ON EXTENSIONS OF LATTICES

H. Jacobinski

Let k be an algebraic number field of finite degree, o a Dedekind-ring with quotient field k, Γ/k a finite-dimensional semi-simple algebra over k, and R an o-order in Γ. We consider R-lattices M, N, that is, finitely generated unitary R-modules that are torsion-free as o-modules. D. G. Higman has constructed an ideal $i(R) \neq 0$ in o such that $i(R)\, \mathrm{Ext}^1_R(M, N) = 0$ for all R-lattices M and N (see Curtis and Reiner [1, p. 522]). In particular, if G is a group of order n and $R = oG$, then $i(R) = (n)$. A refinement of this has been established by Reiner [3]: If kM or kN affords an absolutely irreducible representation of G of degree m, then

$$\frac{n}{m}\, \mathrm{Ext}^1_R(M, N) = 0 .$$

In this note, by embedding R in a maximal order $\mathfrak{O}$, we construct an ideal F(R) in the center of R that annihilates $\mathrm{Ext}^1_R(M, N)$ for arbitrary R-lattices M and N. The corresponding o-ideal $f(R) = F(R) \cap o$ may be a proper divisor of i(R) and may even contain fewer prime ideals. An even better annihilator of $\mathrm{Ext}^1_R(M, N)$ may be constructed if kM or kN does not afford a faithful representation of Γ, that is, if $eM = M$ or $eN = N$ for some central idempotent $e \neq 1$ in Γ. For the case where $R = oG$ is the group ring of a finite group, we shall derive explicit expressions for these annihilators; our expressions include the above-mentioned result of Reiner as a special case.

1. Let C be the maximal order in the center of Γ, and let $\mathfrak{O}$ be a maximal order in Γ that contains R. We define the central conductor to be

$$F(\mathfrak{O}/R) = \{z \mid z\mathfrak{O} \subset R,\ z \in C\} .$$

Since C is contained in every maximal order of Γ, the central conductor is an ideal in C. Now let $\mathfrak{O}$ range over all maximal orders in Γ that contain R, and let F(R) be the C-ideal generated by all the central conductors of R.

THEOREM 1. *For arbitrary* R-*lattices* M *and* N,

$$F(R)\, \mathrm{Ext}^1_R(M, N) = 0 .$$

Proof. Let

$$0 \to A \to B \to M \to 0$$

be an exact sequence of R-lattices, where B is projective. Put $kB = k \otimes_o B$, and regard A and B as submodules of kB. Since M is a torsion-free o-module, A is a primitive o-submodule of B; that is, $kA \cap B = A$. Let $\mathfrak{O}$ be a maximal order containing R; then $\mathfrak{O}B$ is the minimal $\mathfrak{O}$-lattice containing B. Now $kA \cap \mathfrak{O}B = \overline{A}$ is an $\mathfrak{O}$-lattice and at the same time a primitive o-submodule of $\mathfrak{O}B$. This implies

Received December 3, 1965.

that $X = \mathfrak{O}B/\overline{A}$ is an $\mathfrak{O}$-lattice. But since $\mathfrak{O}$ is hereditary, every $\mathfrak{O}$-lattice is a projective $\mathfrak{O}$-module. Therefore

$$(*) \qquad \mathfrak{O}B = \overline{A} \oplus X.$$

Let $z \in F(\mathfrak{O}/R)$ and $\phi \in \mathrm{Hom}_R(A, N)$. To prove the theorem, we have to show that $z\phi$ can be extended to an R-homomorphism $B \to N$. Now $z\mathfrak{O} \subset R$ implies $z\mathfrak{O}B \subset B$ and $z\overline{A} \subset B \cap kA = A$. Consequently, $z\phi$ induces an R-homomorphism $\overline{A} \to N$. Since $\overline{A}$ is a direct summand of $\mathfrak{O}B$, $z\phi$ can be extended to an R-homomorphism $\mathfrak{O}B \to N$. Since $B \subset \mathfrak{O}B$, this proves the theorem.

THEOREM 2. *Let* e *be a central idempotent of* Γ, *and define the* o-*ideal* $f_e(R) = \{z \mid ez \in F(R), z \in o\}$. *If* M *and* N *are* R-*lattices with* $eM = M$ *or* $eN = N$, *then*

$$f_e(R)\,\mathrm{Ext}^1_R(M, N) = 0.$$

Proof. Suppose first that $eN = N$. Then $(1 - e)\mathrm{Hom}_R(Q, N) = 0$ for every R-lattice Q. If in the exact sequence above, B is taken to be a projective R-module, $\mathrm{Ext}^1_R(M, N)$ is isomorphic to a factor module of $\mathrm{Hom}_R(A, N)$. This shows that $(1 - e)\mathrm{Ext}^1_R(M, N) = 0$. Since the elements of $f_e(R)$ are of the form $z = ze + z(1 - e)$ with $ze \in F(R)$, they clearly annihilate $\mathrm{Ext}^1_R(M, N)$.

