ON ISOMORPHISMS OF ORDERS

D. G. Higman

1. INTRODUCTION

Let there be given a commutative ring $\mathfrak{o}$ with identity element, and an $\mathfrak{o}$-algebra $\mathfrak{O}$. As in [2], we denote by $I(\mathfrak{O})$ the ideal consisting of the elements of $\mathfrak{o}$ which annihilate the cohomology groups $H^1(\mathfrak{O}, T)$ for all two-sided $\mathfrak{O}$-modules T (cohomology being taken in the sense of $\mathfrak{o}$-algebras [1, Chapter IX]). There is a reduction theorem [1] stating that for $n > 1$, $H^n(\mathfrak{O}, T) = H^{n-1}(\mathfrak{O}, T')$ for a suitable two-sided $\mathfrak{O}$-module T'. Hence $H^n(\mathfrak{O}, T)$ is annihilated by $I(\mathfrak{O})$ for all $n > 0$.

In case $\mathfrak{o}$ is an integral domain with quotient field k, an $\mathfrak{o}$-algebra $\mathfrak{O}$ is called an *$\mathfrak{o}$-order* if it is finitely generated and torsion-free as an $\mathfrak{o}$-module. We shall call an $\mathfrak{o}$-order $\mathfrak{O}$ *separable* if its k-hull $\mathfrak{O} \otimes_{\mathfrak{o}} k$ is a separable k-algebra; a necessary and sufficient condition for this is that $I(\mathfrak{O})$ be different from 0 [2]. When $\mathfrak{O}$ is a group ring of a finite group of order N, $I(\mathfrak{O}) = N\mathfrak{o}$.

If $\mathfrak{o}$ is the valuation ring and $\mathfrak{p}$ the prime ideal of a field k with a discrete valuation, every non-zero ideal is a power of $\mathfrak{p}$, and therefore, for a separable $\mathfrak{o}$-order $\mathfrak{O}$, $I(\mathfrak{O}) = \mathfrak{p}^s$ with $s \geq 0$. We call s the *depth* of $\mathfrak{O}$.

Two $\mathfrak{o}$-orders are called *isomorphic* if there is an $\mathfrak{o}$-algebra isomorphism of the one onto the other. The purpose of this note is to prove the

THEOREM. *Let $\mathfrak{o}$ be the valuation ring and $\mathfrak{p}$ the prime ideal of a field k complete with respect to a discrete valuation. A separable $\mathfrak{o}$-order $\mathfrak{O}$ is isomorphic with an $\mathfrak{o}$-order $\mathfrak{Q}$ if and only if the $\mathfrak{o}/\mathfrak{o}\,\mathfrak{p}^{2s+1}$-algebras $\mathfrak{O}/\mathfrak{p}^{2s+1}\mathfrak{O}$ and $\mathfrak{Q}/\mathfrak{p}^{2s+1}\mathfrak{Q}$ are isomorphic.*

Our proof is simplified following a suggestion of the referee. The theorem reduces the problem of isomorphism of orders over complete, discrete valuation rings having finite residue class rings to a problem concerning finite algebras. Thus an immediate consequence is the

COROLLARY 1. *If $\mathfrak{o}$ as in the Theorem has finite residue class rings, there are only finitely many non-isomorphic separable $\mathfrak{o}$-orders of given finite rank and depth.*

A second corollary, concerning *genera* of orders in a separable algebra over the quotient field of a Dedekind domain $\mathfrak{o}$, is given. Here two $\mathfrak{o}$-orders are put in the same genus if their $\mathfrak{p}$-adic completions are isomorphic for each prime $\mathfrak{p}$ of $\mathfrak{o}$.

2. PROOF OF THE THEOREM

We are assuming that $\mathfrak{o}$ is the valuation ring and $\mathfrak{p}$ the prime ideal of a field k with a complete discrete valuation. Since the valuation ring $\mathfrak{o}$ is a principal ideal domain, the $\mathfrak{o}$-orders $\mathfrak{O}$ and $\mathfrak{Q}$ have free $\mathfrak{o}$-module bases. Hence an isomorphism $\mathfrak{O}/\mathfrak{p}^{2s+1}\mathfrak{O} \approx \mathfrak{Q}/\mathfrak{p}^{2s+1}\mathfrak{Q}$ is induced by an $\mathfrak{o}$-module isomorphism $\alpha\colon \mathfrak{O} \approx \mathfrak{Q}$ such that

(1) $$\alpha(xy) \equiv \alpha(x)\alpha(y) \pmod{\mathfrak{p}^{2s+1}}.$$

Received October 30, 1958.

