

INJECTIVE MODULES OVER TWISTED POLYNOMIAL RINGS

BARBARA L. OSOFSKY

Differential polynomial rings over a universal field and localized twisted polynomial rings over a separably closed field of non-zero characteristic twisted by the Frobenius endomorphism were the first domains not divisions rings that were shown to have every simple module injective (see [C] and [C-J]). By modifying the separably closed condition for the polynomial rings twisted by the Frobenius, the conditions of every simple being injective and only a single isomorphism class of simple modules were shown to be independent (see [O]). In this paper we continue the investigation of injective cyclic modules over twisted polynomial rings with coefficients in a commutative field.

Let κ be a field and σ an endomorphism of κ . We can then form the twisted polynomial ring $R = \kappa[X; \sigma]$ with

$$R = \left\{ \sum_{i=0}^n \alpha_i X^i \mid n \in \mathbf{Z}, \alpha_i \in \kappa \right\}$$

under usual polynomial addition and multiplication given by the relation

$$X\alpha = \sigma(\alpha)X.$$

We are interested in non-zero cyclic injective left modules over this ring R .

It is well known (see [J]) that R is a left Euclidean domain using the degree function, and so a left principal ideal domain. Thus a left R -module is injective if and only if it is divisible (see [R, page 70]).

The field κ is an R -module under the action

$$\left(\sum_{i=0}^n p_i X^i \right) \cdot \alpha = \sum_{i=0}^n p_i \sigma^i(\alpha).$$

Using this action, we get

THEOREM 1. *Let κ be a field and $R = \kappa[X; \sigma]$. Then the following are equivalent:*

Received September 9, 1989.

- (1) For every $q \in R$ with constant term $\neq 0$, R/Rq is injective.
- (2) There exists a non-zero $\alpha \in \kappa$ with $R/R(X - \alpha)$ injective.
- (3) For every $t \in \kappa$ and every non-zero $p = \sum_{i=0}^l p_i X^i \in R$, there is an $\alpha \in \kappa$ such that $p \cdot \alpha = t$, that is, the “ σ -polynomial” equation $\sum_{i=0}^n p_i \sigma^i(\alpha) - t = 0$ has a root in κ .
- (4) The right-left analog of any of the above conditions.

Proof. Clearly (1) \Rightarrow (2).

We now examine injectivity of cyclic modules by looking at divisibility properties of quotients of R in order to complete the proof.

It is easy to see that the twisting endomorphism must be an automorphism if a twisted polynomial ring has a non-zero cyclic injective module. In particular, let $q(X) = \sum_{i=0}^k q_i X^i$ be a monic polynomial of degree $k > 0$. Then $X^k \equiv -\sum_{i=0}^{k-1} q_i X^i$ modulo Rq , and Xp has constant term in $\sigma[\kappa]q_0$ modulo Rq_0 for any polynomial p , so any α not in $\sigma[\kappa]q_0$ cannot be divisible by X modulo q . Hence we will assume that σ is onto.

We observe that

$$\sum_{i=0}^l p_i X^i = \sum_{i=0}^l X^i \sigma^{-i}(p_i).$$

Thus there is left-right symmetry and everything we say about left modules also holds on the right.

Now let $p = \sum_{i=0}^l p_i X^i$ and $q = \sum_{j=0}^k q_j X^j$ be two elements of R . The statement that R/Rq is divisible by p means that for every $r \in R$ there is an $s \in R$ such that $r - ps \in Rq$, that is, $R = pR + Rq$. By the left Euclidean algorithm we can take s of degree less than q . By the left and right Euclidean algorithms, to test this divisibility we need only show that every r of degree less than $\min\{\deg(p), \deg(q)\}$ lies in $pR + Rq$. Let $\deg(p) = l$ and $\deg(q) = k$. We then have $R = pR + Rq$ if and only if for all $\sum_{i=0}^{\min(k,l)-1} \tau_i X^i$,

$$\left(\sum_{i=0}^l p_i X^i\right)\left(\sum_{j=1}^{k-1} \alpha_j X^j\right) + \left(\sum_{i=0}^{l-1} \beta_i X^i\right)\left(\sum_{j=0}^k q_j X^j\right) = \sum_{i=0}^{\min(k,l)-1} \tau_i X^i.$$

For convenience, we also set $\tau_i = 0$ for $i > \min(k, l) - 1$.

We thus get the systems (linear over $\kappa[X; \sigma]$) of $k + l$ equations in $k + l$ variables

$$\left(\sum_{i+j=n} p_i \sigma^i(\alpha_j)\right) + \left(\sum_{i+j=n} \beta_i \sigma^i(q_j)\right) = \tau_n \quad \text{for } 0 \leq n \leq k + l - 1.$$

We abbreviate this system

$$(*) \quad \mathbf{A} \cdot \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{k-1} \\ \beta_0 \\ \vdots \\ \beta_{l-1} \end{pmatrix} = \begin{pmatrix} \tau_0 \\ \tau_1 \\ \vdots \\ \tau_{k-1} \\ \tau_k \\ \vdots \\ \tau_{k+l-1} \end{pmatrix}$$

