FAILURE OF THE KRULL-SCHMIDT THEOREM FOR INTEGRAL REPRESENTATIONS

Irving Reiner

1. The following notation will be used throughout:

G is a finite group of order g;

K is an algebraic number field;

R is the ring of all algebraic integers in K;

P is a prime ideal in R;

R_P is the P-adic valuation ring in $K = \{\alpha/\beta : \alpha, \beta \in R, \beta \notin P\}$;

K_P^* is the P-adic completion of K, and R_P^* the ring of P-adic integers in K_P^*;

$\tilde{R} = \bigcap_{P|g} R_P = \{\alpha/\beta : \alpha, \beta \in R, R\beta + Rg = R\}$.

Let RG denote the group ring of G with coefficients from R. By an RG-*module* we shall always mean a finitely-generated left RG-module which is R-torsion-free, and upon which the identity element of G acts as identity operator. Analogous definitions hold for R_PG-modules, KG-modules, and so forth.

THEOREM 1.1 (Krull-Schmidt). *In any decomposition of a* KG-*module* M *into a direct sum of indecomposable submodules, the indecomposable summands are uniquely determined by* M, *up to* KG-*isomorphism and order of occurrence.*

The standard proof (see, for example, Curtis and Reiner [2, p. 83]) shows that K may be replaced by any commutative ring whose ideals satisfy the descending chain condition.

In the present paper we wish to consider the validity of the Krull-Schmidt theorem for RG-modules. Let us observe at once that the theorem already fails when $G = \{1\}$ if R contains non-principal ideals. Let $J_1, \cdots, J_n$ be ideals of R, and let $\dotplus$ denote the external direct sum operation. As is well known,

$$J_1 \dotplus \cdots \dotplus J_n \cong R \dotplus \cdots \dotplus R \dotplus J_1 \cdots J_n,$$

where $n - 1$ R's occur on the right-hand side.

Returning to an arbitrary finite group G, we might reasonably hope that the non-principal ideals of R are the only source of counterexamples. To avoid the difficulties arising from them, we may work with $\tilde{R}G$-modules instead of RG-modules, where $\tilde{R}$ is the principal ideal ring defined above.

To each RG-module M there corresponds an $\tilde{R}G$-module, denoted by $\tilde{R}M$ and defined by

$$\tilde{R}M = \tilde{R} \otimes_R M.$$

Received March 2, 1962.

This research was supported in part by a contract with the Office of Naval Research.

Clearly, $M \cong N$ implies $\tilde{R}M \cong \tilde{R}N$, but not conversely. On the other hand, $\tilde{R}M \cong \tilde{R}N$ if and only if for each P dividing g, $R_P M \cong R_P N$.

The usefulness of $\tilde{R}$ stems from the following result.

THEOREM 1.2. *An* RG-*module* M *is indecomposable if and only if the corresponding* $\tilde{R}G$-*module* $\tilde{R}M$ *is indecomposable.*

Proof. If M is decomposable, then obviously $\tilde{R}M$ is decomposable. Conversely, let X be an $\tilde{R}G$-direct summand of $\tilde{R}M$, and define $N = M \cap X$. It is easily verified that N is an RG-submodule of M for which $\tilde{R}N = X$, and such that M/N is R-torsion-free.

For each P dividing g, $\tilde{R}$ is a subring of R_P. Since X is a direct summand of $\tilde{R}M$, it follows at once that for each such P, $R_P N$ is an $R_P G$-direct summand of $R_P M$. This implies (see deLeeuw [3], Reiner [6]) that N is an RG-direct summand of M, and the theorem is proved.

The preceding result is quite useful in the determination of indecomposable RG-modules. Furthermore, if $\Sigma^{\oplus} M_i$ is a direct sum of indecomposable RG-modules, then $\Sigma^{\oplus} \tilde{R}M_i$ is a direct sum of indecomposable $\tilde{R}G$-modules. If one could establish a Krull-Schmidt theorem for $\tilde{R}G$-modules, then the $\{M_i\}$ would be unique up to order of occurrence and $\tilde{R}G$-isomorphism.

Our principal result, however, is that the Krull-Schmidt theorem does not hold either for $\tilde{R}G$- or for RG-modules, whenever G contains a normal subgroup of prime index and G is not a p-group. Indeed, in this case not even the R-ranks of the $\{M_i\}$ are uniquely determined.

