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 $\mathfrak{J}$ contains an ideal which is not principal then there exists a quadratic extension $\mathfrak{F}'$ over $\mathfrak{F}$ which has no integral basis over $\mathfrak{F}$.*

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

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

$$\alpha = \frac{x_0 + x_1\theta}{b}; \qquad x_0, x_1 \in \mathfrak{J}.$$

The integers x_1 appearing in these representations form an ideal a of J.

LEMMA 1. *We have $\mathfrak{a}=\mathfrak{d}$, where $\mathfrak{d}$ is the different of $\mathfrak{F}'$ over $\mathfrak{F}$.*

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

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

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

$$x^2c + bxy + y^2 \equiv 0 \pmod{b^2}. \tag{1}$$

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

Received by the editors May 28, 1957.

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

$$x^2(c + b + 1) \equiv 0 \pmod{\mathfrak{q}^2},$$
$$x^2(c + b + 1) \equiv 0 \pmod{\mathfrak{q}'^2},$$

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

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

References

1. H. B. Mann, *Introduction to algebraic number theory*, The Ohio State University Press, Columbus, 1955.

2. ———, *On integral bases*, Proc. Amer. Math. Soc. vol. 9 (1958) pp. 167–172.

The Ohio State University