On the different in orders in an algebraic number field
and special units connected with it*

by

E. C. Dade and O. Taussky (Pasadena, Calif.)

To L. J. Mordell to his 70-th birthday

1. Introduction. An order \( \mathcal{O} \) in an algebraic number field \( \mathbb{F} \) is called
principal if it can be generated over the rational integers \( \mathbb{Z} \) by a single
element. We are concerned with relations between two possible generators
of the same principal order.

Our result was stimulated by an attempt to explain the following
phenomenon:

Let \( \mathcal{O} \) be a principal order in a cubic field and let \( \theta, \lambda \) be two dif-
f erent generators of \( \mathcal{O} \). Then a set of relations of the following type must
exist for rational integral \( a_3 \) with \( |a_3| = \pm 1 \).

\[
\begin{align*}
  a_1 & = 1, \\
  a_1 + a_2 \theta + a_3 \theta^2 & = \lambda, \\
  a_1 + a_2 \theta^2 + a_3 \theta & = \lambda'.
\end{align*}
\]

(1)

Clearly,

\[
\begin{align*}
  |a_2| & = |a_3| = \pm 1.
\end{align*}
\]

(2)

Let \( \theta \) be a zero of the irreducible polynomial

\[
f(X) = X^3 + aX^2 + bX + c.
\]

(3)

Since the third equation in (1) is obtained by squaring the second
equation the quantities \( a_2, a_3 \) can be expressed in terms of \( a_1, a_2, a_3 \)
and \( a, b, c \). An easy computation shows that the left-hand side of (2)
is a cubic form in \( x = a_2, y = a_3 \):

\[
x^3 - 2ax^2y + (a^2 + b)xy^2 + (c - ab)yx^2.
\]

(4)

* This work was carried out (in part) under a National Science Foundation Grant
We noticed that this form is the norm of the element
\[(6) \quad \eta = x+y(\theta_1 + \theta_2)\]
where \(\theta = \theta_1, \theta_2, \theta_3\) are the zeros of (3). By (2) and this observation, \(\eta\) must be a unit. The unit \(\eta\) is in \(F\) and is connected with the system (1) in another manner.

The second equation of (1) implies that
\[(7) \quad (\theta - \theta_2)(\theta - \theta_3)(x+y(\theta_1 + \theta_2))(x+y(\theta_1 + \theta_3)) = (\lambda - \lambda_2)(\lambda - \lambda_3),\]
where \(\lambda_2, \lambda_3\) are the conjugates of \(\lambda\), corresponding to \(\theta_2, \theta_3\). Since both \(\theta\) and \(\lambda\) generate the order, the ratio of the differences \((\theta - \theta_2)/(\theta - \theta_3)\) and \((\lambda - \lambda_2)/(\lambda - \lambda_3)\) is a unit \(\epsilon\). We have
\[(8) \quad (x+y(\theta_1 + \theta_2))(x+y(\theta_1 + \theta_3)) = \epsilon = \pm \eta^{-1}.\]
This unit is in \(F\) and has norm \(\pm 1\) because this norm is the square of the rational integer \(\frac{\epsilon}{\gamma}\), so \(\epsilon = \eta^{-1}\). Since \(\theta_1 + \theta_3 = -\theta - \theta_2\), we may express \(\eta\) in the form \(x - ay - y\theta\). It is noteworthy that \(\eta\) is of a special form, not containing a term \(\theta^j\).

2. Some polynomials connected with the generator of a principal order
Now we consider a more general situation.

Let \(O = \mathbb{Z}[\theta]\) and \(O' = \mathbb{Z}[\lambda]\) be two principal orders in the algebraic number field \(F\) of degree \(n\). Suppose that \(O' \subset O\). Then
\[(9) \quad \lambda = x_1 + x_2 \theta + \cdots + x_{n-1} \theta^{n-1}\]
for some rational integers \(x_1, \ldots, x_{n-1}\).

Let \(f_\delta(X) = X^n - a_1 X^{n-1} + \cdots + a_n\)
be the monic irreducible polynomial for \(\theta\) over \(Z\), and let \(f_\delta(X)\) be the corresponding polynomial for \(\lambda\).

Let \(X_1, \ldots, X_{n-1}, \theta_1, \ldots, \theta_n\) be independent variables over \(F\). Define the polynomial \(l\) by
\[(10) \quad l(X_1, \ldots, X_{n-1}; \theta_1, \theta_2) = \sum_{i=1}^{n-1} X_i \theta_i - \theta_i.\]

Let \(\theta_1 = \theta, \theta_2, \ldots, \theta_n\) be the distinct conjugates of \(\theta\) in some common normal closure of \(F\). Let \(\lambda_1, \lambda_2, \ldots, \lambda_n\) be the corresponding conjugates of \(\lambda\). Then (7) implies that, for \(i \neq j, \lambda_i - \lambda_j = l(X_1, \ldots, X_{n-1}; \theta_i, \theta_j).\)
3. The main theorem. Each element of the ring $\mathcal{O}[\bar{x}_0, \ldots, \bar{x}_{n-1}]$ is of the form:

$$B_0 + B_1 \theta + \ldots + B_{n-1} \theta^{n-1}$$

where the $B_i$ lie in $\mathbb{Z}[\bar{x}_0, \ldots, \bar{x}_{n-1}]$. We apply this to the powers of the element:

$$A = \bar{x}_0 + \bar{x}_1 \theta + \ldots + \bar{x}_{n-1} \theta^{n-1}$$

obtaining unique polynomials $B_{ik}$ in $\mathbb{Z}[\bar{x}_0, \ldots, \bar{x}_{n-1}]$ such that:

$$A^i = B_{0i} + B_{1i} \theta + \ldots + B_{n-1i} \theta^{n-1}, \quad i \geq 0.$$ 

Clearly $B_{0i} = \delta_{ik}$, $B_{1k} = \bar{x}_k$, and $B_{1k}$ is homogeneous of degree $i$ in $\bar{x}_0, \ldots, \bar{x}_{n-1}$.

