Can. J. Math., Vol. XLII, No. 2, 1990, pp. 342–364

THE REDUCTION OF AN RG-LATTICE MODULO p^n

PETER SYMONDS

1. Introduction. We define the cover of an RG-module V to consist of an RG-lattice $\tilde{V}$ and a homomorphism $\pi : \tilde{V} \longrightarrow V$ such that π induces an isomorphism on $\mathrm{Ext}^*_{RG}(M, -)$ for any RG-lattice M. Here G is a finite group and, for simplicity in this introduction, R is a complete discrete valuation ring of characteristic zero with prime element p and perfect valuation class field. Let $p^{n(G)}$ be the highest power of p that divides $|G|$ and, given an RG-lattice M, let $p^{n(M)}$ be the smallest power of p such that $p^{n(M)}\mathrm{id}_M : M \longrightarrow M$ factors through a projective lattice: $n(M) \leqq n(G)$. Then $\widetilde{M/p^n} \cong M \oplus \Omega^{-1}M$ if $n \geqq n(M)$, and we use this to analyze the endomorphism ring of M/p^n.

We can prove the following theorems, similar to those of Maranda [**5**].

THEOREM 1.1. *Suppose that M and N are RG-lattices, that $M/p^n \cong N/p^n$ and that $n(M) \geqq n(N)$.*

a) *If $n \geqq n(M) + 1$ then $M \cong N$.*

Suppose also that M is indecomposable and that $n \geqq 1$.

b) *If $n = n(M)$ then either $M \cong N$ or $M \cong \Omega N \cong \Omega^2 M$.*

c) *If $n = n(G)$ then $M \cong N$ unless p divides 2 and the Sylow, 2-subgroup of G is of order two.* (*cf.* 4.3, 4.4, 5.7 *in this paper.*)

THEOREM 1.2. *Let M be an indecomposable RG-lattice.*

a) *If $n \geqq n(M) + 1$ then M/p^n is indecomposable.*

b) *If $n = n(M)$ then either M/p^n is indecomposable or $M/p^n \cong A \oplus \Omega A$, where A is indecomposable.*

c) *If $n = n(G)$ then M/p^n is indecomposable.* (*cf.* 4.5, 4.9, 5.9.)

These results are sharper than those of [**5**], but, more importantly, our methods yield information about the endomorphism rings of these modules and about exact sequences.

THEOREM 1.3. *The reduced endomorphism ring $\overline{\mathrm{End}}(M/p^n)$ is independent of n for $n \geqq 2n(M)$.* (*cf.* 3.9.)

Note that the isomorphism between these rings for two different values of n is not induced by a homomorphism of the modules.

We can also obtain information easily about the number $n(M)$.

THEOREM 1.4. *For an absolutely indecomposable RG-lattice M, we have $n(M) = n(G)$ if and only if $\mathrm{rank}_R(M)$ is prime to p.* (*cf.* 5.3.)

Received November 1, 1988 and in revised form May 31, 1989.

2. The cover of a module. We shall always use R to denote a Dedekind domain of characteristic zero and G for a finite group. All RG-modules will be finitely generated. An RG-lattice is an RG-module that is projective over R. The category of RG-modules will be denoted by Mod(RG) and the full subcategory of RG-lattices by Lat(RG). If M and N are RG-modules then the trace map,

$$\mathrm{Tr}_G : \mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_{RG}(M, N),$$

is defined by

$$\mathrm{Tr}_G f = \sum_{g \in G} g^{-1} f g,$$

where $f \in \mathrm{Hom}_R(M, N)$. The reduced homorphism group, $\overline{\mathrm{Hom}}_{RG}(M, N)$, is defined to be

$$\mathrm{Hom}_R \mathrm{Hom}_{RG}(M, N) / \mathrm{Tr}_G \mathrm{Hom}_R(M, N).$$

An RG-module M is called weakly projective if

$$\overline{\mathrm{End}}_{RG}(M) = 0.$$

When M is an RG-lattice, weakly projective implies projective. For much of the time we shall work in the stable categories of RG-modules (respectively RG-lattices), which we denote by $\overline{\mathrm{Mod}}(RG)$ (respectively $\overline{\mathrm{Lat}}(RG)$). The objects here are just the RG-modules (or lattices) as before, but the morphism groups are the $\overline{\mathrm{Hom}}_{RG}$. Two RG-modules M and N are isomorphic in $\overline{\mathrm{Mod}}(RG)$ if and only if there exist two weakly-projective RG-modules P_1 and P_2 such that $M \oplus P_1 \cong N \oplus P_2$ in Mod(RG). The word 'stable' will always mean that we are working in $\overline{\mathrm{Mod}}(RG)$, whilst 'strict' will be used to indicate Mod(RG). We shall often write $\overline{\mathrm{Hom}}$ instead of $\overline{\mathrm{Hom}}_{RG}$ when no confusion is likely to arise.

On $\overline{\mathrm{Lat}}(RG) \times \overline{\mathrm{Mod}}(RG)$ we can define a bifunctor E^r_{RG}, for $r \in \mathbf{Z}$, such that $E^0_{RG} \cong \overline{\mathrm{Mod}}_{RG}$ and $E^r_{RG} \cong \mathrm{Ext}^r_{RG}$ for $r \geqq 1$, see [**6**]. Short exact sequences in either variable lead to long exact sequences in E^*_{RG}.

Proposition 2.1. *Let V be an RG-module. Then there exists an RG-lattice $\tilde{V}$ and a homomorphism $\pi : \tilde{V} \longrightarrow V$ such that π induces an isomorphism on $E^*_{RG}(M, -)$ for any RG-lattice M. The lattice $\tilde{V}$ and the homomorphism π are uniquely determined in* $\overline{\mathrm{Mod}}(RG)$, *up to an automorphism of $\tilde{V}$. We shall refer to $\tilde{V}$ as the cover of V.*

Proof. Existence: Let L be an RG-lattice with a surjection onto V, which leads to a short exact sequence

$$0 \longrightarrow K \xrightarrow{i} L \longrightarrow V \longrightarrow 0,$$

https://doi.org/10.4153/CJM-1990-019-0 Published online by Cambridge University Press

where K is a lattice. Let $\tilde{V} = C(i)$, the cone space lattice as in [**6**]. We get a diagram

$$\begin{array}{ccccc} K & \longrightarrow & L & \longrightarrow & C(i) \\ \| & & \| & & \downarrow \pi \\ K & \longrightarrow & L & \longrightarrow & V \end{array}$$

which commutes stably. If we apply $E^*_{RG}(M, -)$ to both rows, we get long exact sequences and so, by the Five Lemma, π induces an isomorphism on $E^*_{RG}(M, -)$.

Uniqueness: Suppose that $\eta : N \longrightarrow V$ also induces an isomorphism on $E^*_{RG}(M, -)$, where N is an RG-lattice. Then $\eta \in \overline{\mathrm{Hom}}(N, V) \cong E^0_{RG}(N, V)$ lifts to some $\eta' \in \overline{\mathrm{Hom}}(N, \tilde{V})$ such that $\eta = \pi\eta'$: also $\pi \in \overline{\mathrm{Hom}}(\tilde{V}, V)$ lifts to some $\pi' \in \overline{\mathrm{Hom}}(\tilde{V}, N)$ such that $\pi = \eta\pi'$. We see that $\eta = \eta\pi'\eta'$ and hence $\pi'\eta' = \mathrm{id}_N$. Similarly, $\eta'\pi' = \mathrm{id}_{\tilde{V}}$, and so π' is an isomorphism in $\overline{\mathrm{Mod}}(RG)$ which satisfies $\pi = \eta\pi'$, as required.

PROPOSITION 2.2. *Given any two RG-modules U and V there is a canonical homomorphism*

$$\theta : \overline{\mathrm{Hom}}(U, V) \longrightarrow \overline{\mathrm{Hom}}(\tilde{U}, \tilde{V})$$

such that the diagram

$$\begin{array}{ccc} \tilde{U} & \xrightarrow{\theta(f)} & \tilde{V} \\ \downarrow \pi_U & & \downarrow \pi_V \\ U & \xrightarrow{f} & V \end{array}$$

commutes stably.

Remark. We shall often write $\tilde{f}$ for $\theta(f)$.

