pmatrix} b_{11} & \ldots & b_{1n} \\ & \ldots & \\ b_{n1} & \ldots & b_{nn} \end{pmatrix}. \tag{1.25}$$

By (1.22) and (1.24) we see that

$$\alpha^{j-1}\delta = b_{1j} + b_{2j}\alpha + \cdots + b_{nj}\alpha^{n-1} \tag{1.26}$$

for $j = 1, 2, \ldots, n$. Let $\tilde{b}_{ij}$ denote the cofactor of the (i, j)-entry b_{ij}, and let

$$\alpha^{j-1}\frac{D}{\delta} = s_{1j} + s_{2j}\alpha + \cdots + s_{nj}\alpha^{n-1}, \tag{1.27}$$

where $s_{ij} \in \boldsymbol{Z}$, $1 \leq j \leq n$. From (1.15), (1.17), (1.20) and (1.21), we obtain

$$(\det B)B^{-1}A^{j-1} = s_{1j}I_n + s_{2j}A + \cdots + s_{nj}A^{n-1}. \tag{1.28}$$

By (1.8) we see that the first column of the matrix A^{j-1} is $\boldsymbol{e}_j$. From (1.14) we obtain

$$\begin{aligned} (s_{1j}, \ldots, s_{nj})^T &= (\det B)B^{-1}\boldsymbol{e}_j \\ &= (\tilde{b}_{j1}, \ldots, \tilde{b}_{jn})^T. \end{aligned}$$

Hence (1.27) becomes

$$\alpha^{j-1}\frac{D}{\delta} = \tilde{b}_{j1} + \tilde{b}_{j2}\alpha + \cdots + \tilde{b}_{jn}\alpha^{n-1} \tag{1.29}$$

for $j = 1, 2, \ldots, n$. In particular,

$$\frac{D}{\delta} = \tilde{b}_{11} + \tilde{b}_{12}\alpha + \cdots + \tilde{b}_{1n}\alpha^{n-1}. \tag{1.30}$$

It follows from (1.29) and (1.30) that every cofactor $\tilde{b}_{ij}$ is divisible by the greatest common divisor of $\tilde{b}_{11}, \ldots, \tilde{b}_{1n}$:

$$(\tilde{b}_{11}, \tilde{b}_{12}, \ldots, \tilde{b}_{1n}) \mid \tilde{b}_{ij}, \tag{1.31}$$

where $1 \le i \le n$, $1 \le j \le n$.

Clearly, the column vector

$$\boldsymbol{x} = (1, \alpha, \ldots, \alpha^{n-1})^T \tag{1.32}$$

is an eigenvector of the matrix A^T corresponding to the eigenvalue α:

$$A^T\boldsymbol{x} = \alpha\boldsymbol{x}, \quad \boldsymbol{x} \ne \mathbf{o}. \tag{1.33}$$

It is easily seen that an eigenvector of the matrix A corresponding to the eigenvalue α is given by $M\boldsymbol{x}$:

$$A(M\boldsymbol{x}) = \alpha M\boldsymbol{x}, \tag{1.34}$$

where

$$M = \begin{pmatrix} a_{n-1} & a_{n-2} & \ldots & a_1 & 1 \\ a_{n-2} & a_{n-3} & \ldots & 1 & \\ \vdots & \vdots & \unicode{x22F0} & & \\ a_1 & 1 & & 0 & \\ 1 & & & & \end{pmatrix}. \tag{1.35}$$

Since $1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent over $\boldsymbol{Q}$, it follows from (1.33) and (1.34) that

$$AM = MA^T. \tag{1.36}$$

Hence

$$A^jM = M(A^T)^j \tag{1.37}$$

for every $j \in \boldsymbol{Z}$.