We form the matrix $(B_{ik})$, $i, k = 0, \ldots, n-1$. Its determinant must be a homogeneous polynomial $p(\bar{x}_0, \ldots, \bar{x}_{n-1})$ of degree $n(n-1)/2$ in the ring $\mathbb{Z}[\bar{x}_0, \ldots, \bar{x}_{n-1}]$.

The two polynomials $y(x_1, \ldots, x_{n-1}; \theta)$ and $z(x_0, \ldots, x_{n-1})$ are related by:

**Theorem 1.** The norm from $F(x_1, \ldots, x_{n-1})$ to $Q(x_1, \ldots, x_{n-1})$ of $y(x_1, \ldots, x_{n-1}; \theta)$ is $z(x_0, \ldots, x_{n-1})$. In particular, $x_0$ does not appear in $z$.

Proof. Let $\lambda_1 = \lambda_2, \ldots, \lambda_n$ be the conjugates of $\lambda$ corresponding to the conjugates $\theta_1, \ldots, \theta_n$ of $\theta$. By the matrix equation:

$$B_{10} = \begin{pmatrix} 1 & \ldots & 1 \\ \theta_1 & \ldots & \theta_n \\ \ldots & \ldots & \ldots \\ \theta_0^{n-1} & \ldots & \theta_n^{n-1} \\ \theta_1^{n-1} & \ldots & \theta_n^{n-1} \\ \ldots & \ldots & \ldots \\ \theta_0^{n-1} & \ldots & \theta_n^{n-1} \\ \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \ldots \\ \lambda_n \\ \end{pmatrix} = \begin{pmatrix} \lambda_1 \\ \ldots \\ \lambda_n \\ \end{pmatrix}$$

Taking determinants, we obtain:

$$z(x_0, \ldots, x_{n-1}) \prod_{i=1}^{n-1} (\theta_i - \theta) = \prod_{i=1}^{n-1} (\lambda_i - \lambda_0).$$

By (9) and (14), for $i \neq j$, we have

$$A_i - A_j = \sum_{k=1}^{n-1} x_k \frac{\theta_k - \theta_j}{\theta_i - \theta_j} = \lambda_k \frac{\theta_k - \theta_j}{\theta_i - \theta_j}.$$ 

Therefore (17) implies

$$z(x_0, \ldots, x_{n-1}) = \prod_{i=1}^{n-1} I(x_1, \ldots, x_{n-1}; \theta, \theta).$$

On the other hand, by (11),

$$\text{norm}[y(x_1, \ldots, x_{n-1}; \theta)] = \prod_{i=1}^{n-1} y(x_1, \ldots, x_{n-1}; \theta_i) = \prod_{i=1}^{n-1} I(x_1, \ldots, x_{n-1}; \theta_i, \theta_i) = z(x_0, \ldots, x_{n-1})^2.$$ 

4. Further remarks. The main theorem generalizes the fact observed in the introduction for cubic fields, not only to fields of arbitrary degree, but also to generators of two orders $\mathcal{O}, \mathcal{O}'$ with $\mathcal{O} \supseteq \mathcal{O}'$. Since the order $\mathcal{O}'$ is a sublattice of $\mathcal{O}$ the absolute value of the determinant of the transformation sending the basis $1, \theta, \ldots, \theta^{n-1}$ of $\mathcal{O}$ into the basis $1, \lambda_1, \ldots, \lambda^{n-1}$ of $\mathcal{O}'$ is $(\mathcal{O} : \mathcal{O}')$. By definition, $z(x_0, \ldots, x_{n-1})$ is this determinant. Therefore

$$z(x_0, \ldots, x_{n-1}) = \pm z(x_0, \ldots, x_{n-1}).$$

Hence we have the following theorem.

**Theorem 2.** The following three statements are equivalent:

1. $\mathcal{O} = \mathcal{O}'$,
2. $z(x_0, \ldots, x_{n-1}) = \pm 1$,
3. $y(x_1, \ldots, x_{n-1}; \theta)$ is a unit in $\mathbb{Z}[\theta]$ with norm $+1$.

An alternative proof of our results can be obtained by noticing that

$$y(x_1, \ldots, x_{n-1}; \theta) = f(\lambda) f(\theta).$$

is the ratio of the different of the two elements $\lambda$ and $\theta$. We call, as usual, $(-1)^{n(n-1)/2}$ times the norm of the different of an element its discriminant. The discriminant of $\theta$ coincides with the discriminant $d(\mathcal{O})$ of $\mathcal{O}$ and that of $\lambda$ with the discriminant $d(\mathcal{O}')$ of $\mathcal{O}'$. Further, for any two orders $\mathcal{O} \supseteq \mathcal{O}'$ (even for non principal orders)

$$d(\mathcal{O})/d(\mathcal{O}') = (\mathcal{O} : \mathcal{O})^2.$$ 

Hence, we have again

$$[z(x_0, \ldots, x_{n-1})] = \text{norm}[y(x_1, \ldots, x_{n-1}; \theta)] = (\mathcal{O} : \mathcal{O})^2.$$ 

**California Institute of Technology**

*Reçu par la Rédaction le 27.4.1963*