BULL. AUSTRAL. MATH. SOC. 16A52
VOL. 9 (1973), 11-19.

Twisted group rings and a problem of Faith

John H. Cozzens

A homological characterization is given of when a twisted group ring relative to an automorphism of an arbitrary field has all of its simple right modules injective (= a right V-ring). This answers a question raised by Osofsky. A "Hilbert Theorem 90" type theorem determines the cardinality of the isomorphism classes of one-dimensional simple modules.

The question of the existence of integral domains, not fields, having the property that *every* simple right module is injective was first raised by Faith [3, Problem 17, p. 130]. Any ring with the property that all simple right modules are injective is called a *right* V*-ring*. The first examples of Cozzens [1] of such right V-domains were differential polynomial rings over (Kolchin) universal differential fields, and analogous examples were certain twisted polynomial rings with respect to certain automorphisms over fields. All these domains (including those of Cozzens and Johnson [2]) possessed, however, a unique simple right R-module, and the question naturally arose whether or not there existed right V-domains with a specified number of simple right modules. This question remains open even today, although Osofsky [7] showed that there exist right V-domains with infinitely many simple right modules. Inasmuch as these examples were twisted polynomial rings over fields of finite characteristic (where one might expect some pathology), the question arises to what extent such examples are generally possible.

The main theorem generalizes Osofsky's examples to fields of arbitrary

Received 6 February 1973. Communicated by Carl Faith.

https://doi.org/10.1017/S0004972700042817 Published online by Cambridge University Press

characteristic, and, moreover, for more general types of automorphisms (dispensing with the requirement of Osofsky that the automorphism σ be Frobenius in the sense that $\sigma(a) = a^p$ for all a). Moreover, by developing certain rather obvious functorial isomorphisms for the modules over the twisted group ring (which are trivial generalizations of those for ordinary group rings), we are able to obtain our examples conceptually, and co-incidentally, much more briefly than heretofore.

In doing this we completely solve a question raised by Osofsky [7]:

In the case of differential polynomials, Cozzens *in his thesis characterizes the situation when all simple modules are injective and isomorphic. It seems much more difficult to get a nice description for twisted polynomials. The problem is that* ... .

We completely solve this problem, as we stated, functorially, (Theorem 1), and, moreover, (Theorem 2) determine the cardinality of isomorphism classes of one-dimensional simple modules over the twisted group ring: (the twisted analog of Hilbert's "Theorem 90").

1. The ring $L_G(R)$

Let R be a ring and G a group acting on R . Recall that the twisted group ring $L_G(R)$ over R can be defined as follows:

$$\left(L_G(R),\ +\right) = \left(R(G),\ +\right)$$

where $R(G)$ is the ordinary group ring. Multiplication in $L_G(R)$ is induced by the relations

$$\sigma a = \sigma(a)\sigma\ ,\quad \sigma \in G\ ,\quad a \in R\ ;$$

(here $\sigma(a)$ represents the group action of $\sigma \in G$ on $a \in R$).

It is well known that for $G = \langle \rho \rangle$ (the infinite cyclic group generated by ρ), $L_G(R) = L_\rho(R)$ is a simple pli-(pri-)domain whenever R is a field and ρ is an automorphism of R having infinite period ([4], p. 38 and [5] p. 211). Moreover, in this case, each left (right)

https://doi.org/10.1017/S0004972700042817 Published online by Cambridge University Press

ideal of $L_\rho(R)$ can be generated by an element $a \in L_\rho(R)$ having the form $a = \sum_{i=0}^{n} a_i\rho^i$. Since a fixed R and G will be assumed during the ensuing discussion, we shall replace the symbol $L_G(R)$ with L.

Let $M \in L$-mod, the category of all unital left L-modules and let R be commutative. Note that if we denote the L action of σ on $m \in M$ by $\sigma(m)$, we obtain for each $\sigma \in G$ an additive homomorphism of M satisfying $\sigma(am) = \sigma(a)\sigma(m)$ for all $m \in M$, $a \in R$. Using these observations, it is quite easy to define an L action on $\hom_R(M, N)$ and $M \otimes_R N$ whenever $M, N \in L$-mod.