Proof. Given $f : U \longrightarrow V$ then, corresponding to $f\pi_U \in \overline{\mathrm{Hom}}(\tilde{U}, V)$, there is a unique $g \in \overline{\mathrm{Hom}}(\tilde{U}, \tilde{V})$ such that $\pi_V g = f\pi_U$. Let $\theta(f) = g$.

Remark 2.3. If necessary, given $\tilde{U}$, π_U, f, etc. in Mod(RG), we can make the diagram in Proposition 2.2 commute strictly. This is because $f\pi_U - \pi_V g = \mathrm{Tr}_G(h)$ for some $h \in \mathrm{Hom}_R(\tilde{U}, V)$: h lifts to $h' \in \mathrm{Hom}_R(\tilde{U}, \tilde{V})$ and we can replace g by $g + \mathrm{Tr}_G(h')$.

A sequence $U \xrightarrow{u} V \xrightarrow{v} W$ in $\overline{\mathrm{Mod}}(RG)$ is called *stably exact* if it is isomorphic in $\overline{\mathrm{Mod}}(RG)$ to a sequence that is short exact in Mod(RG).

PROPOSITION 2.4. *If $U \xrightarrow{u} V \xrightarrow{v} W$ is a stably exact sequence of RG-modules, then $\tilde{U} \xrightarrow{\tilde{u}} \tilde{V} \xrightarrow{\tilde{v}} \tilde{W}$ is a stably exact sequence of lattices.*

Proof. We can construct $L(\tilde{v})$, the path space on $\tilde{v}$ ([**6**]), and obtain a stably exact sequence of lattices

$$L(\tilde{v}) \xrightarrow{\tilde{v}_1} \tilde{V} \xrightarrow{\tilde{v}} W.$$

If we apply $E^*_{RG}(L(\tilde{v}), -)$ to $U \xrightarrow{u} V \xrightarrow{v} W$, we obtain a long exact sequence, hence the sequence

$$\overline{\mathrm{Hom}}(L(\tilde{v}), \tilde{U}) \xrightarrow{\tilde{u}_*} \overline{\mathrm{Hom}}(L(\tilde{v}), \tilde{V}) \xrightarrow{\tilde{v}_*} \overline{\mathrm{Hom}}(L(\tilde{v}), \tilde{W})$$

is exact at the middle term. Now $\tilde{v}_*(\tilde{v}_1) = \tilde{v}\tilde{v}_1 = 0$ and so there exists an $r \in \overline{\mathrm{Hom}}(L(\tilde{v}), \tilde{U})$ such that $\tilde{v}_1 = \tilde{u}_*(r) = \tilde{u}r$, and we get a commutative diagram

$$\begin{array}{ccccc} L(\tilde{v}) & \xrightarrow{\tilde{v}_1} & \tilde{V} & \xrightarrow{\tilde{v}} & \tilde{W} \\ \downarrow r & & \| & & \| \\ \tilde{U} & \xrightarrow{\tilde{u}} & \tilde{V} & \xrightarrow{\tilde{v}} & \tilde{W} \\ \downarrow \pi_U & & \downarrow \pi_V & & \downarrow \pi_W \\ U & \longrightarrow & V & \longrightarrow & W \end{array}$$

On applying $E^*_{RG}(\tilde{U}, -)$ to the bottom and top rows we get long exact sequences. The homomorphisms π_V and π_W both induce isomorphisms on $E^*_{RG}(\tilde{U}, -)$ and thus $\pi_U r$ must do so too. But as π_U also induces an isomorphism on $E^*_{RG}(\tilde{U}, -)$, we see that r must induce an isomorphism on

$$\overline{\mathrm{Hom}}_{RG}(\tilde{U}, -) = E^0_{RG}(\tilde{U}, -).$$

It follows easily that r is a stable isomorphism (cf. [**6**], Corollary 2.3).

Let Ω be the Heller operator on $\overline{\mathrm{Lat}}(RG)$. It is well defined and has an inverse Ω^{-1}. We shall also use it for modules that are projective over R/I, where I is an ideal of R. Here it is understood that we perform the construction over $(R/I)G$ i.e., ΩV is the kernel of an epimorphism $(R/I)G^n \longrightarrow V$.

Recall from [**6**] that if $A \xrightarrow{a} B \xrightarrow{b} C$ is a stably exact sequence in Lat(G) then there is a homomorphism $c : C \longrightarrow \Omega^{-1}A$ such that the infinite sequence

$$\cdots \longrightarrow \Omega B \xrightarrow{\Omega b} \Omega C \xrightarrow{\Omega c} A \xrightarrow{a} B \xrightarrow{b} C \xrightarrow{c} \Omega^{-1}A \xrightarrow{\Omega^{-1}a} \Omega^{-1}B \cdots,$$

called a *Puppe sequence*, has the property that if we apply $\overline{\mathrm{Hom}}(M, -)$ to every term then the result is isomorphic to the long exact sequence for $E^*_{RG}(M, -)$. Every three-lattice stretch of the Puppe sequence is stably exact. These constructions also work when applied to RG-modules that are all projective over R/I.

LEMMA 2.5. *If one of the homomorphisms in the Puppe sequence is zero in* $\overline{\mathrm{Lat}}(RG)$, *then the Puppe sequence decomposes stably into split short exact sequences.*

Proof. Suppose without loss of generality that $c = 0$ in the sequence above. Then

$$b_* : \mathrm{Hom}(C, B) \longrightarrow \mathrm{Hom}(C, C)$$

https://doi.org/10.4153/CJM-1990-019-0 Published online by Cambridge University Press

is onto and so b is split.

At this point it simplifies matters if we assume that R is a principal ideal domain. In any case we can ensure this by inverting all the primes of R that do not divide $|G|$. The change of ring does not alter $\overline{\mathrm{Hom}}$, thus it has no effect on $\overline{\mathrm{Mod}}(RG)$.

When $q \in R$ and V is an R-module we shall write V/q for V/qV.

PROPOSITION 2.6. *Suppose that M is an RG-lattice and that $q \in R$ is such that $q\overline{\mathrm{End}}(M) = 0$. Then there exists a canonical sequence which is stably exact and split;*

$$M \xrightarrow{i} \widetilde{M/q} \longrightarrow \Omega^{-1}M.$$

Also $\pi i = m$, where $m : M \longrightarrow M/q$ is the quotient homomorphism.

Proof. Since $0 \longrightarrow M \xrightarrow{q} M \longrightarrow M/q \longrightarrow 0$ is exact, we can construct $\widetilde{M/q}$ from the stably exact sequence $M \xrightarrow{q} M \longrightarrow \widetilde{M/q}$. Part of the Puppe sequence is

$$\cdots \longrightarrow M \xrightarrow{q} M \longrightarrow \widetilde{M/q} \longrightarrow \Omega^{-1}M \xrightarrow{q} \Omega^{-1}M \longrightarrow \cdots,$$

thus $M \longrightarrow \widetilde{M/q} \longrightarrow \Omega^{-1}M$ is stably exact. Since $q\,\mathrm{id}_M = 0$ in $\mathrm{Lat}(RG)$, the sequence must split by Lemma 2.5.

Remark. The splitting need not be canonical. When we write

$$\widetilde{M/q} \cong M \oplus \Omega^{-1}M$$

we are assuming that we have fixed some splitting.

