ACTA ARITHMETICA
IX (1964)

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 75-th birthday

1. Introduction. An order $\mathfrak{O}$ in an algebraic number field F is called *principal* if it can be generated over the rational integers 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 $\mathfrak{O}$ be a principal order in a cubic field and let θ, λ be two different generators of $\mathfrak{O}$. Then a set of relations of the following type must exist for rational integral a_{ik} with $|a_{ik}| = \pm 1$.

$$\begin{aligned} a_{11} \qquad\qquad &= 1, \\ a_{21} + a_{22}\theta + a_{23}\theta^2 &= \lambda, \\ a_{31} + a_{32}\theta + a_{33}\theta^2 &= \lambda^2. \end{aligned} \tag{1}$$

Clearly,

$$\begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} = \pm 1. \tag{2}$$

Let θ be a zero of the irreducible polynomial

$$f(X) = X^3 + aX^2 + bX + c. \tag{3}$$

Since the third equation in (1) is obtained by squaring the second equation the quantities a_{32}, a_{33} can be expressed in terms of a_{21}, a_{22}, a_{23} and a, b, c. An easy computation shows that the left-hand side of (2) is a cubic form in $x = a_{22}$, $y = a_{23}$:

$$x^3 - 2ax^2y + (a^2+b)xy^2 + (c-ab)y^3. \tag{4}$$

* This work was carried out (in part) under a National Science Foundation Grant

We noticed that this form is the norm of the element

$$\eta = x+y(\theta_2+\theta_3) \tag{5}$$

where $\theta = \theta_1, \theta_2, \theta_3$ are the zeros of (3). By (2) and this observation, η must be a unit. The unit η is in F and is connected with the system (1) in another manner.

The second equation of (1) implies that

$$(\theta-\theta_2)(\theta-\theta_3)\big(x+y(\theta_1+\theta_2)\big)\big(x+y(\theta_1+\theta_3)\big) = (\lambda-\lambda_2)(\lambda-\lambda_3),$$

where λ_2, λ_3 are the conjugates of $\lambda = \lambda_1$, corresponding to θ_2, θ_3. Since both θ and λ generate the order, the ratio of the differents $(\theta-\theta_2)(\theta-\theta_3)$ and $(\lambda-\lambda_2)(\lambda-\lambda_3)$ is a unit ε. We have

$$\big(x+y(\theta_1+\theta_2)\big)\big(x+y(\theta_1+\theta_3)\big) = \varepsilon = \pm\eta^{-1}. \tag{6}$$

This unit is in F and has norm $+1$ because this norm is the square of the rational integer $\prod_{i<j}\big(x+y(\theta_i+\theta_j)\big)$. Since $\theta_2+\theta_3 = -a-\theta$, we may express η in the form $x-ay-y\theta$. It is noteworthy that η is of a special form, not containing a term θ^2.

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

Let $\mathfrak{O} = Z[\theta]$ and $\mathfrak{O}' = Z[\lambda]$ be two principal orders in the algebraic number field F of degree n. Suppose that $\mathfrak{O}' \subseteq \mathfrak{O}$. Then

$$\lambda = X_0+X_1\theta+\ldots+X_{n-1}\theta^{n-1} \tag{7}$$

for some rational integers $X_0, \ldots, X_{n-1}$.

Let

$$f_\theta(\overline{X}) = \overline{X}^n-a_1\overline{X}^{n-1}+\ldots\pm a_n \tag{8}$$

be the monic irreducible polynomial for θ over Z, and let $f_\lambda(\overline{X})$ be the corresponding polynomial for λ.

Let $\overline{X}_0, \ldots, \overline{X}_{n-1}, \Theta_1, \ldots, \Theta_n$ be independent variables over F. Define the polynomial l by

$$l(\overline{X}_1, \ldots, \overline{X}_{n-1};\ \Theta_i, \Theta_j) = \sum_{k=1}^{n-1}\overline{X}_k\frac{\Theta_i^k-\Theta_j^k}{\Theta_i-\Theta_j}. \tag{9}$$

Let $\theta_1 = \theta, \theta_2, \ldots, \theta_n$ be the distinct conjugates of θ in some convenient normal closure of F. Let $\lambda_1 = \lambda, \lambda_2, \ldots, \lambda_n$ be the corresponding conjugates of λ. Then (7) implies that, for $i \neq j$,

$$\frac{\lambda_i-\lambda_j}{\theta_i-\theta_j} = l(X_1, \ldots, X_{n-1};\ \theta_i, \theta_j). \tag{10}$$

Define the polynomial y by

$$y(\overline{X}_1, \ldots, \overline{X}_{n-1}; \Theta) = \prod_{i=2}^{n} l(\overline{X}_1, \ldots, \overline{X}_{n-1}; \Theta, \theta_i). \tag{11}$$

The following lemma gives some basic properties of y.