Let $\boldsymbol{c}_j$ denote the j-th column of the matrix $C(\alpha)$:

$$C(\alpha) = (\boldsymbol{c}_1\boldsymbol{c}_2 \ldots \boldsymbol{c}_n). \tag{1.38}$$

By definition,

$$\boldsymbol{c}_j = (Tr(\alpha^{j-1}), Tr(\alpha^j), \ldots, Tr(\alpha^{j+n-2}))^T. \tag{1.39}$$

From (1.32), (1.33) and (1.39), we obtain

$$\boldsymbol{c}_j = A^T\boldsymbol{c}_{j-1} \tag{1.40}$$

for $j = 2, 3, \ldots, n$. From (1.19),

$$\boldsymbol{b}_2 = \begin{pmatrix} -na_n \\ -(n-1)a_{n-1} \\ \vdots \\ -2a_2 \\ -a_1 \end{pmatrix}. \tag{1.41}$$

Newton's formula gives

$$M\boldsymbol{c}_2 = \boldsymbol{b}_2. \tag{1.42}$$

From (1.19), (1.37), (1.40) and (1.42), we obtain the following formula (cf. [2], §10):

$$B = MC(\alpha). \tag{1.43}$$

Let m^2 ($m \in \boldsymbol{Z}$) denote the largest square dividing D. Then

$$\frac{D}{m\delta} \in O_K, \tag{1.44}$$

where O_K denotes the ring of integers of K ([4], Theorem 1). Let t denote the index of α:

$$t = (O_K : \boldsymbol{Z}[\alpha]). \tag{1.45}$$

Then

$$(-1)^{\frac{n(n-1)}{2}} D = d_K t^2, \tag{1.46}$$

where d_K denotes the discriminant of K. It follows from (1.30), (1.44) and (1.45) that

$$\frac{t\tilde{b}_{1j}}{m} \in \boldsymbol{Z} \tag{1.47}$$

for $j = 1, 2, \ldots, n$. By (1.46) we see that

$$\frac{D\tilde{b}_{1j}^{\ 2}}{m^2 d_K} \in \boldsymbol{Z} \tag{1.48}$$

for $j = 1, 2, \ldots, n$. By hypothesis d_K is divisible by p^{2k}. Since D/m^2 is a square-free integer, $\tilde{b}_{1j}$ is divisible by p^k. From (1.31) we obtain

$$p^k \mid \tilde{b}_{ij} \tag{1.49}$$

for all i, j ($1 \leq i \leq n, 1 \leq j \leq n$).

By (1.35) we see that every entry of the inverse matrix of M is a rational integer:

$$M^{-1} \in M_n(\boldsymbol{Z}). \tag{1.50}$$

From (1.43),

$$C(\alpha) = M^{-1}B. \tag{1.51}$$

Hence the adjugate of $C(\alpha)$ satisfies

$$\mathrm{adj}C(\alpha) = \mathrm{adj}B \ \ \mathrm{adj}(M^{-1}). \tag{1.52}$$

It follows from (1.49), (1.50) and (1.52) that the entries of the matrix $\mathrm{adj}C(\alpha)$ are all divisible by p^k. Q.E.D.

Remark. It follows from (1.1) that, for any integer α of K, $\det C(\alpha)$ is equal to the discriminant of α in $K/\boldsymbol{Q}$, which is divisible by every prime factor p of the discriminant d_K of K. However, if d_K is not divisible by p^2, K may have an integer

α such that at least one minor of order $n-1$ of the matrix $C(\alpha)$ is not divisible by p. A simple example is

(1.53) $$K = \boldsymbol{Q}(\alpha), \quad \alpha^2 - p = 0,$$

where p is an odd prime. The matrix

(1.54) $$C(\alpha) = \begin{pmatrix} 2 & 0 \\ 0 & 2p \end{pmatrix}$$

has four minors of order one. One of them is not divisible by p, and the other three are all divisible by p.

2. The corner of order $n-1$.

In this section we prove a theorem on the corner of order $n-1$ (i.e. the cofactor of the (n,n)-entry) of the matrix $C(\alpha)$.

Theorem 2. *Let K be an algebraic number field of degree $n > 1$, and let α be an integer of K. Then for a prime number p to divide all the minors of order $n-1$ of the $n \times n$ matrix*

$$C(\alpha) = \begin{pmatrix} Tr(1) & Tr(\alpha) & \dots & Tr(\alpha^{n-1}) \\ Tr(\alpha) & Tr(\alpha^2) & \dots & Tr(\alpha^n) \\ & & \dots & \\ Tr(\alpha^{n-1}) & Tr(\alpha^n) & \dots & Tr(\alpha^{2n-2}) \end{pmatrix}$$

it is necessary and sufficient that the determinant of $C(\alpha)$ and its corner of order $n-1$ are both divisible by p.

To prove our theorem we require the following lemma.