Suppose next that $eM = M$. We first observe that $f_e(R)$ may be defined in a slightly different way, namely as the o-ideal generated by all $z \in o$ such that $ze\mathfrak{O} \subset R$ for some maximal order $\mathfrak{O} \supset R$. Let g be this ideal; then clearly $g \subset f_e(R)$. On the other hand, let p be a prime ideal in o, and suppose that $f_e(R)$ is exactly divisible by p^t. This means that there is a maximal order $\mathfrak{O} \supset R$ such that the ideal $eF(\mathfrak{O}/R) \cap eo$ in eo is exactly divisible by ep^t. Consequently, there exists a $z \in g$ that is not divisible by p^{t+1}, and so $g = f_e(R)$. To prove the theorem, we then have to show that for every maximal order $\mathfrak{O}$ containing R, $ze\mathfrak{O} \subset R$ with $z \in o$ implies $z\,\mathrm{Ext}^1_R(M, N) = 0$.

Consider the exact sequence above and the decomposition (*). From the relation $eM = M$ we deduce that $eX = X$ for $kM \cong kB/kA = k\mathfrak{O}B/k\overline{A} \cong kX$. Now $ze\mathfrak{O} \subset R$ implies $zX = zeX \subset ze\mathfrak{O}B \subset B$. Put $B' = B + X$; then there is an R-lattice $A' \subset \overline{A}$ such that $B' = A' \oplus X$. Further, $zX \subset B$ implies $zB' \subset B$, and so $zA' \subset B \cap kA = A$. If $\phi \in \mathrm{Hom}_R(A, N)$, then $z\phi$ induces a homomorphism $A' \to N$, which we may extend to a homomorphism $B' \to N$ by letting $X \to 0$. Since $B \subset B'$, this proves the theorem.

2. If $R = oG$ is the group ring over o of a group of order n, the ideals F(R) and $f_e(R)$ may be calculated explicitly. Let $\mathfrak{O}$ be a maximal order in kG that contains $R = oG$, and denote by $L(\mathfrak{O}/R) = \{x \mid \mathfrak{O}x \subset R, x \in \mathfrak{O}\}$ the left conductor of R in $\mathfrak{O}$. Then $L(\mathfrak{O}/R)$ is the maximal left $\mathfrak{O}$-lattice contained in R. Obviously, $F(\mathfrak{O}/R) = L(\mathfrak{O}/R) \cap C$. We shall first determine $L(\mathfrak{O}/R)$, and then use this to determine F(R) and $f_e(R)$. Let

$$\Gamma = kG = \oplus \sum \Gamma_i$$

be the decomposition of Γ/k into simple algebras Γ_i/k, and let e_i be the corresponding central idempotents. Then there are analogous decompositions

$$C = \oplus \sum C_i \quad \text{and} \quad \mathfrak{O} = \oplus \sum \mathfrak{O}_i.$$

Let $s_i(x)$ be the reduced trace of Γ_i over its center kC_i, denote by $\mathfrak{D}_i$ the different of $\mathfrak{O}_i$ over C_i (with respect to s_i) and by D_i the different of C_i over oe_i, and put $D_i^{-1} \cap ke_i = d_i^{-1} e_i$. Then d_i is an ideal in o and $d_i e_i$ is the intersection of all ideals in oe_i that divide D_i. Finally, let n_i^2 be the degree of Γ_i over kC_i.