PROPOSITION 2.7. *If M is an RG-lattice, $q, r \in R$ and $q\overline{\mathrm{End}}(M) = 0$, then there are splittings of $\widetilde{M/qr}$ and $\widetilde{M/q}$ such that*

a) *the quotient homomorphism $m : M/qr \longrightarrow M/q$ lifts to give a stably commutative diagram*

$$\begin{array}{ccccc} \widetilde{M/qr} & \cong & M & \oplus & \Omega^{-1}M \\ \downarrow{\scriptstyle \tilde{m}} & & \| & & \downarrow{\scriptstyle r} \\ \widetilde{M/qr} & \cong & M & \oplus & \Omega^{-1}M \end{array}$$

b) *the inclusion $n : M/q \longrightarrow M/qr$ lifts to give a stably commutative diagram*

$$\begin{array}{ccccc} \widetilde{M/q} & \cong & M & \oplus & \Omega^{-1}M \\ \downarrow{\scriptstyle \tilde{n}} & & \downarrow{\scriptstyle r} & & \| \\ \widetilde{M/qr} & \cong & M & \oplus & \Omega^{-1}M \end{array}$$

https://doi.org/10.4153/CJM-1990-019-0 Published online by Cambridge University Press

Proof. a) The commutative diagram

$$\begin{array}{ccccc} M & \xrightarrow{qr} & M & \longrightarrow & M/qr \\ \downarrow r & & \| & & \downarrow m \\ M & \xrightarrow{q} & M & \longrightarrow & M/q \end{array}$$

leads, as in the proof of Proposition 2.6, to

$$\begin{array}{ccccc} M & \longrightarrow & \widetilde{M/q} & \longrightarrow & \Omega^{-1}M \\ \| & & \downarrow \tilde{m} & & \downarrow r \\ M & \longrightarrow & M/q & \longrightarrow & \Omega^{-1}M \end{array}$$

A splitting homomorphism $\widetilde{M/q} \longrightarrow M$ automatically leads to one $\widetilde{M/qr} \longrightarrow M$, by composition with $\tilde{m}$, hence we get two consistent splittings (and, in particular, $\tilde{m}$ does not involve any homomorphism $\Omega^{-1}M \longrightarrow M$).

The proof of (b) is similar.

PROPOSITION 2.8. *Suppose that $q \in R$ and that V is an RG-module that is projective over R/q. Then there is a canonical stably exact sequence*

$$\Omega^{-1}V \longrightarrow \tilde{V}/q \xrightarrow{\pi'} V,$$

where π' is induced from $\pi : \tilde{V} \longrightarrow V$ and $\Omega^{-1}V$ is determined over $(R/q)G$.

Proof. By adding projectives to $\tilde{V}$ if necessary, we can assume that $\pi : \tilde{V} \longrightarrow V$ is surjective. $P = \ker(\pi)$ is a lattice for which $E^*_{RG}(M, P)$ is always zero, hence it is projective. We have an exact sequence

$$0 \longrightarrow P \longrightarrow \tilde{V} \longrightarrow V \longrightarrow 0.$$

Reducing this modulo q we obtain an exact sequence

$$0 \longrightarrow q\tilde{V}/qP \xrightarrow{\sigma} P/qP \longrightarrow \tilde{V}/q\tilde{V} \xrightarrow{\pi'} V \longrightarrow 0.$$

Now $q\tilde{V}/q\tilde{P} \cong \tilde{V}/P \cong V$ and P/qP is weakly projective, thus

$$\ker(\pi') \cong \operatorname{coker}(\sigma) \cong \Omega^{-1}V,$$

as required.

PROPOSITION 2.9. *If V is an RG-module that is projective over R/q, then the following conditions are equivalent.*

i) *V is a direct summand of L/q for some RG-lattice L.*

ii) $\theta : \overline{\mathrm{End}}(V) \longrightarrow \overline{\mathrm{End}}(\tilde{V})$ *is injective.*
iii) *The sequence* $\Omega^{-1}V \longrightarrow \tilde{V}/q \longrightarrow V$ *of Proposition* 2.8 *splits.*

Proof. (i) $\Rightarrow$ (ii): The composition $L \longrightarrow L/q \longrightarrow V$ must factor through $\tilde{V}$, hence we get a diagram

$$\begin{array}{ccccc} \overline{\mathrm{Hom}}(V,V) & \longrightarrow & \overline{\mathrm{Hom}}(\tilde{V},V) & \xleftarrow[\cong]{\pi_*} & \overline{\mathrm{Hom}}(\tilde{V},\tilde{V}) \\ \downarrow & & \downarrow & & \downarrow \\ \overline{\mathrm{Hom}}(L/q,V) & \xrightarrow[\cong]{} & \overline{\mathrm{Hom}}(L,V) & \xleftarrow[\cong]{\pi_*} & \overline{\mathrm{Hom}}(L,\tilde{V}) \end{array}$$

where $\overline{\mathrm{Hom}}(L/q, V) \cong \overline{\mathrm{Hom}}(L, V)$ because $qV = 0$.

But θ is the composition of the top row from left to right, and so it must be injective.

(ii) $\Rightarrow$(iii): Consider the Puppe sequences

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & \Omega^{-1}\tilde{V} & \longrightarrow & \widetilde{\tilde{V}/q} & \longrightarrow & \tilde{V} & \xrightarrow{\theta(d)} & \tilde{V} & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & \Omega^{-1}\tilde{V} & \longrightarrow & \tilde{V}/q & \longrightarrow & V & \xrightarrow{d} & V & \longrightarrow & \cdots \end{array}$$

The first three terms of the top row from a split sequence by Proposition 2.6. Thus $\theta(d) = 0$, hence $d = 0$ and the bottom row splits.

(iii) $\Rightarrow$ (i): This is clear.

3. Endomorphism rings.

PROPOSITION 3.1. *Suppose that* M *is an* RG*-lattice and that* $q \in R$ *annihilates* $\overline{\mathrm{End}}(M)$. *Choose a splitting* $\widetilde{M/q} \cong M \oplus \Omega^{-1}M$. *Then there is an isomorphism*

$$\varphi_q : \overline{\mathrm{End}}(M/q) \longrightarrow \overline{\mathrm{End}}(M) \oplus \overline{\mathrm{Hom}}(M, \Omega^{-1}M)$$

such that, after applying the homomorphism

$$\theta : \overline{\mathrm{End}}(M/q) \longrightarrow \overline{\mathrm{End}}(\widetilde{M/q}) \cong \overline{\mathrm{End}}(M \oplus \Omega^{-1}M),$$

$\varphi_q^{-1}(f, 0)$ *has matrix*

$$A(f) = \begin{bmatrix} f & U_f \\ 0 & \Omega^{-1}f \end{bmatrix}$$

and $\varphi_q^{-1}(0, g)$ *has matrix*

$$B(g) = \begin{bmatrix} 0 & X_g \\ g & Y_g \end{bmatrix},$$

for $f \in \overline{\mathrm{End}}(M)$, $g \in \overline{\mathrm{Hom}}(M, \Omega^{-1}M)$ *and some* $U_f \in \overline{\mathrm{Hom}}(\Omega^{-1}M, M)$, $X_g \in \overline{\mathrm{Hom}}(\Omega^{-1}M, M)$, $Y_g \in \overline{\mathrm{End}}(\Omega^{-1}M)$.

Furthermore $\varphi_q^{-1}(f,g)$ *is the composition*

$$M/q \xrightarrow{f'\oplus g'} M/q \oplus \Omega^{-1}M/q \xrightarrow{\pi'} M/q.$$

Remark. For a fixed element of $\overline{\mathrm{End}}(M/q)$, only g is necessarily independent of the splitting. We shall always fix a splitting and consider $\overline{\mathrm{End}}(M/q)$ as a subring of $\overline{\mathrm{End}}(M \oplus \Omega^{-1}M)$ via θ.

Proof.

$$\begin{aligned}\overline{\mathrm{End}}(M/q) &\cong \overline{\mathrm{Hom}}(M/q, M/q) \cong \overline{\mathrm{Hom}}(M, M/q)\\ &\cong \overline{\mathrm{Hom}}(M, \widetilde{M/q}) \cong \overline{\mathrm{Hom}}(M, M) \oplus \overline{\mathrm{Hom}}(M, \Omega^{-1}M).\end{aligned}$$

This defines φ_q and shows that it is an isomorphism. This definition is easily seen to be equivalent to taking the first column of $\theta(\alpha)$ for $\varphi_q(\alpha)$, and so all that remains is to show that the bottom right-hand entry in $A(f)$ is actually $\Omega^{-1}f$. This is a consequence of Lemma 3.2 below.

LEMMA 3.2. *The composition*

$$\overline{\mathrm{End}}(M) \longrightarrow \overline{\mathrm{End}}(M/q) \xrightarrow{\theta} \mathrm{End}(\widetilde{M/q})$$

sends f *to* $A(f)$.

Proof. The diagram

$$\begin{array}{ccccc} M & \xrightarrow{q} & M & \longrightarrow & M/q \\ \downarrow f & & \downarrow f & & \downarrow \\ M & \xrightarrow{q} & M & \longrightarrow & M/q \end{array}$$

leads to

$$\begin{array}{ccccc} M & \longrightarrow & \widetilde{M/q} & \longrightarrow & \Omega^{-1}M \\ \downarrow f & & \downarrow \varphi_q^{-1}(f,0) & & \downarrow \Omega^{-1}f \\ M & \longrightarrow & \widetilde{M/q} & \longrightarrow & \Omega^{-1}M \end{array}$$

hence $A(f)$ must have the form claimed.