Lemma 1. *Let F be a field, and let $S = (s_{ij})$ be a symmetric $n \times n$ matrix with (i,j)-entry $s_{ij} \in F$. Let $\tilde{s}_{ij}$ denote the cofactor of the entry s_{ij}. If $\det S = \tilde{s}_{nn} = 0$, then $\tilde{s}_{nj} = 0$ for $j = 1, 2, \dots, n$.*

Proof. By hypothesis,

(2.1) $$S\boldsymbol{v} = \mathbf{o},$$

where $\boldsymbol{v} = (\tilde{s}_{n1}, \tilde{s}_{n2}, \dots, \tilde{s}_{nn})^T$. For $j = 1, 2, \dots, n$, let S_j denote the $(n-1) \times (n-1)$ matrix obtained from S by deletion of the j-th row and the n-th column. Since $\tilde{s}_{nn} = 0$, it follows from (2.1) that

(2.2) $$S_j \boldsymbol{v}_0 = \mathbf{o}$$

for $j = 1, 2, \dots, n$, where

(2.3) $$\boldsymbol{v}_0 = (\tilde{s}_{n1}, \tilde{s}_{n2}, \dots, \tilde{s}_{n(n-1)})^T.$$

Suppose that $\tilde{s}_{nj} \neq 0$ for some $j < n$. Then $\boldsymbol{v}_0 \neq \mathbf{o}$, and so $\det S_j = 0$. This implies that $\tilde{s}_{jn} = \tilde{s}_{nj} = 0$, a contradiction. Hence $\tilde{s}_{nj} = 0$ for $j = 1, 2, \dots, n$.

Proof of Theorem. We may assume that $K = \boldsymbol{Q}(\alpha)$ (See the proof of Theorem 1).

Let $\tilde{c}_{ij}$ denote the cofactor of the (i,j)-entry c_{ij} of the matrix $C(\alpha)$. Let δ (resp. $d(\alpha)$) denote the different (resp. discriminant) of α in $K/\boldsymbol{Q}$. Then, from (1.30), (1.35) and (1.43),

$$\frac{d(\alpha)}{\delta} = \tilde{c}_{n1} + \tilde{c}_{n2}\alpha + \cdots + \tilde{c}_{nn}\alpha^{n-1}. \tag{2.4}$$

Let p denote a prime number such that $\det C(\alpha) \equiv \tilde{c}_{nn} \equiv 0 \pmod p$. Then Lemma 1 implies that $\tilde{c}_{nj} \equiv 0 \pmod p$ for $j = 1, 2, \ldots, n$. It follows from (1.31), (1.50) and (1.52) that $\tilde{c}_{ij} \equiv 0 \pmod p$ for all i, j.

3. Minors of order i.

In this section we discuss some elementary properties of the matrix $C(\alpha)$ and its minors.

Let K be an algebraic number field of degree $n > 1$, and let α be an integer of K. Let $i \in \boldsymbol{Z}$, $1 \le i \le n$. We denote by $\tilde{c}_i(\alpha)$ the greatest common divisor of all the minors of order i of the matrix $C(\alpha)$. Clearly, $\tilde{c}_i(\alpha)$ is divisible by $\tilde{c}_{i-1}(\alpha)$ for every $i > 1$.

Theorem 1 becomes

Theorem 1a. *Let $s^2 (s \in \boldsymbol{Z})$ denote the largest square dividing the discriminant of an algebraic number field K of degree $n > 1$. Then, for any integer α of K, $\tilde{c}_{n-1}(\alpha)$ is divisible by s.*

Now we have

Proposition 1. *Let O_K denote the ring of integers of an algebraic number field K of degree $n > 1$, and let $j \in \boldsymbol{Z}$, $1 \le j \le n-1$. Let $\alpha \in O_K$, and let $c_0, \ldots, c_{j-1}$, m_0 ($m_0 \ne 0$) be rational integers such that*

$$\frac{c_0 + c_1\alpha + \cdots + c_{j-1}\alpha^{j-1} + \alpha^j}{m_0} \in O_K. \tag{3.1}$$

Then $\tilde{c}_{j+1}(\alpha)$ is divisible by m_0.