THEOREM 3. *If* $R = oG$ *is the group ring of a group* G *of order* n, *then*

$$L(\mathfrak{O}/R) = \oplus \sum \frac{n}{n_i} \mathfrak{D}_i^{-1} D_i^{-1}, \quad F(R) = \oplus \sum \frac{n}{n_i} D_i^{-1}, \quad f_e(R) = \bigcap_{ee_i \neq 0} \frac{n}{n_i} d_i^{-1}.$$

Proof. Denote by T(x) the trace of the regular representation of G; then $T(g) = 0$ for $g \neq 1$, and $T(1) = n$. For an o-lattice V in kG with $kV = kG$, let

$$\tilde{V} = \{x \mid T(Vx) \subset o, \ x \in kG\}$$

be the dual of V with respect to T(xy). Since T(xy) is nonsingular, the map $V \to \tilde{V}$ reverses proper inclusions. Moreover it takes right $\mathfrak{O}$-lattices into left ones and vice versa. If $V = R$, then

$$\tilde{R} = \frac{1}{n} R.$$

Let $\mathfrak{O}$ be a maximal order in kG with $oG \subset \mathfrak{O}$. Then $\tilde{R}\mathfrak{O} = \frac{1}{n}\mathfrak{O}$ is the minimal right $\mathfrak{O}$-lattice containing $\tilde{R}$, and so its dual is the maximal left $\mathfrak{O}$-lattice in R, which is $L(\mathfrak{O}/R)$. Consequently,

$$L(\mathfrak{O}/R) = n\tilde{\mathfrak{O}} = \oplus \sum n\tilde{\mathfrak{O}}_i.$$

On the other hand, $T(x) = \sum n_i S_i(x)$, where S_i is the reduced trace of Γ_i over k. This implies that

$$\tilde{\mathfrak{O}} = \oplus \sum n_i^{-1} \mathfrak{D}_i^{-1} D_i^{-1},$$

and from this one obtains the expression for $L(\mathfrak{O}/R)$. (It turns out that $L(\mathfrak{O}/R)$ is in fact a two-sided $\mathfrak{O}$-ideal and is at the same time the right conductor of R with respect to $\mathfrak{O}$.)

Now $F(\mathfrak{O}/R) = L(\mathfrak{O}/R) \cap C$. Since $\frac{n}{n_i} D_i^{-1}$ is already in kC_i, we have to determine $\mathfrak{D}_i^{-1} \cap kC_i$. This is clearly the inverse of an ideal Q_i in C_i. Suppose that $Q_i \neq C_i$, and let P be a prime divisor of Q_i and $\mathfrak{P}$ the indecomposable two-sided $\mathfrak{O}_i$-ideal dividing $P\mathfrak{O}_i$. Then $P\mathfrak{O}_i = \mathfrak{P}^\eta$, and since $\mathfrak{D}_i \subset Q_i \mathfrak{O}_i$, the different $\mathfrak{D}_i$ would be divisible by $\mathfrak{P}^\eta$. This gives a contradiction, since $\mathfrak{D}_i$ is exactly divisible by $\mathfrak{P}^{\eta-1}$ (see Deuring [2, p. 84, Satz 3, and p. 114, Satz 5]). Thus $Q_i = C_i$ and

$$F(\mathfrak{O}/R) = \oplus \sum \frac{n}{n_i} D_i^{-1}.$$

Since $F(\mathfrak{O}/R)$ does not depend on the choice of the maximal order $\mathfrak{O}$, it is equal to F(R). The expression for $f_e(R)$ now follows directly from the definition.

Remark: In the above proof, we only used the fact that R is the group ring of G over o to establish that $\tilde{R} = \frac{1}{n} R$. The same method of determining $L(\mathfrak{O}/R)$ and F(R) applies to any order R such that $\tilde{R}$ is generated as a left R-module by elements of the center kC.

The expression for $f_e(R)$ in Theorem 3 yields the following corollary.

COROLLARY. *If* e_i *is a central simple idempotent of* kG, *and if* M, N *are* oG-*lattices with* $e_i M = M$ *or* $e_i N = N$, *then*

$$\frac{n}{n_i} d_i^{-1} \operatorname{Ext}^1_{oG}(M, N) = 0 .$$

This generalizes the result of Reiner mentioned above.

3. In conclusion we comment on the relation between i(R) and $f(R) = F(R) \cap o$. The ideal i(R) may be calculated by means of an invariant bilinear form on Γ (Curtis and Reiner [1, p. 526, Theorem 75.19]). As such a form we take the reduced trace $S(xy) = \sum S_i(xy)$ of Γ over k. The associated Ikeda-Gaschütz operator is then

$$\gamma(x) = \sum s_i(x) = s(x),$$

where s_i is the reduced trace of Γ_i over kC_i. This is easily seen if each Γ_i is a full ring of matrices over k, by taking the usual matrix-units $e_{\mu,\nu}$ as a k-basis for Γ_i. We can reduce the general case to this by first extending k to a splitting field of Γ. Let R* be the dual of R with respect to S(xy), and put

$$U = \{x \mid R^* x \subset R,\ x \in \Gamma\} .$$

Then

$$i(R) = s(U) \cap o .$$

If R' is an order containing R, then we see from the above expression that $i(R) \subset i(R')$. In particular, if $\mathfrak{O}$ is a maximal order and $R \subset \mathfrak{O}$, then $i(R) \subset i(\mathfrak{O})$. Now, for a maximal order, we have the relations

$$\mathfrak{O}^* = \oplus \sum \mathfrak{D}_i^{-1} D_i^{-1}, \qquad U = \oplus \sum \mathfrak{D}_i D_i, \qquad s(U) = \oplus \sum D_i s_i(\mathfrak{D}_i) .$$