$\hom_R(M, N)$: for $f \in \hom_R(M, N)$, $\sum_\sigma a_\sigma\sigma \in L$, define

$$\sum_\sigma a_\sigma\sigma \circ f(m) = \sum_\sigma a_\sigma\sigma\left(f\left(\sigma^{-1}(m)\right)\right) , \quad m \in M .$$

$M \otimes_R N$: for $\sum_i m_i \otimes n_i \in M \otimes_R N$, $\sum_\sigma a_\sigma\sigma \in L$, define

$$\sum_\sigma a_\sigma\sigma \circ \sum_i m_i \otimes n_i = \sum_{\sigma,i} a_\sigma\left(\sigma\left(m_i\right) \otimes \sigma\left(n_i\right)\right) .$$

One readily verifies that the above definitions actually endow $\hom_R(M, N)$ and $M \otimes_R N$ with the structure of an L-module. Moreover, this L action induces an L action on $\mathrm{ext}_R^p(M, N)$ and $\mathrm{tor}_p^R(M, N)$ for all $p \geq 0$.

DEFINITION. For $M \in L$-mod, the set $I(M) = \{m \in M \mid \sigma(m) = m, \sigma \in G\}$ will be called the G-invariant subset of M. Other notation, M^G.

REMARK. In general, $I(M)$ is not an L-submodule of M, merely an $I(L)$ submodule of M.

The proofs of the following propositions are, for the most part, routine, and will therefore be omitted.

PROPOSITION 1. *Let* $M, N \in L$-mod. *Then*

https://doi.org/10.1017/S0004972700042817 Published online by Cambridge University Press

$$I\left(\hom_R(M, N)\right) = \hom_L(M, N) .$$

R is naturally a left L-module, the L action the obvious one, namely, for all $a = \sum_\sigma a_\sigma \sigma \in L$, $r \in R$,

$$a \circ r = \sum_\sigma a_\sigma \sigma(r) .$$

We shall always denote this L-module by ${}_L R$.

COROLLARY 1. *For* $M \in L\text{-mod}$, $I(M) \cong \hom_L(R, M)$.

Thus I is a left exact functor and its p-th right derived functor $R^p I$ is given by

$$\left(R^p I\right)(M) = \operatorname{ext}_L^p(R, M) .$$

PROPOSITION 2. *For all* $M, N, P \in L\text{-mod}$, *the natural isomorphism*

$$\hom_R\left(M \otimes_R N, P\right) \approx \hom_R\left(M, \hom_R(N, P)\right)$$

is L-*linear*.

COROLLARY 2. $\hom_L\left(M \otimes_R N, P\right) \approx \hom_L\left(M, \hom_R(N, P)\right)$.

COROLLARY 3. *If* $M \in L\text{-mod}$ *is left* R-*flat, and* $N \in L\text{-mod}$ *is* L *injective, then* $\hom_R(M, N)$ *is* L-*injective*.

PROPOSITION 3. *For* $M \in L\text{-mod}$, M R-*reflexive, the natural isomorphism*

$$M \overset{\psi}{\approx} \hom_R\left(\hom_R(M, R), R\right) = M^{**}$$

is in fact an isomorphism of L-*modules*. ψ *is of course defined by* $\psi(m)[f] = f(m)$ *for all* $f \in \hom_R(M, R)$, $m \in M$.

2. V-rings

Throughout this section, we shall assume that $R = k$ is a field, ρ is an automorphism of k having infinite period, and $G = \langle \rho \rangle$. By a *linear difference equation in* ρ *over* k we mean an equation of the form

https://doi.org/10.1017/S0004972700042817 Published online by Cambridge University Press

$$(*) \qquad \sum_{i=0}^{n} a_i \rho^i(x) = b \ , \quad a_i, \ b \in k \ .$$

If $(*)$ contains *at least* two terms and $b = 0$, the equation is said to be *homogeneous*.

DEFINITION. A ring R is said to be a (left) *V-ring* in case each simple left R-module is injective.