To construct an $\mathfrak{o}$-algebra isomorphism of $\mathfrak{O}$ onto $\mathfrak{Q}$, we first construct inductively $\mathfrak{o}$-module homomorphisms $\alpha_i: \mathfrak{O} \to \mathfrak{Q}$ $(i = 1, 2, \cdots)$ such that

$$\alpha_i(xy) \equiv \alpha_i(x)\alpha_i(y) \pmod{\mathfrak{p}^{2s+i}} \tag{2}$$

and

$$\alpha_{i+1} \equiv \alpha_i \pmod{\mathfrak{p}^{s+i}}. \tag{3}$$

Because of (1), we may take $\alpha_1 = \alpha$. Assume that α_i has been defined for some $i \geq 1$. Since $2s + i \geq s + 1$, (2) implies that α_i induces an $\mathfrak{o}$-algebra homomorphism of $\mathfrak{O}$ into $T = \mathfrak{Q}/\mathfrak{p}^{s+1}\mathfrak{Q}$. Hence T is a two-sided $\mathfrak{O}$-module. Now we define $f \in \mathrm{Hom}_{\mathfrak{o}}(\mathfrak{O} \otimes_{\mathfrak{o}} \mathfrak{O}, \mathfrak{Q})$ by

$$f(x \otimes y) = \alpha_i(xy) - \alpha_i(x)\alpha_i(y). \tag{4}$$

The associative law in $\mathfrak{O}$ gives

$$\alpha_i(x) f(y \otimes z) - f(xy \otimes z) + f(x \otimes yz) - f(x \otimes y)\alpha_i(z).$$

By (2),

$$f = \pi^{2s+i} g, \tag{5}$$

where π is a generator of $\mathfrak{p}$, and clearly g must satisfy the same identity as f. This means that the $\mathfrak{o}$-module homomorphism $g^*: \mathfrak{O} \otimes_{\mathfrak{o}} \mathfrak{O} \to T$ induced by g is a 2-cocycle. But $I(\mathfrak{O}) = \mathfrak{p}^s$ annihilates $H^2(\mathfrak{O}, T)$, and therefore $\pi^s g^*$ is a coboundary. It follows that there exists an $h \in \mathrm{Hom}_{\mathfrak{o}}(\mathfrak{O}, \mathfrak{Q})$ such that $\pi^s g \equiv \delta_i h \pmod{\mathfrak{p}^{s+1}}$, where

$$\delta_i h(x \otimes y) = \alpha_i(x) h(y) - h(xy) + h(x)\alpha_i(y).$$

Hence by (5),

$$f \equiv \pi^{s+i}(\delta_i h) \pmod{\mathfrak{p}^{2s+i+1}}. \tag{6}$$

Now let $\alpha_{i+1} = \alpha_i + \pi^{s+i}h$. Since $2(s+1) \geq 2s + i + 1$, (4) and (6) give

$$\begin{aligned}
\alpha_{i+1}(xy) &= \alpha_i(xy) + \pi^{s+i}h(xy) \\
&= \alpha_i(x)\alpha_i(y) + f(x \otimes y) + \pi^{s+i}h(xy) \\
&\equiv \alpha_i(x)\alpha_i(y) + \pi^{s+i}\{\alpha_i(x)h(y) + h(x)\alpha_i(y)\} \\
&\equiv (\alpha_i(x) + \pi^{s+i}h(x))(\alpha_i(y) + \pi^{s+i}h(y)) \\
&\equiv \alpha_{i+1}(x)\alpha_{i+1}(y) \pmod{\mathfrak{p}^{2s+i+1}}.
\end{aligned}$$

The inductive definition of the α_i satisfying (2) and (3) is now complete.

Because of (3), we may define an $\mathfrak{o}$-module homomorphism $\alpha^*: \mathfrak{O} \to \mathfrak{Q}$ by

$$\alpha^*(x) = \mathrm{Lim}\, \alpha_i(x).$$

Then (2) implies that α^* is a ring homomorphism. Since by (3) $\alpha^* \equiv \alpha_1 \pmod{\mathfrak{p}}$, and since $\alpha_1 = \alpha$ is an $\mathfrak{o}$-module isomorphism onto, it follows that α^* is one-to-one and onto.

The converse is immediate, and therefore the theorem is proved.