The dual of $\mathfrak{D}_i$ with respect to s_i is $\mathfrak{D}_i^{-2}$. Thus $s_i(\mathfrak{D}_i)$ is the intersection of all ideals Q in C_i such that $Q\mathfrak{O}_i \supset \mathfrak{D}_i^2$. If $\mathfrak{P}/\mathfrak{D}_i$ is a two-sided indecomposable ideal in $\mathfrak{O}_i$ and $P = \mathfrak{P} \cap C_i$, then $\mathfrak{P}^{\eta} = P\mathfrak{O}_i$ with $\eta > 1$, and $\mathfrak{D}_i^2$ is exactly divisible by $\mathfrak{P}^{2(\eta-1)} = P\mathfrak{P}^{\eta-2}$. Consequently, $s_i(\mathfrak{D}_i)$ is exactly divisible by P. This shows that $i(\mathfrak{O}) = \left\{ \oplus \sum s_i(\mathfrak{D}_i) D_i \right\} \cap o$ is divisible by all prime ideals p_ν in o that are either ramified in some C_i or else in some C_i contain a factor that is ramified in Γ_i. Thus, in general, $i(\mathfrak{O}) \neq (1)$, whereas $f(\mathfrak{O}) = (1)$. This provides an example in which i(R) contains unnecessary prime factors. Other examples may easily be constructed; for instance, let p be a prime ideal dividing $i(\mathfrak{O})$, and a be an ideal in o, not divisible by p. For $R = o + a\mathfrak{O}$, we have the relation $f(R) \supset a$, and so p does not divide f(R).

I do not know whether f(R) is always a divisor of i(R). If, however, for some maximal order $\mathfrak{O}$ with $R \subset \mathfrak{O}$ the left conductor $L = L(\mathfrak{O}/R)$ is a two-sided $\mathfrak{O}$-ideal, it is easy to show that f(R) divides i(R). We first observe that for a two-sided ideal $\mathfrak{A}$ in $\mathfrak{O}_i$

$$s_i(\mathfrak{A}) \subset \mathfrak{A} \cap C_i .$$

We may suppose that $\mathfrak{A}$ has no proper factor of the form $A\mathfrak{O}_i$ where A is an ideal in C_i. But then $\mathfrak{A}$ is a product of two-sided indecomposable ideals in $\mathfrak{O}_i$ that are all ramified over C_i. Since $\mathfrak{A}^* = \mathfrak{A}^{-1}\,\mathfrak{D}_i^{-1}$, we deduce that $s_i(\mathfrak{A})$ is the intersection of all ideals Q in C_i such that $Q\mathfrak{O}_i \supset \mathfrak{A}\,\mathfrak{D}_i$, and the assertion follows from the above-cited theorem concerning the exponent of an indecomposable ideal in $\mathfrak{D}_i$.

Now $\mathfrak{O}$ is the minimal right $\mathfrak{O}$-lattice containing R, and so its dual $\mathfrak{O}^*$ is the maximal left $\mathfrak{O}$-lattice in R^*. But then $\mathfrak{O}^* U \subset R^* U \subset R$, and $\mathfrak{O}^* U$ is a left $\mathfrak{O}$-lattice in R and therefore must be contained in $L = \bigoplus \sum L_i$. Since $\mathfrak{O}^* \supset \mathfrak{O}$, this implies that $U \subset \mathfrak{O}U \subset L$. From the above remark we see that

$$s(U) \subset \bigoplus \sum L_i \cap C_i \subset F(R),$$

and so $i(R) \subset f(R)$.

REFERENCES

1. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Interscience Publishers, New York, 1962.
2. M. Deuring, *Algebren.* Ergebnisse Math. Vol. 143, Springer, Berlin, 1935.
3. I. Reiner, *Extensions of irreducible modules*, Michigan Math. J. 10 (1963), 273-276.

University of Stockholm
Department of Mathematics