PROPOSITION 3.3. *Let* M *be an* RG*-lattice and let* $q, r \in R$ *and suppose that*

$$q\,\mathrm{End}(M) = 0.$$

Let

$$\alpha = \varphi_{qr}^{-1}(f,g) \in \overline{\mathrm{End}}(M/qr).$$

Consider the reduction modulo q of α to $\alpha' \in \overline{\mathrm{End}}(M/q)$, say $\alpha' = \varphi_q^{-1}(f', g')$. Then

$$f = f', g' = rg \quad \textit{and} \quad U_f + X_g = r(U_{f'} + X_{g'}).$$

Proof. Apply Proposition 2.7 to the diagram

$$\begin{array}{ccc} \widetilde{M/qr} & \xrightarrow{\tilde{\alpha}} & \widetilde{M/qr} \\ \downarrow & & \downarrow \\ \widetilde{M/qr} & \xrightarrow{\tilde{\alpha}'} & \widetilde{M/q} \end{array}$$

Recall that on an RG-lattice M, the trace over R is well defined as an additive homomorphism $\mathrm{tr}_R : \overline{\mathrm{End}}(M) \longrightarrow R/|G|$.

LEMMA 3.4. *If M is an RG-lattice and $f \in \overline{\mathrm{End}}(M)$ then* $\mathrm{tr}_R(\Omega f) = -\mathrm{tr}_R(f)$.

Proof. The homomorphism Ωf is defined stably via a diagram of strictly exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Omega M & \longrightarrow & P & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \Omega f} & & \downarrow{\scriptstyle \bar{f}} & & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & \Omega M & \longrightarrow & P & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

where P is projective. It follows that $\mathrm{tr}_R(f) + \mathrm{tr}_R(\Omega f) = \mathrm{tr}_R(\bar{f}) = 0$.

LEMMA 3.5. *If V is a torsion RG-module and θ is as in Proposition* 3.1 *then*

$$\mathrm{tr}_R(\theta(\alpha)) = 0 \quad \textit{for all } \alpha \in \overline{\mathrm{End}}(V).$$

Proof. Let $\sigma : P \longrightarrow V$ be a surjection from a projective lattice onto V. Let $K = \ker(\sigma)$: we get

$$\begin{array}{ccccc} K & \longrightarrow & P & \longrightarrow & V \\ \downarrow{\scriptstyle f''} & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} \\ K & \longrightarrow & P & \longrightarrow & V \end{array}$$

Now $\theta(f) = \Omega f''$ and thus $\mathrm{tr}_R(\theta(f)) = -\mathrm{tr}_R(f'')$ by Lemma 3.4. Since V is a torsion module, $\mathrm{tr}_R(f'') = \mathrm{tr}_R(f')$, but P is projective and so $\mathrm{tr}_R(f') = 0$.

COROLLARY 3.6. *If V is a torsion RG-module then $|G|$ divides* $\mathrm{rank}_R \tilde{V}$ *in R.*

Proof. We know that $\mathrm{rank}_R \tilde{V} = \mathrm{tr}_R(\mathrm{id}_{\tilde{V}})$. But $\mathrm{id}_{\tilde{V}} = \theta(\mathrm{id}_V)$, and so

$$\mathrm{tr}_R(\mathrm{id}_{\tilde{V}}) = 0 \in R/|G|,$$

by Lemma 3.5.

LEMMA 3.7. *If, in the matrices of Proposition* 3.1, U_f *and* X_g *are both zero for all* f *and* g, *then* Y_g *is also zero.*

Proof. Recall that if M and N are RG-lattices then composition and trace

$$\overline{\mathrm{Hom}}(M, N) \otimes \overline{\mathrm{Hom}}(N, M) \longrightarrow \overline{\mathrm{End}}(M) \longrightarrow R/|G|$$

is a duality pairing [**6**]. Suppose that $Y_g \neq 0$ for some g; then there must exist an $h \in \overline{\mathrm{End}}(\Omega^{-1}M)$ such that $\mathrm{tr}_R(hY_g) \neq 0$.

One can easily verify that

$$A(\Omega h)B(g) = \begin{bmatrix} 0 & 0 \\ hg & hY_g \end{bmatrix},$$

hence

$$\mathrm{tr}_R(hY_g) = \mathrm{tr}_R(A(\Omega h)B(g)) = 0$$

by Lemma 3.5, a contradiction.

PROPOSITION 3.8. *Suppose that* $q, r \in R$ *are such that*

$$q\overline{\mathrm{End}}(M) = 0 \quad and \quad r\overline{\mathrm{Hom}}(\Omega^{-1}M, M) = 0.$$

Then

$$\varphi_{qr}^{-1}(f, g) = \begin{bmatrix} f & 0 \\ g & \Omega^{-1}f \end{bmatrix},$$

where $f \in \overline{\mathrm{End}}(M)$, $g \in \overline{\mathrm{Hom}}(M, \Omega^{-1}M)$.

Proof. Proposition 3.3 implies that U_f and Y_g are identically zero, and now Lemma 3.7 implies that X_g is zero.

COROLLARY 3.9. *Suppose that* M *is an* RG*-lattice and that* $n, m \in R$ *are such that*

$$nR = \mathrm{ann}_R\, \overline{\mathrm{End}}(M) \quad and \quad mR = \mathrm{ann}_R\, \overline{\mathrm{Hom}}(\Omega^{-1}M, M).$$

Then for any $l \in R$, *there is an isomorphism of rings*

$$\overline{\mathrm{End}}(M/lmn) \cong \overline{\mathrm{End}}(M/mn).$$

Example 3.10. Let $R = \mathbf{Z}$ and let M be a $\mathbf{Z}G$-lattice; we know that

$$\widetilde{M/|G|} \cong M \oplus \Omega^{-1}M.$$

However, $M/|G|$ is a torsion module so it splits into a direct sum of parts, each of which is annihilated by a power of just one prime:

$$M/|G| \cong \bigoplus_{P||G|} A_p.$$

We deduce that

$$M \oplus \Omega^{-1}M \cong \bigoplus_{P||G|} \tilde{A}_p.$$

If, for example, $M = \mathbf{Z}$, the trivial lattice, then none of the $\tilde{A}_p$ are projective (since $\hat{H}^0(G;\tilde{A}_p) \cong \hat{H}^0(G;\mathbf{Z})_p \oplus H^1(G;\mathbf{Z})_p \neq 0$). Thus $\mathbf{Z} \oplus \Omega^{-1}\mathbf{Z}$ decomposes stably as a direct sum of non-projective parts such that all but at most one are projective at any given prime. The number of summands is equal to the number of prime divisors of $|G|$, contrasting with results of [**3**] which show that, for the lattice $\mathbf{Z}$ alone, the number of such summands is severely restricted, and in any case less than or equal to six.

4. Decompositions modulo p^n. From now on we assume that R is a complete discrete valuation ring of characteristic zero with prime element p. This implies that an RG-lattice M has no stable splitting $M \cong A \oplus B$ with neither A nor B projective if and only if $\overline{\mathrm{End}}(M)$ is a local ring. The Krull-Schmidt-Azumaya Theorem also holds, i.e., a decomposition of an RG-lattice into indecomposable summands is essentially unique. As a consequence, we can consider the cover $\tilde{V}$ to be well defined in Mod(RG), (not just stably), by removing all the projective summands. The same applies to ΩA whenever A is an RG-lattice or is an RG-module that is projective over R/p^n.

In this section we investigate the possible direct sum decompositions of the reduction modulo p^n of an RG-lattice. Since we shall work stably, we need the following lemma to show that there is no essential loss of information.

PROPOSITION 4.1. *Let M be an RG-lattice, V an RG-module and $\pi : M \longrightarrow V$ an epimorphism. Suppose that $V = W \oplus P$ where P is weakly projective. Then $M = \overline{W} \oplus \overline{P}$ (strictly) where $\overline{P}$ is projective and $\pi(\overline{P}) = P$. If* $\ker(\pi) \subset pM$ *then we can arrange that, in addition, $\pi(\overline{W}) = W$.*

Proof. Let $q : \overline{P} \longrightarrow P/p$ be the projective cover of P/p. Let

$$r : M \longrightarrow V \longrightarrow P \longrightarrow P/p$$

be the canonical projection: q lifts to $\bar{q} : \overline{P} \longrightarrow M$ such that $q = r\bar{q}$. We want to show that $\bar{q}$ splits over R, because then it must split over RG, since the projectives over RG are weakly injective.