Proof. Let $\boldsymbol{c}_k$ denote the k-th column of the matrix $C(\alpha)$:

$$\boldsymbol{c}_k = \begin{pmatrix} Tr(\alpha^{k-1}) \\ Tr(\alpha^k) \\ \vdots \\ Tr(\alpha^{k+n-2}) \end{pmatrix}. \tag{3.2}$$

By induction we see that

$$\alpha^{k-1} = s_{k0} + s_{k1}\alpha + \cdots + s_{k(j-1)}\alpha^{j-1} + m_0\xi_k \tag{3.3}$$

for $k = 1, 2, \ldots, n$, where $s_{kl} \in \boldsymbol{Z}$, $\xi_k \in O_K$. Hence

$$\boldsymbol{c}_k = s_{k0}\boldsymbol{c}_1 + s_{k1}\boldsymbol{c}_2 + \cdots + s_{k(j-1)}\boldsymbol{c}_j + m_0 \begin{pmatrix} Tr(\xi_k) \\ \vdots \\ Tr(\alpha^{n-1}\xi_k) \end{pmatrix} \tag{3.4}$$

for $k = 1, 2, \ldots, n$. Let $\boldsymbol{c}_{k_1}, \boldsymbol{c}_{k_2}, \ldots, \boldsymbol{c}_{k_{j+1}}$ be any $(j+1)$ columns of $C(\alpha)$, and let p be a prime number such that m_0 is exactly divisible by p^t $(t > 0)$. Then (3.4) implies that some $\boldsymbol{c}_{k_i}$ is a linear combination modulo p^t of the other j columns with integer coefficients. Hence every minor of order $(j+1)$ of the matrix $C(\alpha)$ is divisible by p^t, and so, by m_0. Hence $\tilde{c}_{j+1}(\alpha)$ is divisible by m_0.

It is well-known (e.g. [6], p.34) that an algebraic number field $K = \boldsymbol{Q}(\alpha)$ $(\alpha \in O_K)$ of degree $n > 1$ has an integral basis of the form

$$(3.5)\quad 1, \frac{c_{10} + \alpha}{m_1}, \frac{c_{20} + c_{21}\alpha + \alpha^2}{m_2}, \ldots, \frac{c_{(n-1)0} + \cdots + c_{(n-1)(n-2)}\alpha^{n-2} + \alpha^{n-1}}{m_{n-1}},$$

where $c_{ij}, m_j \in \boldsymbol{Z}$; m_j is divisible by m_{j-1} for every $j > 1$. By Proposition 1 we see that $\tilde{c}_{j+1}(\alpha)$ is divisible by m_j for every $j \leq n-1$.

Considering the elementary divisors of $C(\alpha)$, we obtain

Proposition 2. *Let K be an algebraic number field of degree $n > 1$, and let α be an integer of K such that $K = \boldsymbol{Q}(\alpha)$. Then $\tilde{c}_{i+1}(\alpha)/\tilde{c}_i(\alpha)$ is divisible by $\tilde{c}_i(\alpha)/\tilde{c}_{i-1}(\alpha)$ for every $i = 1, 2, \ldots, n-1$, where $\tilde{c}_0(\alpha) = 1$. Let p be a prime number such that $\tilde{c}_i(\alpha)$ is divisible by p^t $(t > 0)$. Then $\tilde{c}_{i+1}(\alpha)$ is divisible by p^{t+1}.*

Proof. By hypothesis, $\det C(\alpha) \neq 0$. The integers

$$e_1 = \frac{\tilde{c}_1(\alpha)}{\tilde{c}_0(\alpha)},\ e_2 = \frac{\tilde{c}_2(\alpha)}{\tilde{c}_1(\alpha)},\ \ldots,\ e_n = \frac{\tilde{c}_n(\alpha)}{\tilde{c}_{n-1}(\alpha)}$$

are the elementary divisors of $C(\alpha)$. Since e_{i+1} is divisible by e_i, it follows that $\tilde{c}_{i+1}(\alpha)/\tilde{c}_i(\alpha)$ is divisible by $\tilde{c}_i(\alpha)/\tilde{c}_{i-1}(\alpha)$. To prove the last assertion, suppose that $\tilde{c}_{i+1}(\alpha)$ is not divisible by p^{t+1}. Then $\tilde{c}_{i+1}(\alpha)$ is exactly divisible by p^t; $e_{i+1} = \tilde{c}_{i+1}(\alpha)/\tilde{c}_i(\alpha)$ is not divisible by p. On the other hand,

$$(3.6)\qquad \tilde{c}_{i+1}(\alpha) = e_1 e_2 \cdots e_{i+1}, \qquad e_j | e_{j+1}.$$

This implies that $\tilde{c}_{i+1}(\alpha)$ is not divisible by p, a contradiction.

