<table>
<thead>
<tr>
<th>Title</th>
<th>On discriminants and certain matrices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sub Title</td>
<td></td>
</tr>
<tr>
<td>Author</td>
<td>Komatsu, Kenzo</td>
</tr>
<tr>
<td>Publisher</td>
<td>慶應義塾大学理工学部</td>
</tr>
<tr>
<td>Publication year</td>
<td>1996</td>
</tr>
<tr>
<td>Abstract</td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td></td>
</tr>
<tr>
<td>Genre</td>
<td>Departmental Bulletin Paper</td>
</tr>
</tbody>
</table>
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 $\alpha$ be an integer of $K$. In this paper we discuss the $n \times n$ matrix $C(\alpha) = (\text{Tr}(\alpha^{(i-1)+(j-1)})$ and its minors. Certain minors of $C(\alpha)$ are closely related to the ramification of primes in $K/Q$. 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 $k \in \mathbb{Z}$, $k > 0$. Suppose that the discriminant of $K$ is divisible by $p^{2k}$. Then, for any integer $\alpha$ of $K$, every minor of order $(n-1)$ of the $n \times n$ matrix

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

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

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

$$C(\alpha) = \begin{pmatrix}
1 & \alpha^{(1)} & \ldots & \alpha^{(1)n-1} \\
\alpha^{(1)} & \alpha^{(2)} & \ldots & \alpha^{(2)n-1} \\
\ldots & \ldots & \ldots & \ldots \\
\alpha^{(1)n-1} & \alpha^{(2)n-1} & \ldots & \alpha^{(n)n-1}
\end{pmatrix}
\begin{pmatrix}
1 & \alpha^{(1)} & \ldots & \alpha^{(1)n-1} \\
1 & \alpha^{(2)} & \ldots & \alpha^{(2)n-1} \\
\ldots & \ldots & \ldots & \ldots \\
1 & \alpha^{(n)} & \ldots & \alpha^{(n)n-1}
\end{pmatrix}.$$
Suppose first that $K \neq \mathbb{Q}(\alpha)$. If $n > 2$, then
\[
\text{rank}\begin{pmatrix}
1 & \alpha^{(1)} & \cdots & \alpha^{(1)n-1} \\
1 & \alpha^{(n)} & \cdots & \alpha^{(n)n-1}
\end{pmatrix} \leq \frac{n}{2} < n - 1.
\]

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 $\alpha \in \mathbb{Z}$, $k = 1$ 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 $K = \mathbb{Q}(\alpha)$. Let
\[
f(x) = (x - \alpha^{(1)})(x - \alpha^{(2)}) \cdots (x - \alpha^{(n)}) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n.
\]

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

$K = \mathbb{Q}(\alpha)$ is a vector space over $\mathbb{Q}$. We fix its basis: $1, \alpha, \ldots, \alpha^{n-1}$. An element $\xi = c_0 + c_1 \alpha + \cdots + c_{n-1} \alpha^{n-1} (c_i \in \mathbb{Q})$ of $K$ is then represented by a column vector $(c_0, \ldots, c_{n-1})^T$, where $T$ denotes transposition. The linear transformation $\xi \mapsto \alpha \xi$ is determined by the $n \times n$ matrix
\[
A = (e_2 e_3 \cdots e_n a_1),
\]
where
\[
a_1 = (-a_n, -a_{n-1}, \ldots, -a_2, -a_1)^T;
\]
ej denotes the j-th column of the identity matrix $I_n$. We define $a_2, a_3, \ldots$ inductively:
\[
a_j = A a_{j-1},
\]
where $j \geq 2$. Clearly,
\[
a_1 = A e_n.
\]
By induction on $j$, we see that
\[
A^j = (e_{j+1} e_{j+2} \cdots e_n a_1 \cdots a_j)
\]
for $j = 1, 2, \ldots, n - 1$.