If $x \in M$ and $px = \bar{q}(y)$ for some $y \in \overline{P}$, then

$$q(y) = r\bar{q}(y) = r(px) = pr(x) = 0.$$

Because $\overline{P}/p \cong P/p$, we see that $y = pz$ and hence that $x = \bar{q}(z)$. This shows that $\mathrm{im}(\bar{q})$ is a direct summand of M over R. Now if $\bar{q}$ is not injective, then there is an $x \in \overline{P}$ that is not a multiple of p such that $\bar{q}(x) = 0$. But then $r\bar{q}(x) = q(x) = 0$, which is impossible.

For the case $\ker(\pi) \subset pM$ we sketch another proof which yields $\pi(\overline{W}) = W$. Let $e \in \mathrm{End}(v)$ be the projection onto P. Then $e = \mathrm{Tr}_G f$, for some $f \in \mathrm{End}_R(V)$, and $f\pi$ lifts to $f' : M \longrightarrow \overline{P} \xrightarrow{\bar{q}} M (\overline{P} \xrightarrow{\bar{q}} M$ as before). If we let

$$e' = \mathrm{Tr}_G f' \in \mathrm{End}(M),$$

then $e'\pi = \pi e'$: by the method of lifting idempotents, which applies when $\ker(\pi) \subset pM$, e' can be lifted to an idempotent e'' such that $e''\pi = \pi e''$ and $\mathrm{im}(e'') \subset P$ (and so, in fact, $\mathrm{im}(e'') = P$). Take $\overline{W} = \ker(e'')$.

COROLLARY 4.2. *If M is an indecomposable RG-lattice and M is not projective, then M/p^n can not have any weakly projective direct summands for any $n \in \mathbf{N}$.*

Let $n(G)$ be the largest integer such that $p^{n(G)}$ divides $|G|$. Given an RG-module M, let $n(M)$ be the smallest integer such that

$$p^{n(M)}\overline{\mathrm{End}}(M) = 0$$

and, if M is a lattice, let $m(M)$ be the smallest integer such that

$$p^{m(M)}\overline{\mathrm{Hom}}(M, \Omega^{-1}M) = 0.$$

Then $n(M) \leqq n(G)$ and, since $\overline{\mathrm{Hom}}(\Omega^{-1}M, M)$ is a module over $\overline{\mathrm{End}}(M)$, we see that $m(M) \leqq n(M)$.

PROPOSITION 4.3. *Let M and N be indecomposable RG-lattices, and suppose that $n \in \mathbf{Z}$ is such that $n \geqq n(M)$ and $n \geqq n(N)$. If $M/p^n \cong M/p^n$, then either $M \cong N$ or $M \cong \Omega N \cong \Omega^2 M$.*

Proof. We have

$$M \oplus \Omega^{-1}M \cong \widetilde{M/p}^{\,n} \cong \widetilde{N/p}^{\,n} \cong N \oplus \Omega^{-1}N.$$

By the Krull-Schmidt-Azumaya Theorem, either $M \cong N$ (and $\Omega^{-1}M \cong \Omega^{-1}N$) or $M \cong \Omega^{-1}N$ and $N \cong \Omega^{-1}M$.

PROPOSITION 4.4. ([**5**]) *Let M and N be RG-lattices, and suppose that $n \in \mathbf{Z}$ is such that $n \geqq n(M)$ and $n \geqq n(N)$. If $M/p^{n+1} \cong N/p^{n+1}$, then $M \cong N$.*

Proof. Because

$$\overline{\mathrm{Hom}}(\widetilde{M/p^n}, \widetilde{N/p^n}) \cong \overline{\mathrm{Hom}}(M \oplus \Omega^{-1}M, N \oplus \Omega^{-1}N),$$

we can perform the same operations with matrices as we did for $\overline{\text{End}}(\widetilde{M/p^n})$. An isomorphism

$$\alpha : M/q^n \longrightarrow N/p^n$$

lifts to

$$\tilde{\alpha} = \varphi_{p^{n+1}}^{-1}(f, g)$$

for some $f \in \overline{\text{Hom}}(M, N)$ and $g \in \overline{\text{Hom}}(M, \Omega^{-1}N)$. By Remark 2.3, we can ensure that $\pi\tilde{\alpha} = \alpha\pi$ strictly. Now if we reduce modulo p^n and use primes to denote the reductions of α, f etc., then

$$\tilde{\alpha}' = \varphi_{p^n}^{-1}(f, pg),$$

by Proposition 3.3. Therefore α is equal to the composition

$$M/p^n \xrightarrow{f' \oplus pg'} N/p^n \oplus (\Omega^{-1}N)/p^n \xrightarrow{\pi'} N/p^n$$

by Proposition 3.1, i.e.,

$$\alpha' = f' + p(\pi' g).$$

Now f is an isomorphism by Nakayama's Lemma.

Proposition 4.5. *Suppose that M is an indecomposable RG-lattice and that $n \in \mathbf{Z}$, $n \geqq n(M)$ and that M/q^n decomposes. Then M/p^n has exactly two indecomposable summands; more precisely, $M/p^n \cong A \oplus \Omega^{-1}A$ in* Mod(RG) *for some indecomposable RG-module A such that $\tilde{A} \cong M$. Also $p^{n(G)}$ divides* $\text{rank}_R(M)$.

Proof. There can be no weakly projective summands, by Proposition 4.1. Suppose that $M/p^n \cong A \oplus B \oplus C$: then

$$M \oplus \Omega^{-1}M \cong \widetilde{M/p}^n \cong \tilde{A} \oplus \tilde{B} \oplus \tilde{C},$$

and so, by the Krull-Schmidt-Azumaya Theorem, one of $\tilde{A}$, $\tilde{B}$ or $\tilde{C}$ must be 0; say $\tilde{C} = 0$. Now θ embeds $\overline{\text{End}}(C)$ in $\overline{\text{End}}(\tilde{C})$, by Proposition 2.9, hence $\overline{\text{End}}(C) = 0$; thus C is weakly projective and so $C = 0$. Interchanging A and B if necessary, we have that $\tilde{A} \cong M$ and $\tilde{B} \cong \Omega^{-1}M$.

According to Proposition 2.8, there is a stable exact sequence

$$\Omega^{-1}A \longrightarrow \tilde{A}/p^n \longrightarrow A,$$

i.e.,

$$\Omega^{-1}A \longrightarrow A \oplus B \xrightarrow{r} A.$$

The module A satisfies condition (i) of Proposition 2.9, hence this sequence splits; $A \oplus \Omega^{-1}A \cong A \oplus B$, and so $B \cong \Omega^{-1}A$.

We see that $p^{n(G)}$ divides $\mathrm{rank}_R(M)$ because $\tilde{A} \cong M$ and we can apply Corollary 3.6.

LEMMA 4.6. *Suppose that M is an indecomposable RG-lattice, that $s \geqq n(M)+1$ and that $\alpha \in \overline{\mathrm{End}}(M/p^s)$. Then $Y_g \in \overline{\mathrm{End}}(\Omega^{-1}M)$ in the matrix for $\theta(\alpha)$ is contained in the radical of $\overline{\mathrm{End}}(\Omega^{-1}M)$.*

Proof. Suppose that $Y_g \notin \mathrm{rad}\,\overline{\mathrm{End}}(\Omega^{-1}M)$ for some g. Then, since $\overline{\mathrm{End}}(\Omega^{-1}M) \cong \overline{\mathrm{End}}(M)$ is a local ring, Y_g is an isomorphism. Since the trace yields a duality pairing on $\overline{\mathrm{End}}(\Omega^{-1}M)$, there must be an $h \in \overline{\mathrm{End}}(\Omega^{-1}M)$ with $\mathrm{tr}_R(h) \in R/|G|$ of order $p^{n(M)}$. Let $f = \Omega(hY_g^{-1})$; then

$$A(f)B(g) = \begin{bmatrix} U_f g & * \\ * & h \end{bmatrix},$$

and so

$$\mathrm{tr}_R(A(f)B(g)) = \mathrm{tr}_R(U_f g) + \mathrm{tr}_R(h).$$

Now $\mathrm{tr}(A(f)B(g)) = 0$, by Lemma 3.5, but U_f is a multiple of p, by Proposition 3.3, which contradicts the maximality of the order of $\mathrm{tr}_R(h)$.