4. Examples.

1) Consider now a cubic field:

$$(4.1)\qquad K = \boldsymbol{Q}(\alpha);\quad \alpha^3 + a_1\alpha^2 + a_2\alpha + a_3 = 0, \quad a_i \in \boldsymbol{Z},$$

where $f(x) = x^3 + a_1x^2 + a_2x + a_3$ is irreducible. We obtain:

$$(4.2)\qquad A = \begin{pmatrix} 0 & 0 & -a_3 \\ 1 & 0 & -a_2 \\ 0 & 1 & -a_1 \end{pmatrix};$$

$$(4.3)\qquad B = f'(A) = \begin{pmatrix} a_2 & -3a_3 & a_1a_3 \\ 2a_1 & -2a_2 & a_1a_2 - 3a_3 \\ 3 & -a_1 & {a_1}^2 - 2a_2 \end{pmatrix};$$

(4.4)

$$C(\alpha) = \begin{pmatrix} Tr(1) & Tr(\alpha) & Tr(\alpha^2) \\ Tr(\alpha) & Tr(\alpha^2) & Tr(\alpha^3) \\ Tr(\alpha^2) & Tr(\alpha^3) & Tr(\alpha^4) \end{pmatrix}$$
$$= \begin{pmatrix} 3 & -a_1 & {a_1}^2 - 2a_2 \\ -a_1 & {a_1}^2 - 2a_2 & -{a_1}^3 + 3a_1a_2 - 3a_3 \\ {a_1}^2 - 2a_2 & -{a_1}^3 + 3a_1a_2 - 3a_3 & {a_1}^4 - 4{a_1}^2a_2 + 4a_1a_3 + 2{a_2}^2 \end{pmatrix}.$$

Let $\tilde{b}_{ij}$ (resp. $\tilde{c}_{ij}$) denote the cofactor of the (i,j)-entry of the matrix B (resp. $C(\alpha)$). Then

(4.5)
$$\begin{aligned} \tilde{c}_{31} &= -\tilde{b}_{11} = {a_1}^2a_2 - 4{a_2}^2 + 3a_1a_3, \\ \tilde{c}_{32} &= -\tilde{b}_{12} = 2{a_1}^3 - 7a_1a_2 + 9a_3, \\ \tilde{c}_{33} &= -\tilde{b}_{13} = 2({a_1}^2 - 3a_2). \end{aligned}$$

Let $d(\alpha)$ denote the discriminant of α. Then a classical formula

(4.6)
$$d(\alpha) = -4{a_1}^3a_3 + {a_1}^2{a_2}^2 + 18a_1a_2a_3 - 4{a_2}^3 - 27{a_3}^2$$

follows from

(4.7)
$$d(\alpha) = -\det B = -(a_2\tilde{b}_{11} - 3a_3\tilde{b}_{12} + a_1a_3\tilde{b}_{13}).$$

Let p ($p \neq 2$) be a prime factor of $\tilde{c}_2(\alpha)$ (which we defined in §3). Then $\tilde{c}_{33}$ is divisible by p, and so

(4.8)
$${a_1}^2 \equiv 3a_2 \pmod{p}.$$

Since $d(\alpha) = \det C(\alpha)$ is divisible by p, it follows from (4.6) and (4.8) that

(4.9)
$$27d(\alpha) \equiv -({a_1}^3 - 3^3a_3)^2 \equiv 0 \pmod{p}.$$

Hence

(4.10)
$${a_1}^3 \equiv 3^3a_3 \pmod{p}.$$

Conversely, if p ($p \neq 3$) is a prime number which satisfies (4.8) and (4.10), then $\tilde{c}_{33}$ and $d(\alpha)$ are both divisible by p, and $\tilde{c}_2(\alpha)$ is also divisible by p (Theorem 2).