Now let
\[
g(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in \mathbb{Q}[x],
\]
and let $g_j$ denote the $j$-th column of the matrix $g(A)$:
\[
g(A) = c_0 I_n + c_1 A + \cdots + c_{n-1} A^{n-1},
\]
\[
g(A) = (g_1 g_2 \cdots g_n).
\]
Then
\[
g_j = g(A) e_j
\]
for $j = 1, 2, \ldots, n$. The matrix $g(A)$ determines a linear transformation $\xi \mapsto g(\alpha) \xi$.

By (1.12) we see that the column vector $g_j$ represents $g(\alpha) \alpha^{j-1}$ in $K$. Since
On Discriminants and Certain Matrices

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

it follows from (1.9) that

\[ g_j = A^{j-1} = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} \]

for \( j = 1, 2, \ldots, n \). Hence

\[ g_1 = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix}, \quad g_j = Ag_{j-1}, \]

where \( 2 \leq j \leq n \).

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

\[ h(\alpha) \leftrightarrow h(A). \]

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

\[ N(h(\alpha)) = \det h(A). \]

Now let \( b_j \) denote the \( j \)-th column of the matrix \( B = f'(A) \):

\[ B = f'(A) = nA^{n-1} + (n-1)a_1A^{n-2} + \cdots + a_{n-1}I_n, \]

\[ B = (b_1b_2 \ldots b_n). \]

Then it follows from (1.14) that

\[ b_1 = \begin{pmatrix} a_{n-1} \\ 2a_{n-2} \\ \vdots \\ (n-1)a_1 \\ n \end{pmatrix}, \quad b_j = Ab_{j-1}, \]

where \( 2 \leq j \leq n \).

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

\[ \delta = f'(\alpha), \quad D = N(\delta). \]

Then (1.16) gives

\[ D = \det B. \]
For \( j = 1, 2, \ldots, n \), let
\[
(1.22) \quad \alpha^{j-1} \delta = r_{1j} + r_{2j} \alpha + \cdots + r_{nj} \alpha^{n-1},
\]
where \( r_{ij} \in \mathbb{Z} \). Then it follows from (1.15), (1.20) and (1.17) that
\[
(1.23) \quad \alpha^{j-1} B = r_{1j} I_n + r_{2j} A + \cdots + r_{nj} A^{n-1}
\]
for \( j = 1, 2, \ldots, n \). By (1.19) we see that the first column of \( \alpha^{j-1} B \) is \( \alpha^{j-1} b_1 = b_j \).
Hence, by (1.14),
\[
(1.24) \quad b_j = (r_{1j}, r_{2j}, \ldots, r_{nj})^T.
\]
Now let \( b_{ij} \) denote the \((i,j)\)-entry of the matrix \( B \):
\[
(1.25) \quad B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}.
\]
By (1.22) and (1.24) we see that
\[
(1.26) \quad \alpha^{j-1} \delta = b_{1j} + b_{2j} \alpha + \cdots + b_{nj} \alpha^{n-1}
\]
for \( j = 1, 2, \ldots, n \). Let \( \tilde{b}_{ij} \) denote the cofactor of the \((i,j)\)-entry \( b_{ij} \), and let
\[
(1.27) \quad \alpha^{j-1} \frac{D}{\delta} = s_{1j} + s_{2j} \alpha + \cdots + s_{nj} \alpha^{n-1},
\]
where \( s_{ij} \in \mathbb{Z}, 1 \leq j \leq n \). From (1.15), (1.17), (1.20) and (1.21), we obtain
\[
(1.28) \quad (\det B) B^{-1} B = s_{1j} I_n + s_{2j} A + \cdots + s_{nj} A^{n-1}.
\]
By (1.8) we see that the first column of the matrix \( \alpha^{j-1} \) is \( e_j \). From (1.14) we obtain
\[
(s_{1j}, \ldots, s_{nj})^T = (\det B) B^{-1} e_j = (\tilde{b}_{j1}, \ldots, \tilde{b}_{jn})^T.
\]
Hence (1.27) becomes
\[
(1.29) \quad \alpha^{j-1} \frac{D}{\delta} = \tilde{b}_{j1} + \tilde{b}_{j2} \alpha + \cdots + \tilde{b}_{jn} \alpha^{n-1}
\]
for \( j = 1, 2, \ldots, n \). In particular,
\[
(1.30) \quad \frac{D}{\delta} = \tilde{b}_{11} + \tilde{b}_{12} \alpha + \cdots + \tilde{b}_{1n} \alpha^{n-1}.
\]
It follows from (1.29) and (1.30) that every cofactor \( \tilde{b}_{ij} \) is divisible by the greatest common divisor of \( \tilde{b}_{11}, \ldots, \tilde{b}_{1n} \):
\[
(1.31) \quad (\tilde{b}_{11}, \tilde{b}_{12}, \ldots, \tilde{b}_{1n}) \mid \tilde{b}_{ij},
\]
On Discriminants and Certain Matrices