The following reformulation of the Krull-Schmidt-Azumaya Theorem must be well known. Let $M_t(S)$ denote the ring of $s \times s$ matrices with entries in S.

PROPOSITION 4.7. *Suppose that $L_1, L_2, \ldots, L_n$ are RG- lattices and that no two of them are isomorphic. Let*

$$M = \bigoplus_1^n (L_i)^{r_i} \quad \textit{for some } \{r_i\} \subset \mathbf{N}.$$

a) $\mathrm{End}(M)/\mathrm{rad}\,\mathrm{End}(M) \cong \bigoplus_1^n M_{r_i}(\mathrm{End}(L_i)/\mathrm{rad}\,\mathrm{End}(L_i))$.

b) *If* $\mathrm{End}(M)$ *is written in terms of matrices with entries in* $\mathrm{Hom}(L_i, L_j)$ *in the usual way, then* $\mathrm{rad}\,\mathrm{End}(M)$ *corresponds to the set J of those matrices in which none of the entries is an isomorphism.*

Proof. The set J is easily seen to be an ideal of $\mathrm{End}(M)$, and $\mathrm{End}(M)/J$ is isomorphic to the right-hand side of the equation in part (a). Since this is semi-simple, J must contain $\mathrm{radEnd}(M)$ and it suffices to show that $J \subset \mathrm{rad}\,\mathrm{End}(M)$.

Let B be the set of matrices in J with only one non-zero entry: these generate J over R and so we only need to show that $B \subset \mathrm{rad}\,\mathrm{End}(M)$. Let $b \in B$: it is a well-known property of radicals that $b \in J$ if $1 - ab$ is invertible for any $a \in \operatorname{End}(M)$. However, $1 - ab$ will be of the form

$$\begin{bmatrix} 1 & & & * & & & \\ & \ddots & & \vdots & & & \\ & & 1 & * & & & \\ & & & 1-c & & & \\ & & & * & 1 & & \\ & & & \vdots & & \ddots & \\ & & & * & & & 1 \end{bmatrix}$$

where all entries not marked are zero and $c \in \operatorname{rad}\operatorname{End}(M)$. Now $1-c$ is invertible and so this matrix is invertible (after changing the order of the basis lattices, it is triangular).

Remark. The statements of Proposition 4.7 remain true if we replace Hom by $\overline{\text{Hom}}$ throughout.

PROPOSITION 4.8. *Let M be an indecomposable RG-lattice and let $s \in \mathbf{Z}$, $s \geqq n(M) + 1$. Then*

$$\operatorname{rad}\overline{\operatorname{End}}(M/p^s) = \varphi_{p^s}^{-1}(\operatorname{rad}\overline{\operatorname{End}}(M) \oplus \overline{\operatorname{Hom}}(M, \Omega^{-1}M)).$$

Proof. Let I denote the right-hand side of the equation above. The top right-hand entries of the corresponding matrices are divisible by p, according to Proposition 3.3. It follows that I is an ideal in $\overline{\operatorname{End}}(M/p^s)$; I is clearly maximal and we shall show that it is nilpotent. Note that the diagonal entries in the matrices for I are not isomorphisms, by Lemma 4.6.

If $M \ncong \Omega^{-1}M$ then I is contained in $\operatorname{rad}\overline{\operatorname{End}}(M \oplus \Omega^{-1}M)$, by Proposition 4.7, hence I is nilpotent.

In the case $M \cong \Omega^{-1}M$, the only possible isomorphism in a matrix for an element of I is in the bottom left-hand corner. Hence I^2 has no isomorphisms as entries and so it is contained in $\operatorname{rad}\overline{\operatorname{End}}(M \oplus \Omega^{-1}M)$, by Proposition 4.7, hence I is nilpotent.

COROLLARY 4.9. ([**5**]) *If M is an indecomposable RG-lattice and $s \geqq n(M)+1$, then M/p^s is indecomposable.*

Proof. By Proposition 4.8, $\operatorname{rad}\overline{\operatorname{End}}(M/p^s)$ is a maximal ideal, i.e., $\overline{\operatorname{End}}(M/p^s)$ is local.

When an RG-lattice M is not indecomposable then $M = \oplus N_i$, where each N_i is indecomposable. If $s \geqq n(M) + 1$, then $M/p^s = \oplus N_i/p^s$, again a sum of indecomposables. By the Krull-Schmidt-Azumaya Theorem, any other decomposition of M/p^s into indecomposables will have summands isomorphic to the

https://doi.org/10.4153/CJM-1990-019-0 Published online by Cambridge University Press

N_i/p^s. One can ask whether there is a decomposition of M that is consistent with this new decomposition of M/p^s. This is, of course, a question about lifting idempotents. We want to know whether an idempotent $\varphi_{p^s}^{-1}(f,g) \in \overline{\mathrm{End}}(M/p^s)$ will lift to an idempotent of End(M), i.e., if g must be zero. This is not always the case, for consider the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & a & 1 & 0 \\ b & 0 & 0 & 0 \end{bmatrix}$$

It is idempotent but the bottom left-hand square is not zero. In this manner one can construct idempotents in End(M/p^s) that do not lift whenever M has two summands N_1 and N_2 such that

$$\overline{\mathrm{End}}(N_1, \Omega N_2) \neq 0 \neq \overline{\mathrm{End}}(N_2, \Omega N_1).$$

PROPOSITION 4.10. (cf. [**5**]) *Suppose that M is an RG-lattice, that $s \geqq n(M)+1$ and that $\alpha \in$ End(M/p^s) is idempotent. Then there is an idempotent $\beta \in$ End(M) such that when α and β are both reduced to* End(M/p^{s-t}) *they are equal. Here*

$$t = \begin{cases} m(M) & \text{if } s \geqq n(M) + m(M), \\ n(M) & \text{otherwise,} \end{cases}$$

(in any case $t \leqq n(M)$)).

Proof. Let $\alpha = \varphi_{p^s}^{-1}(f,g)$. If $s \geqq n(M)+m(M)$ then $s-t \geqq n(M)$ and, letting primes denote reductions modulo p^{s-t}, we have

$$\alpha' = \varphi_{p^{s-t}}^{-1}(f,0),$$

by Proposition 3.3. This yields $\alpha' = f'$ in $\overline{\mathrm{End}}(M/p^{s-t})$. If, on the other hand, $t = n(M)$ then, reducing modulo $n(M)$,

$$\alpha'' = \varphi_{p^{n(M)}}^{-1}(f, p^{s-t}g);$$

i.e., α'' is the reduction of $f + p^{s-t}rg$ to $\overline{\mathrm{End}}(M/p^{n(M)})$, where r is the composite homomorphism

$$\Omega^{-1}M \longrightarrow \widetilde{M/p^{n(M)}} \xrightarrow{\pi} M/p^{n(M)}.$$

We see that $\alpha' = f'$ in $\overline{\mathrm{End}}(M/p^{s-t})$.

In either case f can be realized as a homomorphism that is a strict lifting of α', by the method of Remark 2.3. Now, by the method of lifting idempotents, f can be altered to an idempotent β as required.

https://doi.org/10.4153/CJM-1990-019-0 Published online by Cambridge University Press

5. The case $n(M) = n(G)$. We can characterize the RG-lattices for which $n(M) = n(G)$. This will be a corollary of the following proposition, which is an integral version of the Theorem of Benson and Carlson [**1**] in modular representation theory. R continues to denote a complete discrete valuation ring. We say that $f \in \overline{\mathrm{End}}(M)$ has *maximal trace* if $\mathrm{tr}_R(f) \in R/p^{n(G)}$ has order $p^{n(G)}$. We say that an RG-lattice M is *absolutely indecomposable* if

$$\mathrm{End}(M)/\operatorname{rad}\mathrm{End}(M) \cong R/p.$$

This is stronger than the condition that SM should remain indecomposable for any complete d.v.r. S that is an extension of R. However the two conditions are equivalent if R/p is a perfect field [**2**].