Thus we have proved the following result: *For a prime number p ($p \neq 2,3$) to divide all the minors of order two of the matrix $C(\alpha)$ it is necessary and sufficient that ${a_1}^2 \equiv 3a_2 \pmod{p}$ and ${a_1}^3 \equiv 3^3a_3 \pmod{p}$.*

2) Consider now a cubic field (4.1) satisfying $a_2 \equiv a_3 \equiv 0 \pmod{3}$, $a_1 \not\equiv 0 \pmod{3}$. Then by (4.5) and (4.6) we see that both $\tilde{c}_{31}$ and $d(\alpha) = \det C(\alpha)$ are divisible by 3, but $\tilde{c}_{33}$ is not divisible by 3 (cf. Theorem 2, Lemma 1). Suppose that $a_1 \equiv a_3 \equiv 1$, $a_2 \equiv -1 \pmod{4}$. Consider the prime $p = 2$. By (4.5) and (4.6) we see that both $\tilde{c}_{33}$ and $\det C(\alpha)(= d(\alpha))$ are divisible by p^2, but $\tilde{c}_{31}$ is not divisible by p^2 (cf. Theorem 2).

3) The converse of Theorem 1 is not true. Let $k = 1, p = 2$, and let K be a cubic field with odd discriminant d_K such that, for every integer α of K, the discriminant $d(\alpha)$ of α is even (Dedekind[3]). Then, for any integer α of K, $\det C(\alpha) = d(\alpha)$ is

divisible by $p=2$; it follows from Theorem 2 and (4.5) that every minor of order two of the matrix $C(\alpha)$ is divisible by p, but d_K is not divisible by p^2.

4) Let O_K denote the ring of integers of an algebraic number field K of degree $n>1$, and let $\alpha \in O_K$ such that $K=\boldsymbol{Q}(\alpha)$. Let δ (resp. $d(\alpha)$) denote the different (resp. discriminant) of α in $K/\boldsymbol{Q}$, and let $m^2 (m \in \boldsymbol{Z})$ denote the largest square dividing $d(\alpha)$. By (1.44) we see that

$$\frac{d(\alpha)}{m\delta} \in O_K. \tag{4.11}$$

From (2.4),

$$\frac{d(\alpha)}{m\delta} = \frac{\tilde{c}_{n1} + \tilde{c}_{n2}\alpha + \cdots + \tilde{c}_{nn}\alpha^{n-1}}{m}, \tag{4.12}$$

where $\tilde{c}_{ij}$ denotes the cofactor of the (i,j)-entry of the matrix $C(\alpha)$.

Now suppose that $\tilde{c}_{n-1}(\alpha)=1$. Then K has a very simple integral basis (cf. [1],[4],[6]). By Theorem 2 we see that m is prime to $\tilde{c}_{nn}$. Let $a,b \in \boldsymbol{Z}$ such that

$$a\tilde{c}_{nn} + bm = 1, \tag{4.13}$$

and define

$$\beta = \frac{ad(\alpha)}{m\delta} + b\alpha^{n-1} \in O_K. \tag{4.14}$$

Then $\{1, \alpha, \ldots, \alpha^{n-2}, \beta\}$ is an integral basis of K, since

$$\begin{vmatrix} 1 & \alpha^{(1)} & \ldots & \alpha^{(1)n-2} & \beta^{(1)} \\ & & \ldots & & \\ 1 & \alpha^{(n)} & \ldots & \alpha^{(n)n-2} & \beta^{(n)} \end{vmatrix}^2 = \frac{d(\alpha)}{m^2} \tag{4.15}$$

is square-free. The discriminant of K is

$$d_K = \frac{d(\alpha)}{m^2}. \tag{4.16}$$

Since d_K is square-free, it follows from [5] (Theorem 1) that the Galois group of $\bar{K}/\boldsymbol{Q}$ is isomorphic to the symmetric group S_n, where $\bar{K}$ denotes the Galois closure of $K/\boldsymbol{Q}$.

References

[1] H. COHEN, A Course in Computational Algebraic Number Theory, Springer-Verlag, 1993.

[2] R. DEDEKIND und H. WEBER, Theorie der algebraischen Funktionen einer Veränderlichen, J. Reine Angew. Math., 92(1882), 181-290.

[3] R. DEDEKIND, Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen, 23(1878), 1-23.

[4] K. KOMATSU, Integral bases in algebraic number fields, J. Reine Angew. Math., 278/279(1975), 137-144.

[5] K. KOMATSU, Square-free discriminants and affect-free equations, Tokyo J. Math., 14(1991), 57-60.

[6] M. PHOST, Computational Algebraic Number Theory, Birkhäuser Verlag, 1993.