LEMMA 1. *y is homogeneous of degree $n-1$ in $\overline{X}_1, \ldots, \overline{X}_{n-1}$. The coefficients of y lie in $\mathfrak{O} = Z[\theta]$.*

Proof. By (9) each factor l is a linear form in $\overline{X}_1, \ldots, \overline{X}_{n-1}$. So y is homogeneous of degree $n-1$ in these variables.

Since the coefficients of l are rational integers, it is obvious from (11) that the coefficients of y are symmetric rational integral polynomials in $\theta_2, \ldots, \theta_n$. Hence they lie in $F = Q(\theta)$ (where, as usual, Q is the rational number field). It will follow from the following more general lemma that they actually lie in $Z[\theta]$.

LEMMA 2 *Let $g(\Theta_2, \ldots, \Theta_n) \in Z[\Theta_2, \ldots, \Theta_n]$ be symmetric in the variables $\Theta_2, \ldots, \Theta_n$. Then $g(\theta_2, \ldots, \theta_n) \in Z[\theta]$. In fact $g(\Theta_2, \ldots, \Theta_n) \in Z[\Theta_1, A_1, \ldots, A_{n-1}]$, where $A_1, \ldots, A_n$ are the elementary symmetric functions of the variables $\Theta_1, \ldots, \Theta_n$.*

Proof. Let $S_1, \ldots, S_{n-1}$ be the elementary symmetric functions of the variables $\Theta_2, \ldots, \Theta_n$. Since the Θ's are independent transcendentals over Q, so are the S's. Hence $Z[S_1, \ldots, S_{n-1}]$ is integrally closed in its quotient field $Q(S_1, \ldots, S_{n-1})$ (since it is a unique factorization domain). Since $\Theta_2, \ldots, \Theta_n$ are the zeros of $\overline{X}^{n-1}-S_1\overline{X}^{n-2}+\ldots\pm S_{n-1}$, they are integral over $Z[S_1, \ldots, S_{n-1}]$. Therefore

$$Z[\Theta_2, \ldots, \Theta_n] \cap Q(S_1, \ldots, S_{n-1}) = Z[S_1, \ldots, S_{n-1}].$$

Our hypothesis is that $g(\Theta_2, \ldots, \Theta_n)$ lies in the ring on the left. So it lies in $Z[S_1, \ldots, S_{n-1}]$. But

$$\begin{aligned} S_1 &= A_1-\Theta_1, \\ S_2 &= A_2-A_1\Theta_1+\Theta_1^2, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ S_{n-1} &= A_{n-1}-A_{n-2}\Theta_1+\ldots\pm\Theta_1^{n-1}. \end{aligned} \tag{12}$$

Therefore $Z[S_1, \ldots, S_{n-1}] \subseteq Z[\Theta_1, A_1, \ldots, A_{n-1}]$. This proves the second statement of the lemma.

If $\Theta_1, \ldots, \Theta_n$ are specialized to $\theta_1, \ldots, \theta_n$, then $A_1, \ldots, A_n$ specialize to $a_1, \ldots, a_n \in Z$. So

$$g(\theta_2, \ldots, \theta_n) \in Z[\theta_1, a_1, \ldots, a_{n-1}] = Z[\theta].$$

3. The main theorem. Each element of the ring $\mathfrak{O}[\bar{X}_0, \ldots, \bar{X}_{n-1}] = Z[\theta, \bar{X}_0, \ldots, \bar{X}_{n-1}]$ has a unique expression of the form:

$$B_0 + B_1\theta + \ldots + B_{n-1}\theta^{n-1} \tag{13}$$

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

$$\Lambda = \bar{X}_0 + \bar{X}_1\theta + \ldots + \bar{X}_{n-1}\theta^{n-1} \tag{14}$$

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

$$\Lambda^i = B_{i0} + B_{i1}\theta + \ldots + B_{in-1}\theta^{n-1}, \quad i \geqslant 0. \tag{15}$$

Clearly $B_{0k} = \delta_{0k}$, $B_{1k} = \bar{X}_k$, and B_{ik} 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 $z(\bar{X}_0, \ldots, \bar{X}_{n-1})$ of degree $n(n-1)/2$ in the ring $Z[\bar{X}_0, \ldots, \bar{X}_{n-1}]$.