PROPOSITION 5.1. *Let M and N be absolutely indecomposable RG-lattices. Then $\overline{\mathrm{Hom}}(M,N)$ contains an element of order $p^{n(G)}$ if and only if $M \cong N$ and p does not divide* $\mathrm{rank}_R(M)$.

Proof. First of all, we treat the case $M = N$. If $p \nmid \mathrm{rank}_R(M)$ then id_M has maximal trace and so id_M has order $p^{n(G)}$. To prove the converse we suppose that $\overline{\mathrm{End}}(M)$ contains an element of order $p^{n(G)}$. Because of the duality pairing on $\overline{\mathrm{End}}(M)$ that is induced by the trace, there must be an $f \in \overline{\mathrm{End}}(M)$ that has maximal trace. Any element of $\operatorname{rad}\overline{\mathrm{End}}(M)$ is nilpotent and so, when taken modulo p, its trace is zero; hence it does not have maximal trace. Now

$$\overline{\mathrm{End}}(M) = R\,\mathrm{id}_M + \operatorname{rad}\overline{\mathrm{End}}(M),$$

by absolute indecomposability, thus $f = r\,\mathrm{id}_M + j$, $r \in R$, $j \in \operatorname{rad}\overline{\mathrm{End}}(M)$. But $\mathrm{tr}_R(f)$ is maximal and $\mathrm{tr}_R(j)$ is not, thus $\mathrm{tr}_R(\mathrm{id}_M)$ is maximal. Since

$$\mathrm{tr}_R(\mathrm{id}_M) \equiv \mathrm{rank}_R(M) (\mathrm{mod}\, p^{n(G)}),$$

this implies that $p \nmid \mathrm{rank}_R(M)$.

In the general case, the duality pairing shows that if $a \in \overline{\mathrm{Hom}}(M,N)$ has order $p^{n(G)}$ then there is a $b \in \overline{\mathrm{Hom}}(N,M)$ such that $ba \in \overline{\mathrm{End}}(M)$ has maximal trace. By the discussion above, ba must be an isomorphism, hence M is a summand of N and so $M \cong N$ by indecomposability.

The following reformulation is more similar in form to the Theorem of Benson and Carlson.

PROPOSITION 5.2. *Let M and N be absolutely indecomposable RG-lattices. Then* $\mathrm{Hom}_R(M,N)$, *considered as an RG-lattice in the usual way, has the trivial lattice R as a direct summand if and only if $M \cong N$ and p does not divide* $\mathrm{rank}_R(M)$. *The number of summands R is at most one.*

Proof. The RG-lattice $\mathrm{Hom}_R(M,N)$ contains as many direct summands R as

$$\overline{\mathrm{Hom}}(M,N) \cong \hat{H}^0(G;\, \mathrm{Hom}_R(M,N))$$

contains summands $R/p^{n(G)}$, by [**6**] Theorem 1.2.

COROLLARY 5.3. *For an absolutely indecomposable RG-lattice M, we have* $n(M) = n(G)$ *if and only if* $\operatorname{rank}_R(M)$ *is prime to* p.

COROLLARY 5.4. *If* M *is an absolutely indecomposable RG-lattice, then* $M/p^{n(G)}$ *is indecomposable.*

Proof. This follows from Corollary 4.9 unless $n(M) = n(G)$. In the latter case, $\operatorname{rank}_R(M)$ is prime to p by Proposition 5.3. But according to Proposition 4.6, if $M/p^{n(G)}$ is not indecomposable then $p^{n(G)}$ divided $\operatorname{rank}_R(M)$, a contradiction.

In order to deal with the case when the RG-lattice M is not absolutely indecomposable we need to understand the theory of lattices under extension of the ring R. We follow the treatment in [**2**] §30 B. Let $E = \operatorname{End}(M)/\operatorname{rad}\operatorname{End}(M)$, a division ring, and let $\overline{R} = R/p$. For the rest of this section we assume that $\overline{R}$ is perfect. Let K be a maximal subfield of E and let $\overline{S}$ be a finite Galois extension of $\overline{R}$ that contains K. Let

$$\varphi_i : K \longrightarrow \overline{S}, \quad 1 \leqq i \leqq a,$$

be the distinct embeddings of K in $\overline{S}$. There is a homomorphism

$$\Phi : \overline{S} \otimes_{\overline{R}} K \longrightarrow \bigoplus_{i=1}^{a} S_i,$$

where each S_i is a copy of $\overline{S}$, defined by

$$(\Phi(s \otimes k))_i = s\varphi_i(k) \quad \text{for } s \in \overline{S}, k \in K.$$

Φ is an isomorphism of rings and there is a natural transitive action of $\operatorname{Gal}(\overline{S}/\overline{R})$ on $\oplus S_i$ by permuting the S_i that makes Φ equivariant. There exists a complete discrete valuation ring S containing R in which pR is unramified and such that $S/p \cong \overline{S}$, and

$$\begin{aligned} \operatorname{End}(SM)/\operatorname{rad}\operatorname{End}(SM) &\cong \overline{S} \otimes_{\overline{R}} R \cong \overline{S} \otimes_K E \\ &\cong \bigoplus_{i=1}^{a} S_i \otimes_K E \cong \bigoplus_{i=1}^{a} M_t(S_i). \end{aligned}$$

Therefore, by Proposition 4.7, we must have

$$SM \cong \left(\bigoplus_{i=1}^{a} M_i \right)^t$$

with $M_i \ncong M_j$ if $i \neq j$;

$$\operatorname{End}(M_i)/\operatorname{rad}\operatorname{End}(M_i) \cong \overline{S},$$

thus the M_i are absolutely indecomposable. The Galois group $\mathrm{Gal}(S/R)$ permutes the M_i transitively and so they have the same rank, a fact that we shall need later.

From now on we shall write

$$SM \cong \bigoplus_{i=1}^{M} M_i$$

and allow repeated summands. The ring S is free as an R-module and so, upon restricting scalars,

$$M^d \cong \mathrm{Res}_R^S(SM) \cong \bigoplus_{i=1}^{m} \mathrm{Res}_R^S(M_i),$$

where $d = \mathrm{rank}_R(S)$, and hence $\mathrm{Res}_R^S(M_i) \cong M^u$ for some integer $u = d/m$. We shall refer to such a ring S as a *splitting ring* for M.

For the rest of this section we shall write n instead of $n(G)$ and assume that $n \neq 0$.

LEMMA 5.5. *Suppose that M is an RG-lattice such that*

$$\mathrm{rank}_R(M) \equiv \mathrm{rank}_R(\Omega M) \pmod{p^n},$$

and that p does not divide $\mathrm{rank}_R(M)$. *Then $p^nR = 2R$ and the Sylow 2-subgroup of G has order two.*

Proof. By Lemma 3.4,

$$\mathrm{rank}_R(\Omega M) \equiv -\mathrm{rank}_R(M) (\mathrm{mod}\, p^n)$$

and therefore

$$2\ \mathrm{rank}_R(M) \equiv \mathrm{rank}_R(M) + \mathrm{rank}_R(\Omega M) \equiv 0 (\mathrm{mod}\, p^n).$$

Because p^n is a positive rational integer, $p^nR = 2R$; but p^n is the order of the Sylow p-subgroup.

Let C_2 denote the group of order two. The indecomposable RC_2-lattices are R (trivial), R' (rank 1 on which C_2 act as ± 1) and RC_2 (free). The next lemma is immediate.

LEMMA 5.6. *Suppose that p divides 2 and that M is an RC_2-lattice such that $M \cong \Omega M$. Then*

$$M \cong R^a \oplus R'^a \oplus RC_2^c$$

and, in particular, $\mathrm{rank}_R(M)$ *is even.*

PROPOSITION 5.7. *Let M and N be RG-lattices, M indecomposable. If $M/p^n \cong N/p^n$ then we have $M \cong N$ unless p divides 2 and the Sylow 2-subgroup of G has order two.*

Proof. This follows from Proposition 4.4 unless either $n(M)$ or $n(N)$ is equal to n, and in this case $M \cong \Omega N \cong \Omega^2 M$, by Proposition 4.3. But if, say, $n(M) = n$, then

$$n(M) = n(M/p^n) = n(N/p^n) = n(N)$$

and so $n(N) = n$ too. First of all, suppose that M is absolutely indecomposable, so that $\mathrm{rank}_R(M)$ is prime to p by Proposition 5.3. But

$$\mathrm{rank}_R(M) = \mathrm{rank}_R(N) = \mathrm{rank}_R(\Omega M)$$

and thus we can apply Lemma 5.5 to arrive at the conclusion.