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

Clearly, the column vector

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

is an eigenvector of the matrix $A^T$ corresponding to the eigenvalue $\alpha$:

$$ A^T x = \alpha x, \quad x \neq 0. $$

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

$$ A(M x) = \alpha M x, $$

where

$$ M = \begin{pmatrix}
    a_{n-1} & a_{n-2} & \cdots & a_1 & 1 \\
    a_{n-2} & a_{n-3} & \cdots & 1 \\
    \vdots & \vdots & \ddots & \vdots & \vdots \\
    a_1 & 1 & \cdots & 0 \\
    1 & & & & 
\end{pmatrix}. $$

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

$$ AM = M A^T. $$

Hence

$$ A^j M = M (A^T)^j $$

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

Let $c_j$ denote the $j$-th column of the matrix $C(\alpha)$:

$$ C(\alpha) = (c_1 c_2 \ldots c_n). $$

By definition,

$$ c_j = (\text{Tr}(\alpha^{j-1}), \text{Tr}(\alpha^j), \ldots, \text{Tr}(\alpha^{j+n-2}))^T. $$

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

$$ c_j = A^T c_{j-1} $$

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

$$ b_2 = \begin{pmatrix}
    -na_n \\
    -(n-1)a_{n-1} \\
    \vdots \\
    -2a_2 \\
    -a_1 
\end{pmatrix}. $$

Newton's formula gives

$$ M c_2 = b_2. $$
From (1.19), (1.37), (1.40) and (1.42), we obtain the following formula (cf. [2], §10):

\[(1.43) \quad B = MC(\alpha).\]

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

\[(1.44) \quad \frac{D}{m^2} \in \mathcal{O}_K,\]

where \(\mathcal{O}_K\) denotes the ring of integers of \(K\) ([4], Theorem 1). Let \(t\) denote the index of \(\alpha\):

\[(1.45) \quad t = (\mathcal{O}_K : \mathbb{Z}[\alpha]).\]

Then

\[(1.46) \quad (-1)^{\frac{n(n-1)}{2}} D = d_K t^2,\]

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

\[(1.47) \quad \frac{t\tilde{b}_{1j}}{m} \in \mathbb{Z}\]

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

\[(1.48) \quad \frac{D\tilde{b}_{1j}^2}{m^2d_K} \in \mathbb{Z}\]

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

\[(1.49) \quad p^k | \tilde{b}_{ij}\]

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:

\[(1.50) \quad M^{-1} \in M_n(\mathbb{Z}).\]

From (1.43),

\[(1.51) \quad C(\alpha) = M^{-1}B.\]

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

\[(1.52) \quad \text{adj}C(\alpha) = \text{adj}B \text{ adj}(M^{-1}).\]

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

Remark. It follows from (1.1) that, for any integer \(\alpha\) of \(K\), \(\det C(\alpha)\) is equal to the discriminant of \(\alpha\) in \(K/\mathbb{Q}\), 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.
On Discriminants and Certain Matrices

\[ \alpha \text{ such that at least one minor of order } n - 1 \text{ of the matrix } C(\alpha) \text{ is not divisible by } p. \] A simple example is

\[ K = Q(\alpha), \quad \alpha^2 - p = 0, \]

where \( p \) is an odd prime. The matrix

\[ C(\alpha) = \begin{pmatrix} 2 & 0 \\ 0 & 2p \end{pmatrix} \]

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 \( \alpha \) 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

\[ C(\alpha) = \begin{pmatrix} \text{Tr}(1) & \text{Tr}(\alpha) & \ldots & \text{Tr}(\alpha^{n-1}) \\ \text{Tr}(\alpha) & \text{Tr}(\alpha^2) & \ldots & \text{Tr}(\alpha^n) \\ \ldots & \ldots & \ldots & \ldots \\ \text{Tr}(\alpha^{n-1}) & \text{Tr}(\alpha^n) & \ldots & \text{Tr}(\alpha^{2n-2}) \end{pmatrix} \]

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 \( j = 1, 2, \ldots, n \).