The two polynomials $y(\bar{X}_1, \ldots, \bar{X}_{n-1}; \Theta)$ and $z(\bar{X}_0, \ldots, \bar{X}_{n-1})$ are related by:

THEOREM 1. *The norm from $F(\bar{X}_1, \ldots, \bar{X}_{n-1})$ to $Q(\bar{X}_1, \ldots, \bar{X}_{n-1})$ of $y(\bar{X}_1, \ldots, \bar{X}_{n-1}; \theta)$ is $z(\bar{X}_0, \ldots, \bar{X}_{n-1})^2$. In particular, $\bar{X}_0$ does not appear in z.*

Proof. Let $\Lambda_1 = \Lambda, \Lambda_2, \ldots, \Lambda_n$ be the conjugates of Λ corresponding to the conjugates $\theta_1, \ldots, \theta_n$ of θ. By (15), we have the matrix equation:

$$(B_{ik})\begin{pmatrix} 1 & \ldots & 1 \\ \theta_1 & \ldots & \theta_n \\ \cdots & \cdots & \cdots \\ \theta_1^{n-1} & \ldots & \theta_n^{n-1} \end{pmatrix} = \begin{pmatrix} 1 & \ldots & 1 \\ \Lambda_1 & \ldots & \Lambda_n \\ \cdots & \cdots & \cdots \\ \Lambda_1^{n-1} & \ldots & \Lambda_n^{n-1} \end{pmatrix}. \tag{16}$$

Taking determinants, we obtain:

$$z(\bar{X}_0, \ldots, \bar{X}_{n-1})\prod_{i<j}(\theta_i - \theta_j) = \prod_{i<j}(\Lambda_i - \Lambda_j). \tag{17}$$

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

$$\frac{\Lambda_i - \Lambda_j}{\theta_i - \theta_j} = \sum_{k=1}^{n-1} \bar{X}_k \frac{\theta_i^k - \theta_j^k}{\theta_i - \theta_j} = l(\bar{X}_1, \ldots, \bar{X}_{n-1}; \theta_i, \theta_j).$$

Therefore (17) implies

$$z(\bar{X}_0, \ldots, \bar{X}_{n-1}) = \prod_{i<j} l(\bar{X}_1, \ldots, \bar{X}_{n-1}; \theta_i, \theta_j).$$

On the other hand, by (11),

$$\operatorname{norm}\big(y(\bar{X}_1, \ldots, \bar{X}_{n-1}; \theta)\big) = \prod_{j=1}^{n} y(\bar{X}_1, \ldots, \bar{X}_{n-1}; \theta_j)$$
$$= \prod_{i\neq j} l(\bar{X}_1, \ldots, \bar{X}_{n-1}; \theta_j, \theta_i) = z(\bar{X}_0, \ldots, \bar{X}_{n-1})^2.$$

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 $\mathfrak{O}, \mathfrak{O}'$ with $\mathfrak{O} \supseteq \mathfrak{O}'$. Since the order $\mathfrak{O}'$ is a sublattice of $\mathfrak{O}$ the absolute value of the determinant of the transformation sending the basis of $1, \theta, \ldots, \theta^{n-1}$ of $\mathfrak{O}$ into the basis $1, \lambda, \ldots, \lambda^{n-1}$ of $\mathfrak{O}'$ is $(\mathfrak{O} : \mathfrak{O}')$. By definition, $z(X_0, \ldots, X_{n-1})$ is this determinant. Therefore

$$(\mathfrak{O} : \mathfrak{O}') = \pm z(X_0, \ldots, X_{n-1}). \tag{18}$$

Hence we have the following theorem.

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

1. $\mathfrak{O} = \mathfrak{O}'$,
2. $z(X_0, \ldots, X_{n-1}) = \pm 1$,
3. *$y(X_1, \ldots, X_{n-1}; \theta)$ is a unit in $Z[\theta]$ with norm $+1$.*

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

$$y(X_1, \ldots, X_{n-1}; \theta) = f'_\lambda(\lambda)/f'_\theta(\theta)$$

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

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

Hence, we have again

$$[z(X_0, \ldots, X_{n-1})]^2 = \operatorname{norm}\big(y(X_1, \ldots, X_{n-1}; \theta)\big) = (\mathfrak{O} : \mathfrak{O}')^2.$$

CALIFORNIA INSTITUTE OF TECHNOLOGY

Reçu par la Rédaction le 27. 4. 1963