MATH. SCAND. 29 (1971), 50–54

# A PRODUCT THEOREM FOR LATTICES OVER ORDERS

MICHAEL SINGER

In [5], to which the reader may refer for further background to this paper, we proved a product theorem for ideals over orders, which in this paper we generalise to treat lattices over orders. Our earlier theorem is not required in the proof. Indeed, in sharp contrast to previous expositions, we have found it possible to confine ourselves to the most elementary methods throughout.

Roiter's concept of divisibility of lattices [4] immediately suggests a possible generalisation of our theorem, but we show that this suggested generalisation is false.

Let $R$ be a Dedekind domain, to avoid trivial exceptions not a field, with quotient field $K$. Let $A$ be a finite-dimensional commutative separable $K$-algebra. An *$A$-$R$-lattice*, $M$, is a finitely generated projective $R$-module, with the provision of $A$-module structure on $M \otimes_R K$. $M$ is an *$A$-$R$-ideal* in $A$ if it is further contained in $A$ and $KM = A$.

Let $M, N$ be $A$-$R$-lattices spanning the same $K$-module. We remind the reader of the definition of the *module index* of $N$ in $M$, denoted by $[M:N]$. If $R$ is a principal ideal domain, $M$ and $N$ are $R$-free, and the module index is the $R$-fractional ideal generated by the determinant of any $R$-linear transformation from $M$ onto $N$. In general, we have a module index at each prime of $R$, and $[M:N]$ is defined to be the fractional ideal of $R$ determined by these local ideals.

Let $\mathfrak{B}$ denote the maximal order in $A$ over $R$. The index $[\mathfrak{B}M:M]$ is of considerable interest, and is closely related to the *defect* of $M$, $\mathfrak{a}(M)$, defined in [2]. In fact, the defect is the square of this module index, multiplied by a factor which depends only on $R$, $A$ and the $K$-module spanned by $M$, and not on $M$ itself. This factor is chosen so that $\mathfrak{a}(M)$ shall be invariant under finite separable extension of $K$.

Let $M$ be an $A$-$R$-lattice, and let $J$ be an $A$-$R$-ideal in $A$. Denoting by "$\sim$" local isomorphism of $A$-$R$-lattices, we prove here the following

THEOREM. $\mathfrak{a}(JM) \mid \mathfrak{a}(M)$, *with equality if and only if* $JM \sim M$.

Received March 15, 1971.

This theorem generalises two earlier results. In [2], Fröhlich proved that $\mathfrak{a}(JM)|\mathfrak{a}(M)$ when $M\otimes_R K$ is $A$-free. In [5] we proved the whole theorem for the case when $M$ is an $A$-$R$-ideal in $A$.

LEMMA 1. *We can assume that from now on $R$ is a discrete valuation ring, with prime ideal $\mathfrak{p}$.*

PROOF. Obvious.

Now let $L$ be a finite separable extension field of $K$, with ring of integers $S$ over $R$. We shall identify $A$ with $A\otimes_K K$, so $A$ is embedded in $AL=A\otimes_K L$ in a natural fashion. If $M$ is an $A$-$R$-lattice, we identify the $AL$-$S$-lattices $MS=M\otimes_R S$. The next lemma can hardly be new, but our proof is rather simple.

LEMMA 2. *If $M$ is an $S$-$R$-lattice, then $M=MS\cap KM$.*

PROOF. Certainly $M\subseteqq MS\cap KM$, and $(MS\cap KM)S\subseteqq MS$. So

$$(MS\cap KM)S = MS\,.$$

In case $MS\cap KM$ is not finitely generated as $R$-module, let $N$ be an $A$-$R$-lattice with $M\subseteqq N\subseteqq MS\cap KM$. Then

$$MS \subseteqq NS \subseteqq (MS\cap KM)S = MS\,,$$

so $MS=NS$. But introducing module indices,

$$[N:M]S = [NS:MS] = S\,,$$

and so $[N:M]=R$. But $M\subseteqq N$, so $M=N$. Hence $MS\cap KM$ must be finitely generated as $R$-module, and so in the above we may take $N=MS\cap KM$.

The following lemma can be compared with [3] and [2, Appendix B].