THEOREM 1. *The following are equivalent:*

(1) *L is a V-ring;*

(2) *${}_L k$ is injective;*

(3) *each linear difference equation in ρ over k has a solution in k.*

Moreover, L has a unique simple L module iff each homogeneous linear difference equation has a non-trivial solution in k.

Proof (1) ⇒ (2). This is clear since ${}_L k$ is obviously simple.

(2) ⇒ (3). Let $\sum_{i=0}^{n} a_i \rho^i(x) = b$ be an arbitrary linear-difference equation and set $a = \sum_{i=0}^{n} a_i \rho^i$. The map $f : La \to k$ defined by $a \to b$ is obviously L-linear. By injectivity of ${}_L k$, f extends to L. $f(1)$ is the desired solution.

(3) ⇒ (1). We shall show that each $M \in L$-mod satisfying $\dim_k M < \infty$ is injective which clearly implies the desired result. By Proposition 3, $M \approx M^{**}$ as L modules. Since ${}_k M^*$ is clearly flat and ${}_L k$ injective, $\hom_k(M^*, k) = M^{**}$ is injective in L-mod.

To show that ${}_L k$ is unique, it suffices to show that

$$\hom_L(L/Ld, k) \neq 0$$

for all $d \in L$, $d = \sum_{i=0}^{n} a_i \rho^i$, since each left ideal of L can be

https://doi.org/10.1017/S0004972700042817 Published online by Cambridge University Press

generated by an element of this form. Consider the homogeneous difference equation

$$\sum_{i=0}^{n} a_i \rho^i(x) = 0$$

and let α be a non-trivial solution. Clearly, the map

$$f : L/Ld \to k$$

defined by $l+Ld \to l\cdot\alpha$ is L-linear and nonzero.

Conversely, if ${}_Lk$ is unique and $\sum_{i=0}^{n} a_i \rho^i(x) = 0$ is an arbitrary homogeneous difference equation, set $d = \sum_{i=0}^{n} a_i \rho^i$ and let

$$f : L/Ld \to k$$

be nonzero (f exists since ${}_Lk$ is necessarily an injective *cogenerator*). If $f(1+Ld) = \alpha \neq 0$, $d(\alpha) = 0$ and hence, we have found the desired non-trivial solution to $d(x) = 0$.

REMARK 1. We have actually shown that each cyclic L-module, not isomorphic to L , is injective since these are all clearly finite-dimensional over k .

REMARK 2. It is interesting to note that Johnson has established identical theorems for the ring of linear differential operators, thus attesting to the similarity of these rings at the homological level ([1], [2], and [6]).

3. The one-dimensional case

For simplicity, we shall continue to assume throughout this section that $R = k$ is a field, ρ is an automorphism of k and that $G = \langle \rho \rangle$.

Let $S(1)$ denote the set of all isomorphism classes of one-dimensional (k-dimension, that is), L-modules. If M is one-dimensional, (M) will denote the class of M in $S(1)$. For M, M' and M'' all one-dimensional, $M \otimes_k M'$ is an L-module, and clearly $\dim_k(M \otimes_k M') = 1$. Moreover, it is quite easy to show that

https://doi.org/10.1017/S0004972700042817 Published online by Cambridge University Press

$M \otimes M' \cong M' \otimes M$ and $(M \otimes M') \otimes M'' \cong M \otimes (M' \otimes M'')$ as L-modules (of course the L-action is that defined in Section 1).

Since $(k) \in S(1)$ and $k \otimes_k M \cong M$ in L-mod, the operation $(M) \circ (M') = (M \otimes_k M')$ on $S(1)$ is commutative, associative, and has identity (k). Thus, $(S(1), \circ)$ is a commutative monoid. More can be said:

PROPOSITION 4. *For* $M \in L$-mod, $M^* = \hom_k(M, k)$, $M^* \otimes_k M \overset{\phi}{\cong} \hom_k(M, M)$ *as L-modules where* ϕ *is defined by*

$$\phi(f \otimes m)[m'] = f(m')m$$

for all $f \in M^*$, $m, m' \in M$.

It follows immediately from Proposition 4 that $(S(1), \circ)$ is in fact, a group if $(M)^{-1}$ is defined to be (M^*).