**Proof.** By hypothesis,

\[ Sv = 0, \]

where \( v = (\tilde{s}_{n1}, \tilde{s}_{n2}, \ldots, \tilde{s}_{nn})^T \). For \( j = 1, 2, \ldots, n \), 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

\[ S_j v_0 = 0 \]

for \( j = 1, 2, \ldots, n \), where

\[ v_0 = (\tilde{s}_{n1}, \tilde{s}_{n2}, \ldots, \tilde{s}_{n(n-1)})^T. \]

Suppose that \( \tilde{s}_{nj} \neq 0 \) for some \( j < n \). Then \( v_0 \neq 0 \), and so \( \det S_j = 0 \). This implies that \( \tilde{s}_{jn} = \tilde{s}_{nj} = 0 \), a contradiction. Hence \( \tilde{s}_{nj} = 0 \) for \( j = 1, 2, \ldots, n \).

**Proof of Theorem.** We may assume that \( K = Q(\alpha) \) (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 $\delta$ (resp. $d(\alpha)$) denote the different (resp. discriminant) of $\alpha$ in $K/Q$. Then, from (1.30), (1.35) and (1.43),
\begin{equation}
\frac{d(\alpha)}{\delta} = \tilde{c}_{n1} + \tilde{c}_{n2}\alpha + \cdots + \tilde{c}_{nn}\alpha^{n-1}.
\end{equation}

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 $\alpha$ be an integer of $K$. Let $i \in \mathbb{Z}$, $1 \leq i \leq n$. 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 $s^2 (s \in \mathbb{Z})$ denote the largest square dividing the discriminant of an algebraic number field $K$ of degree $n > 1$. Then, for any integer $\alpha$ 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 $j \in \mathbb{Z}$, $1 \leq j \leq n-1$. Let $\alpha \in O_K$, and let $c_0, \ldots, c_{j-1}, m_0 \ (m_0 \neq 0)$ be rational integers such that
\begin{equation}
\frac{c_0 + c_1\alpha + \cdots + c_{j-1}\alpha^{j-1} + \alpha^j}{m_0} \in O_K.
\end{equation}

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

**Proof.** Let $c_k$ denote the $k$-th column of the matrix $C(\alpha)$:
\begin{equation}
c_k = \begin{pmatrix}
\text{Tr}(\alpha^{k-1}) \\
\text{Tr}(\alpha^k) \\
\vdots \\
\text{Tr}(\alpha^{k+n-2})
\end{pmatrix}.
\end{equation}

By induction we see that
\begin{equation}
\alpha^{k-1} = s_{k0} + s_{k1}\alpha + \cdots + s_{k(j-1)}\alpha^{j-1} + m_0\xi_k
\end{equation}
for $k = 1, 2, \ldots, n$, where $s_{kl} \in \mathbb{Z}, \xi_k \in O_K$. Hence
\begin{equation}
c_k = s_{k0}c_1 + s_{k1}c_2 + \cdots + s_{k(j-1)}c_j + m_0
\begin{pmatrix}
\text{Tr}(\xi_k) \\
\vdots \\
\text{Tr}(\alpha^{n-1}\xi_k)
\end{pmatrix}
\end{equation}
for \( k = 1, 2, \ldots, n \). Let \( c_{k_1}, c_{k_2}, \ldots, c_{k_{j+1}} \) 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 \( c_{k_i} \) 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 \( K = \mathbb{Q}(\alpha) \) \((\alpha \in \mathbb{O}_K)\) of degree \( n > 1 \) has an integral basis of the form