LEMMA 3. *Let $J$ be an $A$-$R$-ideal. Then there is a finite separable extension field $L$ of $K$, with ring of integers $S$ over $R$, such that $JS\cong T$, where $T$ is an $AL$-$S$-lattice with $1\in T\subseteqq\mathfrak{B}_L$, and where $\mathfrak{B}_L$ is the maximal order in $AL$ over $S$.*

PROOF. Let $E$ be a finite separable splitting field for $A$ over $K$. Suppose that $(A:K)=n$, and take $L$ to be any finite separable extension field of $E$, such that the residue class field of $S$ has cardinality at least $n$. In particular, $L$ can be any sufficiently large finite separable non-ramified extension of $E$. We shall prove the existence of an element $u\in AL$ such that $1\in uJS\subseteqq\mathfrak{B}_L$.

To simplify notation we assume that in fact $R/\mathfrak{p}$ has cardinality at least $n$, and that $A$ splits over $K$, with maximal order $\mathfrak{B}$ over $R$. Multi-

plying $J$ by a suitable element of $A$, we may assume that $\mathfrak{B}J = \mathfrak{B}$, and we must prove now that there is an element $y \in J$ with $y\mathfrak{B} = \mathfrak{B}$. For then $1 \in y^{-1}J \subseteq \mathfrak{B}$.

Let $e_1, \ldots, e_n$ denote the primitive idempotents of $A$. For some $i$, $1 \leqq i < n$, suppose we have found an element $y_i \in J$ such that $y_i e_j$ is a unit in $Re_j$, $1 \leqq j \leqq i$. Using induction on $i$, it is enough for the proof of the lemma to find a suitable element $y_{i+1} \in J$. We can suppose that $y_i e_j$ is not a unit in $Re_j$ for $j > i$. We write

$$y_i = \sum_{j=1}^{i} \alpha_j e_j + \xi ,$$

with $\xi \in \mathfrak{p}\mathfrak{B}$ and the $\alpha_j$ units in $R$. Let $x \in J$ with $xe_{i+1}$ a unit in $Re_{i+1}$. We write

$$x = \sum_{j=1}^{i+1} \beta_j e_j + \eta ,$$

with $\eta \in \mathfrak{p}\mathfrak{B}$ and the $\beta_j$ in $R$ with $\beta_{i+1}$ a unit. Let $\partial$ run through a set of representatives of $R/\mathfrak{p}$ in $R$. For each $j$, $1 \leqq j \leqq i$,

$$\beta_j - \partial\alpha_j \in \mathfrak{p}$$

if and only if

$$\partial \in \beta_j \alpha_j^{-1} + \mathfrak{p} ,$$

and this can occur for at most one value of $\partial$. Since

$$i \leqq n - 1 < \operatorname{card}(R/\mathfrak{p}) ,$$

there is some unit $\partial$ such that $\beta_j - \partial\alpha_j$ is a unit in $R$ for $1 \leqq j \leqq i$; also, this is certainly the case for $j = i+1$. So $x - \partial y_i \in J$ will serve as our $y_{i+1}$, as required.

Proof of the Theorem. With $L$ as in Lemma 3 let $u \in AL$ with

$$1 \in uJS \subseteq \mathfrak{B}_L ,$$

where $\mathfrak{B}_L$ is again the maximal order in $AL$ over $S$. Hence

$$MS \subseteq uJMS \subseteq \mathfrak{B}_L MS = \mathfrak{B}_L uJMS .$$

So

$$[\mathfrak{B}_L uJMS : uJMS] \mid [\mathfrak{B}_L MS : MS] ,$$

or, equivalently

$$\mathfrak{a}(JMS) \mid \mathfrak{a}(MS) ,$$

with equality if and only if

$$uJMS = MS .$$

Now $\mathfrak{a}(MS)=\mathfrak{a}(M)S$, so we have proved that $\mathfrak{a}(JM)\,|\,\mathfrak{a}(M)$. Suppose that $\mathfrak{a}(JM)=\mathfrak{a}(M)$; then $\mathfrak{a}(JMS)=\mathfrak{a}(MS)$, so $uJMS=MS$.

At this stage we could appeal to a relatively deep result due to Zassenhaus and Reiner, quoted for the case when $K$ is an algebraic number field in [1, p. 538]. We are however able to give a direct elementary exposition. Note that some such approach is needed for reduction to the split case in [5], which is otherwise incomplete on this point.