3. AN APPLICATION

Given a prime ideal $\mathfrak{p}$ of a Dedekind domain $\mathfrak{o}$ with quotient field k, we shall denote by $\mathfrak{o}_{\mathfrak{p}}$ the valuation ring in the $\mathfrak{p}$-adic completion $k_{\mathfrak{p}}$ of k. We shall call two $\mathfrak{o}$-orders $\mathfrak{O}$ and $\mathfrak{Q}$ *isomorphic at* $\mathfrak{p}$ if the $\mathfrak{o}_{\mathfrak{p}}$-orders $\mathfrak{O}_{\mathfrak{p}} = \mathfrak{O} \otimes_{\mathfrak{o}} \mathfrak{o}_{\mathfrak{p}}$ and $\mathfrak{Q}_{\mathfrak{p}} = \mathfrak{Q} \otimes_{\mathfrak{o}} \mathfrak{o}_{\mathfrak{p}}$ are isomorphic. We shall put $\mathfrak{O}$ and $\mathfrak{Q}$ in the same *genus* if they are isomorphic at every prime $\mathfrak{p}$ of $\mathfrak{o}$.

If $\mathfrak{O}$ is a separable $\mathfrak{o}$-order, the discriminant $\Delta(\mathfrak{O})$ is a non-zero ideal of $\mathfrak{o}$ [3].

An $\mathfrak{o}$-order having a k-algebra A as k-hull is called an $\mathfrak{o}$*-order in* A.

COROLLARY 2. *Let* A *be a separable algebra over the quotient field* k *of a Dedekind domain* $\mathfrak{o}$ *having finite residue class rings. Let* $\mathfrak{a}$ *be a non-zero ideal of* $\mathfrak{o}$. *Then there are only a finite number of genera of* $\mathfrak{o}$*-orders* $\mathfrak{O}$ *in* A *such that* $I(\mathfrak{O}) \cap (\mathfrak{O}) = \mathfrak{a}$.

Proof. Since $\Delta(\mathfrak{O}_{\mathfrak{p}})$ is the $\mathfrak{p}$-component of $\Delta(\mathfrak{O})$ [3], $\Delta(\mathfrak{O}_{\mathfrak{p}}) = \mathfrak{o}_{\mathfrak{p}}$ for every prime $\mathfrak{p}$ of $\mathfrak{o}$ not dividing $\Delta(\mathfrak{O})$, and in particular for every $\mathfrak{p}$ not dividing $\mathfrak{a}$. Hence $\mathfrak{O}_{\mathfrak{p}}$ is a maximal $\mathfrak{o}_{\mathfrak{p}}$-order in $A_{\mathfrak{p}} = A \otimes_k k_{\mathfrak{p}}$ for every $\mathfrak{p}$ not dividing $\mathfrak{a}$ [3]. But any two maximal $\mathfrak{o}_{\mathfrak{p}}$-orders in $A_{\mathfrak{p}}$ are isomorphic. Hence, if $h_{\mathfrak{p}}$ is the number of classes under isomorphism at $\mathfrak{p}$ of $\mathfrak{o}$-orders $\mathfrak{O}$ in A such that $I(\mathfrak{O}) \cap (\mathfrak{O}) = \mathfrak{a}$, then $h_{\mathfrak{p}} = 1$ when $\mathfrak{p}$ does not divide $\mathfrak{a}$.

Since $I(\mathfrak{O}_{\mathfrak{p}})$ is easily seen [2] to be the $\mathfrak{p}$-component of $I(\mathfrak{O})$, the depth of $\mathfrak{O}_{\mathfrak{p}}$ is the exponent of the highest power of $\mathfrak{p}$ dividing $I(\mathfrak{O})$, and so is no larger than the exponent of the highest power of $\mathfrak{p}$ dividing $\mathfrak{a}$. Hence by Corollary 1, $h_{\mathfrak{p}}$ is finite for every $\mathfrak{p}$, under our assumption that $\mathfrak{o}$ has finite residue class rings. The number g of genera of $\mathfrak{o}$-orders $\mathfrak{O}$ in A such that $I(\mathfrak{O}) \cap (\mathfrak{O}) = \mathfrak{a}$ is given by $g = \prod_{\mathfrak{p} | \mathfrak{a}} h_{\mathfrak{p}}$. Hence g is finite.

REFERENCES

1. H. Cartan and S. Eilenberg, *Homological algebra,* Princeton, 1956.

2. D. G. Higman, *On orders in separable algebras,* Canadian J. Math. 7 (1955), 509-515.

3. W. E. Jenner, *Block ideals and arithmetics of algebras,* Compositio Math. 11 (1953), 187-203.

The University of Michigan