In the general case we take an extension S of R that splits both M and N, i.e., $SM \cong \oplus M_i$ and $SN \cong \oplus N_i$ as sums of absolutely indecomposable SG-lattices. Now $SM/p^n \cong SN/p^n$ and so $\oplus M_i/p^n \cong \oplus N_i/p^n$. The summands are indecomposable, by Corollary 5.4, hence $M_1/p^n \cong N_j/p^n$ for some j. But now $M_1 \cong N_j$, by the absolutely indecomposable case (unless p divides 2 etc.). On restricting scalars we see that $M^u \cong N^v$, hence $M \cong N$.

The two RC_2-lattices R and R' are isomorphic modulo 2, which shows that the second possibility in Proposition 5.7 can indeed occur.

PROPOSITION 5.8. *If M is an indecomposable RG-lattice and $n(G) \neq 0$ then $m(M) \neq n(G)$.*

Proof. Suppose that $m(M) = n(G)$: let S be a splitting ring for M, so that $SM \cong \oplus M_i$ as a sum of absolutely indecomposables. Now

$$\overline{\mathrm{Hom}}_{SG}(SM, \Omega^{-1}SM) \cong S \otimes_R \overline{\mathrm{Hom}}_{RG}(M, \Omega^{-1}M)$$

and hence some $\overline{\mathrm{Hom}}(M_i, \Omega^{-1}M_j)$ contains an element of order p^n. Therefore $M_i \cong \Omega^{-1}M_j$ and $\mathrm{rank}_R(M_i)$ is prime to p, by Proposition 5.1. Because the M_i all have the same rank, we can apply Lemma 5.5 to see that $p^n = 2$ and the Sylow 2-subgroup of G has order two. We know that

$$\mathrm{Res}^G_{C_2}(M_i) \cong S^a \oplus S'^b \oplus SC_2^c$$

and that $\mathrm{rank}_R(M_i) = a + b + 2c$ is odd. We shall derive a contradiction by showing that $a = b$. Upon restricting scalars we get

$$\mathrm{Res}^G_{C_2}(M^u) \cong (R^a \oplus R'^b \oplus RC_2^c)^d,$$

hence

$$\mathrm{Res}^G_{C_2}(M) \cong (R^a \oplus R'^b \oplus RC_2^c)^{d/u}.$$

However restricting scalars in the equation $M_i \cong \Omega^{-1}M_j$ leads to $M \cong \Omega^{-1}M$, and so $a = b$ by Lemma 5.6.

PROPOSITION 5.9. *If M is an indecomposable RG-lattice then $M/p^{n(G)}$ is indecomposable.*

Proof. This follows from Corollary 4.9 unless $n(M) = n$, and from Proposition 4.5 unless $M/p^n \cong A \oplus \Omega^{-1}A$. Suppose that both of these hold. Let S be a splitting ring for

$$M : SM \cong \bigoplus_{i=1}^{m} M_i.$$

Now

$$\bigoplus_{i=1}^{m} M_i/p^n \cong SM/p^n \cong SA \oplus \Omega^{-1}SA,$$

hence there is a subset $I \subset \{1, \ldots, m\}$ such that

$$SA \cong \bigoplus_{i \in I} M_i/p^n.$$

On restricting scalars we obtain

$$A^d \cong \bigoplus_{i \in I} M^u/p^n \cong \bigoplus_{i \in I} (A/p^n \oplus \Omega^{-1}A/p^n)^u,$$

hence $A \cong \Omega^{-1}A$ and so

$$M \cong \tilde{A} \cong \Omega^{-1}\tilde{A} \cong \Omega^{-1}M.$$

Therefore $m(M) = n(M) = n$; this is impossible, according to Proposition 5.8, unless $n = 0$, in which case the proposition is trivial.

Example 5.10. Let G be the cyclic group of order p^2, for some prime p. The indecomposable modules for G over $\mathbf{Z}/p$ are easy to describe: there is one in each dimension $1 \leqq i \leqq p^2$; denote it by $L(i)$. The indecomposable $\hat{\mathbf{Z}}_pG$-lattices are harder to describe but they have been classified; in the notation of [**2**] they are as follows.

M	M/p	$\mathrm{rank}_R(M)$	$n(M)$
Z	$L(1)$	1	2
R_1	$L(p-1)$	$p-1$	2
E	$L(p)$	p	1
R_2	$L(p^2-p)$	p^2-p	1
$(R_2, Z; 1)$	$L(p^2-p+1)$	p^2-p+1	2
$(R_2, E; 1)$	$L(p^2)$	p^2	0
$(R_2, E; \lambda^k)$, $1 \leqq k \leqq p-1$	$L(p^2-k) \oplus L(k)$	p^2	1
$(R_2, Z+E; 1+\lambda^k)$, $1 \leqq k \leqq p-2$	$L(p^2-k) \oplus L(k+1)$	p^2+1	2
$(R_2, R_2; 1)$	$L(p^2-1)$	p^2-1	2
$(R_2, R_1; \lambda^k)$, $1 \leqq k \leqq p-2$	$L(p^2-k-1) \oplus L(k)$	p^2-1	2
$(R_2, Z+R_1; 1 \oplus \lambda^k)$, $0 \leqq k \leqq p-2$	$L(p^2-k-1) \oplus L(k+1)$	p^2	1

The reduction M/p is calculated in [**4**]. The number $n(M)$ is most easily calculated using Corollary 5.3. For this one needs to know that all these lattices are absolutely indecomposable. For the first four in the list one can show that

$$\mathrm{End}(M)/\,\mathrm{rad}\,\mathrm{End}(M) \cong \mathbf{Z}/p$$

by using the canonical ring structure on the lattice. The other lattices are all of the form

$$M = (R_2, X; \alpha),$$

an extension of R_2 by X. X is a distinguished sublattice of M, hence we get a homomorphism of rings

$$\psi : \mathrm{End}(M) \longrightarrow \mathrm{End}(R_2),$$

which reduces to a surjection of rings

$$\bar{\psi} : \mathrm{End}(M)/\,\mathrm{rad}\,\mathrm{End}(M) \longrightarrow \mathrm{End}(R_2)/\,\mathrm{rad}\,\mathrm{End}(R_2) \cong \mathbf{Z}/p.$$

But, since the domain is a division ring, this must be an isomorphism.

Using the calculations in [**4**] one can easily see that

$$\widetilde{L(i)} \cong \begin{cases} (R_2, Z+R_1;\ \lambda^{i-1}), & 1 \leqq i \leqq p-1, \\ R_2 \oplus E, & p \leqq i \leqq p^2-p, \\ (R_2, E;\ \lambda^{p^2-i}), & p^2-p+1 \leqq i \leqq p^2-1, \\ 0, & i = p^2. \end{cases}$$

Note that when $(R_2, E;\ \lambda^k)$ or $(R_2, Z+R_1;\ 1+\lambda^{k-1})$ is taken modulo p, it decomposes as $L(k) \oplus \Omega L(k)$, so the second possibilities in Propositions 4.3 and 4.5 can both occur.

References

1. D. J. Benson and J. F. Carlson, *Nilpotent elements in the Green ring*, J. Algebra *104* (1986), 329–350.
2. C. W. Curtis and I. Reiner, *Methods of representation theory*, vol. 1 (Wiley, New York, 1981).
3. K. W. Gruenberg, *Partial Euler characteristics of finite groups and the decomposition of lattices*, Proc. London Math. Soc. *48* (1984), 91–107.
4. A. Jones and G. O. Michler, *On the structure of the integral Green ring of a cyclic group of order p^2*, in *Representation theory II, groups and orders*, Lecture Notes in Math. *1178* (Springer Verlag, Berlin/Heidelberg, 1984).
5. J. M. Maranda, *On p-adic integral representations of finite groups*, Can. J. Math. *45* (1953), 344–355.
6. P. A. Symonds, *Cohomological methods in integral representation theory*, J. Pure and Applied Algebra *56* (1989), 163–176.

McMaster University,
Hamilton, Ontario