To conclude this introduction, we recall that the Krull-Schmidt theorem holds for R_P^*G-modules (see Borevich and Fadeev [1], Reiner [7], Swan [8]). It also holds for $R_P G$-modules (see Heller [4]) whenever K is a splitting field for G, that is, whenever KG splits into a direct sum of full matrix algebras over K. Still unsettled is the question as to whether this latter hypothesis may be omitted.

2. In this section we shall show how to construct counterexamples to the Krull-Schmidt theorem for RG-modules, whenever there exist RG-modules with certain properties. We shall write Ext instead of Ext^1_{RG}, for convenience. If M and N are RG-modules, then to each $F \in \mathrm{Ext}(N, M)$ there corresponds an RG-module which is an extension of N by M with extension class F. We denote this module by (M, N; F) or by

$$\begin{pmatrix} M & F \\ & N \end{pmatrix};$$

the latter notation is used to remind us of the matrix representation afforded by this module.

To each RG-module M there corresponds a KG-module denoted by KM, and defined as $K \otimes_R M$.

LEMMA 2.1. *Let* M *and* N *be indecomposable* RG-*modules such that*

$$\mathrm{Hom}_{KG}(KM, KN) = 0 \quad \textit{and} \quad \mathrm{Hom}_{KG}(KN, KM) = 0,$$

and let $F \in \mathrm{Ext}(N, M)$. *Then the* RG-*module* (M, N; F) *is decomposable if and only if* $F = 0$.

Proof. See Heller and Reiner [5, II].

Suppose now that A, B, and C are RG-modules satisfying the following conditions:

(I) The modules KA, KB, and KC are irreducible, and no two of them are isomorphic.

(II) There exist non-zero elements $F \in \mathrm{Ext}(B, A)$ and $F' \in \mathrm{Ext}(C, A)$, such that the orders of F and F' are relatively prime integers.

THEOREM 2.2. *Let* A, B, *and* C *be* RG-*modules satisfying* (I) *and* (II). *Then the modules* A, (A, B; F), (A, C; F') *and* (A, B $\dotplus$ C; F + F') *are indecomposable, and*

$$A \dotplus (A, B \dotplus C; F + F') \cong (A, B; F) \dotplus (A, C; F').$$

Proof. Indecomposability of the above modules follows readily from the preceding lemma. Now let m be the order of F, let n be the order of F', and choose an integer k such that $kn \equiv 1 \pmod m$. In matrix notation, the module $A \dotplus (A, B \dotplus C; F + F')$ may be written as

$$M = \left[\begin{array}{c|ccc} A & & & \\ \hline & A & F & F' \\ & & B & 0 \\ & & & C \end{array}\right].$$

Let

$$X_1 = \left[\begin{array}{c|ccc} I & knI & & \\ \hline & I & & \\ & & I & \\ & & & I \end{array}\right],$$

the symbols I denoting identity matrices of appropriate sizes. Then

$$M_1 = X_1 M X_1^{-1} = \left[\begin{array}{c|ccc} A & 0 & knF & knF' \\ \hline & A & F & F' \\ & & B & 0 \\ & & & C \end{array}\right].$$

The entry knF' lies in Ext(C, A), and it lies in the zero class. Thus if we set

$$X_2 = \left[\begin{array}{c|ccc} I & & & T \\ \hline & I & & \\ & & I & \\ & & & I \end{array}\right],$$

then for a suitable choice of T we obtain the relation

$$M_2 = X_2 M_1 X_2^{-1} = \left[\begin{array}{c|ccc} A & 0 & knF & 0 \\ \hline & A & F & F' \\ & & B & 0 \\ & & & C \end{array}\right].$$

On the other hand, $knF = F$ in $\text{Ext}(B, A)$. Set

$$X_3 = \begin{bmatrix} I & & & \\ -I & I & & \\ & & I & \\ & & & I \end{bmatrix}.$$

Then

$$M_3 = X_3 M_2 X_3^{-1} = \left[\begin{array}{c|ccc} A & 0 & F & 0 \\ \hline & A & 0 & F' \\ & & B & 0 \\ & & & C \end{array}\right].$$

Since $M_3 \cong (A, B; F) \dotplus (A, C; F')$, the theorem is established.

Thus, once we know the existence of RG-modules A, B, and C satisfying (I) and (II), the Krull-Schmidt theorem cannot possibly hold for RG-modules. Indeed, the R-ranks of the indecomposable summands in a direct sum are not uniquely determined by that direct sum.