THEOREM 2. *Let* k^* *be the multiplicative group of units of the field* k *and define* $\phi : k^* \to k^*$ *by* $\phi(\alpha) = \alpha^{-1}\rho(\alpha)$. *Then*

$$S(1) \cong k^*/\mathrm{im}\phi .$$

Proof. Let $(M) \in S(1)$ and $m \in M$. Then $\rho(m) = \alpha(m)m$ for a unique $\alpha(m) \in k$. Since $M = km$ for some $m \in M$,

$$\alpha(\beta m)\beta m = \rho(\beta m) = \rho(\beta)\rho(m) = \rho(\beta)\alpha(m)m .$$

Thus, $\alpha(\beta m) \equiv \alpha(m) \bmod \mathrm{im}\phi$. Hence, the correspondence $(M) \mapsto \alpha(m)\mathrm{im}\phi$ is a map $\psi : S(1) \to k^*/\mathrm{im}\phi$. The verifications that ψ is a surjective group homomorphism are routine and will be left to the reader.

Injectivity of ψ. Suppose $(M) \in S(1)$, $M = km$ and $\alpha(m)\mathrm{im}\phi = \psi((M)) = \xi^{-1}\rho(\xi)$ for some $\xi \in k$. By the above, for each $m \in M$, $\alpha(m) = \beta^{-1}\rho(\beta)$ for some $\beta \in k$. Since $\rho(m)$ can be written in the form $\beta\rho(\beta)^{-1}m$ $(\beta = \xi^{-1})$, we see that the map $M \to k$ defined by $\beta m \mapsto 1$ is an L-linear isomorphism, implying that $(M) = (k)$.

4. Applications

Let k be a field of characteristic p and $\rho : k \to k$ be defined by

https://doi.org/10.1017/S0004972700042817 Published online by Cambridge University Press

$\rho(\alpha) = \alpha^p$ for all $\alpha \in k$.

Set $G = \langle \rho \rangle$ and $L = L_G(k)$. In this context, linear difference equations are polynomials of the form

$$\text{(xx)} \qquad \sum_{i=0}^{n} a_i X^{p^i} , \quad a_i \in k .$$

By Theorem 1, if each polynomial of the form

$$\sum_{i=0}^{n} a_i X^{p^i} = b , \quad a_i , b \in k ,$$

has a root in k , then L is a V-ring. This is precisely Proposition 9 of [7] which of course implies Proposition 8 of the same paper. Moreover, in order to have a unique simple L-module, each polynomial of type (xx) containing at least two terms must have a non-trivial root in k . Osofsky [7] exhibited a field k where (1) of Theorem 1 is satisfied but where ${}_L k$ is not unique.

References

[1] John H. Cozzens, "Homological properties of the ring of differential polynomials", *Bull. Amer. Math. Soc.* 76 (1970), 75-79.

[2] John Cozzens and Joseph Johnson, "Some applications of differential algebra to ring theory", *Proc. Amer. Math. Soc.* 31 (1972), 354-356.

[3] Carl Faith, *Lectures on injective modules and quotient rings* (Lecture Notes in Mathematics, 49. Springer-Verlag, Berlin, Heidelberg, New York, 1967).

[4] Nathan Jacobson, *The theory of rings* (Amer. Math. Soc. Surveys, 2. Amer. Math. Soc., New York City, 1943).

[5] Nathan Jacobson, *Structure of rings* (Colloquium Publ. 37, revised ed. Amer. Math. Soc., Providence, Rhode Island, 1964).

[6] Joseph Johnson, Extensions of differential modules over formal power series rings", *Amer. J. Math.* 93 (1971), 731-741.

https://doi.org/10.1017/S0004972700042817 Published online by Cambridge University Press

[7] B.L. Osofsky, "On twisted polynomial rings", *J. Algebra* 18 (1971), 597-607.

Columbia University,
New York,
New York,
USA

and

Department of Mathematics,
Rider College,
Lawrenceville,
New Jersey,
USA.

https://doi.org/10.1017/S0004972700042817 Published online by Cambridge University Press