A NOTE TO THE PAPER ON INTEGRAL BASES
BY H. B. MANN

VIRGINIA HanLY AND H. B. MANN

The definitions and notation are those of (2). We shall prove the following theorem.

THEOREM. If \( \mathfrak{I} \) contains an ideal which is not principal then there exists a quadratic extension \( \mathfrak{I}' \) over \( \mathfrak{I} \) which has no integral basis over \( \mathfrak{I} \).

The theorem was proved in (2) for the case that \( \mathfrak{I} \) has characteristic different from 2. Here we shall give the proof in the case that \( \mathfrak{I} \) has characteristic 2.

Let \( \mathfrak{I} \) have characteristic 2 and let \( \mathfrak{I}' = \mathfrak{I}(\theta) \) where \( \theta^2 + b\theta + c = 0 \); \( b, c \in \mathfrak{I}, b \neq 0 \). Every \( \alpha \in \mathfrak{I}' \) may be written as \( y_0 + y_1\theta \); \( y_0, y_1 \in \mathfrak{I} \). If \( \alpha \) is integral then \( T(\alpha) = by_1 \) and \( T(\alpha\theta) + y_1b^2 = by_0 \) are integers. Hence we may write

\[
\alpha = \frac{x_0 + x_1\theta}{b}; \quad x_0, x_1 \in \mathfrak{I}.
\]

The integers \( x_1 \) appearing in these representations form an ideal \( a \) of \( \mathfrak{J} \).

LEMMA 1. We have \( a = b \), where \( b \) is the different of \( \mathfrak{I}' \) over \( \mathfrak{I} \).

PROOF. The ideal \( a \) is the g.c.d. of all traces of elements in \( \mathfrak{I}' \). Hence \( b \equiv 0 \pmod{a} \). On the other hand \( a \) is also the g.c.d. of all differents of elements of \( \mathfrak{I}' \) since \( \mathfrak{I} \) has characteristic 2. Hence \( a \equiv 0 \pmod{d} \) and so \( a = b \). (The proof of Lemma 11.5.1 of (1) carries over without change to any Dedekind ring.)

LEMMA 2. Let \( \mathfrak{I} \) have characteristic 2 and let \( q \) be any squarefree ideal of \( \mathfrak{I} \). There exists a quadratic extension \( \mathfrak{I}' \) over \( \mathfrak{I} \) whose different over \( \mathfrak{I} \) is \( q \).

PROOF. We determine \( q' \) so that \( (q', q') = 1 \) and \( q'q = (b), b \in \mathfrak{I} \) and \( q'' \) so that \( (b, q'') = 1 \) and \( q''q = (c), c \in \mathfrak{I} \) and \( c \equiv b + 1 \pmod{q''} \). The polynomial \( x^2 + bx + c \) is irreducible by Eisenstein's criterion. If \( \theta \) is one of its roots then \( \alpha = (y + \theta x)/b \), \( x, y \in \mathfrak{I} \) is integral if and only if \( N(\alpha) \) is integral, hence if and only if

\[
x^2c + bxy + y^2 \equiv 0 \pmod{b^2}.
\]

By Lemma 1 \( b \) is the g.c.d. of all \( x \) for which (1) has a solution \( y \in \mathfrak{I} \).

Received by the editors May 28, 1957.

173
We then have $y \equiv 0 \pmod{q}$, hence $x \equiv 0 \pmod{q}$. On the other hand for $x = y \equiv 0 \pmod{q}$ we have by our construction of $b$ and $c$

\begin{align*}
x^2(c + b + 1) &\equiv 0 \pmod{q^2}, \\
x^2(c + b + 1) &\equiv 0 \pmod{q^2},
\end{align*}

whence $x^2(c + b + 1) \equiv 0(b^2)$ and therefore $b = q$.

Our theorem now follows easily from Lemma 2 and Theorem 5 of (2).

References


The Ohio State University