3. We shall now show the existence of RG-modules for which (I) and (II) hold, provided that the group G satisfies certain hypotheses. One preliminary result will be needed.

LEMMA 3.1. *Let* p *be a prime divisor of the order of* G, *and let* A *be the* RG-*module* R *on which* G *acts trivially. Then there exists an* RG-*module* B *such that*

(i) KB *is irreducible,* $KB \not\cong KA$, *and*

(ii) Ext (B, A) *contains a non-zero element of order* p.

Proof. Suppose the result false, and let P be a prime ideal of R which divides p. Then for each RG-module satisfying (i), the p-primary component of Ext (B, A) is zero, and thus

$$R_P \cdot \text{Ext}(B, A) = 0.$$

This in turn implies that

$$\text{Ext}(R_P B, R_P A) = 0.$$

Let M be the quotient module $R_P G/R_P A$. Then there is an exact sequence of $R_P G$-modules

$$(3.2) \qquad 0 \to R_P A \to R_P G \to M \to 0.$$

We shall show that $\operatorname{Ext}(M, R_P A) \neq 0$. For otherwise, the above sequence splits. If we write $\bar{R} = R/P$, $\overline{M} = M/PM$, and so on, then $\overline{R_P A} \cong \bar{R}$ as $\bar{R}G$-modules, where G acts trivially on $\bar{R}$. If the sequence (3.2) splits, then so does

$$0 \to \bar{R} \to \bar{R}G \to \overline{M} \to 0. \tag{3.3}$$

Let H be a p-Sylow subgroup of G; each $\bar{R}G$-module can be viewed as an $\bar{R}H$-module, and then (3.3) also splits as an exact sequence of $\bar{R}H$-modules. On the other hand, $\bar{R}H$ is an indecomposable $\bar{R}H$-module (see Curtis and Reiner [2, Section 54, Exercise 1], for example), and $\bar{R}G$ is (as $\bar{R}H$-module) a direct sum of [G:H] copies of $\bar{R}H$. We have thus obtained a contradiction to the Krull-Schmidt theorem for $\bar{R}H$-modules. Therefore we have proved that $\operatorname{Ext}(M, R_P A) \neq 0$.

Next we observe that the irreducible module KA cannot occur as a composition factor of KM, since KA occurs with multiplicity 1 as a composition factor of the left regular module KG. Suppose for the moment that KM is itself irreducible. We may write $M = R_P M_0$ for some RG-module M_0, and then

$$\operatorname{Ext}(M, R_P A) = R_P \operatorname{Ext}(M_0, A).$$

This implies that $\operatorname{Ext}(M_0, A)$ has a non-zero p-primary component and so must contain a non-zero element of order p. Choosing $B = M_0$, we obtain the desired module.

On the other hand, if KM is reducible, we can find an R_P-pure $R_P G$-submodule N of M of lower R_P-rank, and then there exists an exact sequence

$$0 \to N \to M \to L \to 0,$$

say. From this we get an exact sequence

$$\operatorname{Ext}(L, R_P A) \to \operatorname{Ext}(M, R_P A) \to \operatorname{Ext}(N, R_P A),$$

and thus at least one of $\operatorname{Ext}(L, R_P A)$ and $\operatorname{Ext}(N, R_P A)$ is non-zero. Continuing in this manner, after a finite number of steps we arrive at an $R_P G$-module V such that KV is irreducible and is a composition factor of KM, and such that $\operatorname{Ext}(V, R_P A) \neq 0$. The rest of the argument is as in the preceding paragraph. This completes the proof.

We are now ready to prove

THEOREM 3.4. *Suppose that the order of* G *has at least two distinct prime divisors, and that* G *contains a normal subgroup of prime index. Then there exist* RG-*modules* A, B, *and* C *satisfying conditions* (I) *and* (II); *in fact,* A *may be chosen to be the* RG-*module* R *on which* G *acts trivially.*

Proof. Let G_0 be a normal subgroup of G, of prime index p, and let H be a cyclic group of order p. Then there is a homomorphism of G onto H with kernel G_0. Let $g \in G$ map onto $\bar{g} \in H$ under this homomorphism. Each RH-module M can be turned into an RG-module, again denoted by M, by defining

$$g \cdot m = \bar{g}m \qquad (g \in G,\ m \in M).$$

Indecomposable RH-modules become indecomposable RG-modules in this process, and irreducibility (as KH- or KG-modules) is also preserved. Furthermore, for a pair of RH-modules M and N,

$$\mathrm{Ext}_{RG}(M, N) = \mathrm{Ext}_{RH}(M, N),$$

where on the left-hand side M and N are viewed as RG-modules.