Some power (and any higher power) of $J$ is invertible. This appears in [2] as a Corollary to the product theorem there, but is in fact a quite elementary result. For consider the ideals $(uJS)^q$, $q=1,2,\ldots$, in $AL$ over $S$. They form an increasing sequence since $1\in uJS$, and all terms are contained in $\mathfrak{B}$. It follows readily that from some point on all the terms are equal, and indeed equal to an order in $AL$. The corresponding $J^q$ are invertible by [2, Lemma 5.1]. Thus there is a positive integer $r$, an order $\mathfrak{A}$ in $A$ and elements $v,w$ in $A$ such that $J^r=v\mathfrak{A}$, $J^{r+1}=w\mathfrak{A}$. But by induction, $u^rJ^rMS=MS$, and if $\mathfrak{O}_R(M)$ denotes the order of $M$ in $A$ over $R$, we have

$$\mathfrak{O}_S(MS) = \mathfrak{O}_S(J^rMS) \supseteq \mathfrak{O}_S(J^rS) = \mathfrak{A}S\,.$$

So

$$MS = u^rv\mathfrak{A}MS = u^rvMS\,.$$

Similarly

$$MS = u^{r+1}wMS\,.$$

Hence $u^{-1}MS=(v^{-1}wM)S=JMS$. So by Lemma 2,

$$v^{-1}wM=JM\,.$$

Thus $JM\cong M$.

According to Roiter's definition [4], the $A$-$R$-lattice $M$ *divides* the $A$-$R$-lattice $N$, written $M\succ N$, if the lattice

$$M.\mathrm{HOM}_{A-R}(M,N) = \{\textstyle\sum m\alpha : m\in M,\ \alpha\in \mathrm{HOM}_{A-R}(M,N)\}$$

is equal to $N$.

Certainly $M\succ JM$ for every ideal $J$ in $A$. This suggests the generalisation: if $M,N$ are $A$-$R$-lattices spanning the same $K$-module with $M\succ N$, does the theorem still hold with $N$ in place of $JM$? Unfortunately, as the following example shows, it does not.

Let $M$ span $A+A$ (external direct sum), and be of the form $U+V$, with $U,V$ ideals in $A$. Let $\alpha$ be the $A$-automorphism of $A+A$ which transposes the two summands. Take $N=M+M\alpha$, so certainly $M\succ N$.

Now $N=(U+V)+(U+V)$. The relation $\mathfrak{a}(N)\subset\mathfrak{a}(M)$ (strict inclusion)

which gives our counterexample, will certainly hold if the ideals $U, V$ satisfy

$$\mathfrak{a}(U+V) \subset \mathfrak{a}(U), \quad \mathfrak{a}(U+V) \subset \mathfrak{a}(V),$$

so we are reduced to finding ideals in $A$ satisfying this.

Let $R$ be a local ring, with prime ideal $\mathfrak{p}$. Let $A$ be split with dimension 3 over $K$. Let $g, h, e$ denote the primitive idempotents. Let

$$U = \{\mathfrak{p}^3 g + \mathfrak{p}^3 h + R(g+h+e)\}^*, \quad V = \{\mathfrak{p}^4 g + \mathfrak{p}(g+h) + Re\}^*.$$

Now

$$U+V = (U^* \cap V^*)^* = \{\mathfrak{p}^4 g + \mathfrak{p}^3(g+h) + \mathfrak{p}(g+h+e)\}^*.$$

An easy direct calculation now gives

$$[\mathfrak{B}U:U] = [\mathfrak{B}V:V] = \mathfrak{p}^3, \quad [\mathfrak{B}(U+V):(U+V)] = \mathfrak{p}^4.$$

**Acknowledgements.** The author wishes to extend his thanks to Chalmers University of Technology and University of Göteborg for their hospitality, and to Professor Heinz Jacobinski for several helpful comments.

## REFERENCES

1. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras* (Pure and Appl. Math. 11), Interscience Publishers, New York · London, 1962.
2. A. Fröhlich, *Invariants for modules over commutative separable orders*, Quart. J. Math. Oxford Ser. (2) 16 (1965), 193–232.
3. H. E. Gorman, *Invertibility of modules over prüfer rings*, Ph. D. Thesis, University of Chicago, 1968.
4. A. V. Roiter, *Categories with division and integral representations*, Dokl. Akad. Nauk SSSR 153 (1963), 46–48 (= Soviet Math. Dokl. 4 (1963), 1621–1623).
5. M. Singer, *A product theorem for ideals over orders*, Proc. Cambridge Philos. Soc. 68 (1970), 17–20.

CHALMERS UNIVERSITY OF TECHNOLOGY AND UNIVERSITY OF GÖTEBORG, SWEDEN