\[
(3.5) \quad \frac{c_{10} + \alpha}{m_1}, \frac{c_{20} + c_1 \alpha + \alpha^2}{m_2}, \ldots, \frac{c_{(n-1)0} + \cdots + c_{(n-1)(n-2)} \alpha^{n-2} + \alpha^{n-1}}{m_{n-1}},
\]

where \( c_{ij}, m_j \in \mathbb{Z} \); \( m_j \) 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 \( \alpha \) be an integer of \( K \) such that \( K = \mathbb{Q}(\alpha) \). 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,

\[
\tilde{c}_{i+1}(\alpha) = e_1 e_2 \cdots e_{i+1}, \quad e_j | e_{j+1}.
\]

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

4. Examples.

1) Consider now a cubic field:

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

where \( f(x) = x^3 + a_1 x^2 + a_2 x + a_3 \) is irreducible. We obtain:

\[
(4.2) \quad A = \begin{pmatrix} 0 & 0 & -a_3 \\ 1 & 0 & -a_2 \\ 0 & 1 & -a_1 \end{pmatrix};
\]

\[
(4.3) \quad B = f'(A) = \begin{pmatrix} a_2 & -3a_3 & a_4 a_3 \\ 2a_1 & -2a_2 & a_1 a_2 - 3a_3 \\ 3 & -a_1 & a_1^2 - 2a_2 \end{pmatrix};
\]
(4.4) \[ C'(\alpha) = \begin{pmatrix} \text{Tr}(1) & \text{Tr}(\alpha) & \text{Tr}(\alpha^2) \\ \text{Tr}(\alpha) & \text{Tr}(\alpha^2) & \text{Tr}(\alpha^3) \\ \text{Tr}(\alpha^2) & \text{Tr}(\alpha^3) & \text{Tr}(\alpha^4) \end{pmatrix} \]

\[ = \begin{pmatrix} 3 & -a_1 & a_1^2 - 2a_2 \\ -a_1 & a_1^2 - 2a_2 & -a_1^3 + 3a_1a_2 - 3a_3 \\ a_1^2 - 2a_2 & -a_1^3 + 3a_1a_2 - 3a_3 & a_1^4 - 4a_1^2a_2 + 4a_1a_3 + 2a_2^2 \end{pmatrix}. \]

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

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

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

\[
(4.6) d(\alpha) = -4a_1^3a_3 + a_1^2a_2^2 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2 
\]
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 \( a_2 \equiv a_3 \equiv 0 \pmod{3} \), \( a_1 \equiv 0 \pmod{3} \). 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 \( \alpha \) of \( K \), the discriminant \( d(\alpha) \) of \( \alpha \) is even (Dedekind[3]). Then, for any integer \( \alpha \) of \( K \), \( \det C'(\alpha) = d(\alpha) \) is
On Discriminants and Certain Matrices

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 \( K = \mathbb{Q}(\alpha) \). Let \( \delta \) (resp. \( d(\alpha) \)) denote the different (resp. discriminant) of \( \alpha \) in \( K/\mathbb{Q} \), and let \( m^2 (m \in \mathbb{Z}) \) denote the largest square dividing \( d(\alpha) \). By (1.44) we see that

\[
\frac{d(\alpha)}{m\delta} \in O_K.
\]

From (2.4),

\[
d(\alpha) = \frac{\tilde{c}_{n1} + \tilde{c}_{n2} \alpha + \cdots + \tilde{c}_{nn} \alpha^{n-1}}{m},
\]

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 \( a, b \in \mathbb{Z} \) such that

\[
a \tilde{c}_{nn} + bm = 1,
\]

and define

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

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

\[
\begin{vmatrix}
1 & \alpha^{(1)} & \cdots & \alpha^{(1)n-2} & \beta^{(1)} \\
1 & \alpha^{(n)} & \cdots & \alpha^{(n)n-2} & \beta^{(n)}
\end{vmatrix}^2 = \frac{d(\alpha)}{m^2}
\]

is square-free. The discriminant of \( K \) is

\[
d_K = \frac{d(\alpha)}{m^2}.
\]

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

References