Choose A to be the RG-module on which G acts trivially. Then A is also an RH-module on which H acts trivially. By the preceding lemma, there exists an RH-module B satisfying conditions (i) and (ii) of that lemma. On viewing B as an RG-module, it is clear that KB is irreducible, $KB \not\cong KA$, and $\mathrm{Ext}_{RG}(B, A)$ contains a non-zero element of order p.

Now let q be a prime divisor of g distinct from p. By Lemma 3.1, there exists an RG-module C such that KC is irreducible, $KC \not\cong KA$, and Ext(C, A) contains a non-zero element of order q. Surely KC and KB are not KG-isomorphic. For if they were, then C could be viewed as an RH-module, and then the order of Ext(C, A) would be a power of p. This completes the proof of the theorem.

For any solvable group G which is not a p-group, the hypotheses of the preceding theorem hold automatically, and thus there exist RG-modules satisfying (I) and (II). We may conjecture that such modules exist for each finite group other than a p-group, but it is not clear how to prove their existence when G is a simple group, for example.

4. Since the Krull-Schmidt theorem fails for $\tilde{R}G$-modules, as well as for RG-modules, it is desirable to know under what conditions two direct sums of indecomposable $\tilde{R}G$-modules are isomorphic. This can be decided in a fairly trivial manner.

We have already remarked that if M and N are a pair of $\tilde{R}G$-modules, then $M \cong N$ if and only if $R_P M \cong R_P N$ for each prime ideal P dividing g. If M is an indecomposable $\tilde{R}G$-module, it may very well happen that $R_P M$ is decomposable as R_P G-module.

For convenience of notation, let b[M] denote the direct sum of b copies of the module M, where b is a positive integer. Now let $M_1, \cdots, M_r, N_1, \cdots, N_s$ be indecomposable $\tilde{R}G$-modules. We would like to know when there exists an isomorphism

$$a_1[M_1] \dotplus \cdots \dotplus a_r[M_r] \cong b_1[N_1] \dotplus \cdots \dotplus b_s[N_s], \tag{4.1}$$

where the $\{a_i\}$ and $\{b_i\}$ are positive integers.

For each P dividing g, let $V_1^P, V_2^P, \cdots$ denote a full set of non-isomorphic indecomposable $R_P G$-modules. Then we may write each $R_P M_i$ as a finite direct sum

$$R_P M_i = m_{i1}^P[V_1^P] \dotplus m_{i2}^P[V_2^P] \dotplus \cdots \qquad (1 \leq i \leq r),$$

where only finitely many non-zero coefficients occur. Likewise, let

$$R_P N_i = n_{i1}^P[V_1^P] \dotplus n_{i2}^P[V_2^P] \dotplus \cdots .$$

Obviously, if

$$\sum_{i=1}^{r} a_i m_{ij}^P = \sum_{i=1}^{s} b_i n_{ij}^P \text{ for each } P \text{ and each } j, \tag{4.2}$$

then (4.1) is valid.

Conversely, if the Krull-Schmidt theorem holds for $R_P G$-modules for each P dividing g, then (4.1) implies (4.2). In particular, (4.1) and (4.2) are equivalent statements whenever K is a splitting field for G.

In the special case where the set $\{V_j^P\}$ is finite for each P, the above considerations are especially useful in determining all relations of the form (4.1).

REFERENCES

1. Z. I. Borevich and D. K. Fadeev, *Theory of homology in groups, II,* Proc. Leningrad Univ. 7 (1959), 72-87.

2. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras,* Wiley, New York, 1962.

3. K. deLeeuw, *Some applications of cohomology to algebraic number theory and group representations* (unpublished).

4. A. Heller, *On group representations over a valuation ring,* Proc. Nat. Acad. Sci. 47 (1961), 1194-1197.

5. A. Heller and I. Reiner, *Representations of cyclic groups in rings of integers, I, II,* Ann. of Math., (to appear).

6. I. Reiner, *On the class number of representations of an order,* Can. J. Math. 11 (1959), 660-672.

7. ———, *The Krull-Schmidt theorem for integral group representations,* Bull. Amer. Math. Soc. 67 (1961), 365-367.

8. R. G. Swan, *Induced representations and projective modules,* Ann. of Math. (2) 71 (1960), 552-578.

University of Illinois
Urbana, Illinois