where \mathbf{A} is the $(k + l) \times (k + l)$ matrix

$$\begin{pmatrix} p_0 & 0 & & & 0 & q_0 & 0 & & & 0 \\ p_1X & p_0 & 0 & & & q_1 & \sigma(q_0) & 0 & & \\ p_2X^2 & p_1X & p_0 & & & q_2 & \sigma(q_1) & \sigma^2(q_0) & & \\ \vdots & \vdots & \vdots & \ddots & & \vdots & \vdots & \vdots & \ddots & \\ p_iX^i & & \cdots & p_0 & 0 & q_i & & \cdots & \sigma^i(q_0) & 0 \\ p_{k-1}X^{k-1} & & & & p_0 & q_{k-1} & & & & \\ p_lX^l & & \cdots & \vdots & p_1X & q_k & & \cdots & & \sigma^{l-1}(q_0) \\ \vdots & & \ddots & \vdots & \vdots & \vdots & & \ddots & \vdots & \sigma^{l-1}(q_1) \\ \vdots & & \ddots & \vdots & p_nX^n & \vdots & & \ddots & \vdots & \\ \vdots & & \ddots & \vdots & \vdots & \vdots & & \ddots & \vdots & \\ 0 & & & & p_lX^l & 0 & & & & \sigma^{l-1}(q_k) \end{pmatrix}$$

pictured here as though $k = l$. Modifications for $k \neq l$ are very minor.

The significant properties of \mathbf{A} are that the first k columns correspond to p and the last l columns correspond to q . The left $(k + l) \times k$ submatrix has the constant p_0 on its diagonal, zeros above the diagonal, and multiples of X below the diagonal. The right $(k + l) \times l$ submatrix also has zeros above its diagonal and its bottom l rows form an upper triangular submatrix with diagonal entries $\sigma^i(q_k)$. These entries $\sigma^i(q_k)$ are also on the diagonal of \mathbf{A} .

Let \mathbf{A}_1 denote the upper left $k \times k$ submatrix of \mathbf{A} .

Since q has degree k , $\sigma^i(q_k) \neq 0$ for $0 \leq i \leq l - 1$. Also,

$$XR + Rq = R \iff RX + Rq = R \iff q_0 \neq 0$$

so we may take $p_0 \neq 0$ and $q_0 \neq 0$ in testing to see if R/Rq is injective.

We now proceed using Gaussian elimination in a manner similar to that used in [O].

By pivoting successively on $\sigma^{l-1}(q_k), \sigma^{l-2}(q_k), \dots, q_k$ we can make every non-diagonal entry in the last l columns 0 (and the diagonal entries 1). In this process, all polynomials which are added to the entries in the upper left $k \times k$ submatrix A_1 are multiples of X . Let a_i denote the i th row of A_1 , and assume $\sum_{i=0}^k r_i a_i = 0$. If some $r_i \neq 0$, there must be a j with r_j of smallest order (the smallest power of X which occurs with non-zero coefficient). Then the j th entry of $\sum_{i=0}^k r_i a_i$ contains a term of smallest order from a_j which cannot be cancelled by any other term in $\sum_{i=0}^k r_i a_i$, a contradiction. By a series of elementary row operations using the Euclidean algorithm to decrease degree, we can bring A_1 into lower echelon form, and the preceding discussion shows that we can never get a zero polynomial on the diagonal, as that would give us a zero row.

Doing the same row operations on the column of constants in (*) as were done in the matrix A gives us a new system

$$(**) \quad L \cdot \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{k-1} \\ \beta_0 \\ \vdots \\ \beta_{l-1} \end{pmatrix} = \begin{pmatrix} \hat{\tau}_0 \\ \hat{\tau}_1 \\ \vdots \\ \hat{\tau}_{k-1} \\ \hat{\tau}_k \\ \vdots \\ \hat{\tau}_{k+l-1} \end{pmatrix}$$

where L is a lower triangular matrix with non-zero polynomials on the diagonal and the $\hat{\tau}_i$ are obtained from the τ_i by multiplication by an invertible matrix. In summary, this system has a solution for any $\{\hat{\tau}_i | 0 \leq i \leq k + l - 1\} \Leftrightarrow pR + Rq = R$.

We note that the R -module κ is isomorphic to $R/R(X - 1)$. Statement (3) is precisely the statement that κ is a divisible R -module. We can now complete the proof of the theorem.

Given (3), the equations (**) can be solved by forward substitution, so (3) \Rightarrow (1).

For (2) \Rightarrow (3), we take $k = 1$ and $q = X - \alpha$ with $\alpha \neq 0$. Then

$$A = \begin{pmatrix} p_0 & \alpha & & & & \\ p_1X & 1 & \sigma(\alpha) & & & \\ p_2X^2 & 0 & 1 & & & \\ \vdots & & & \ddots & & \\ \vdots & & & & \ddots & \sigma^{t-1}(\alpha) \\ p_tX^t & & & & & 1 \end{pmatrix},$$

and L has $(1, 1)$ entry $\sum_{i=0}^t (-1)^i p_i \prod_{j=0}^{i-1} \sigma^j(\alpha) X^i$. If $\alpha \neq 0$ and $R/R(X - \alpha)$ is divisible by all non-zero polynomials p , then the coefficients of the $(1, 1)$ entry of L are arbitrary, so every “ σ -polynomial” equation must have a solution, and $(2) \Rightarrow (3)$.

Since κ is commutative, (3) is left-right symmetric, so one gets (4) by this symmetry. □

A module over a ring or object in an $\mathcal{AB5}$ category is called CS (or extending, or having property C1, or ...) provided every submodule is essential in some direct summand. In [O-S], the condition that every cyclic R -module is CS is studied as an example to illustrate the main result. That paper contains a sketch of a proof that every cyclic R -module is CS implies that, for any simple R -module M with injective hull $E(M)$, if the annihilators of non-zero elements of M are not two-sided, then $E(M)/M$ is semi-simple. Theorem 1 enables us to complete the discussion of when every cyclic R -module is CS begun in [O-S], filling in details just sketched there.

LEMMA A. *Let $\alpha \in \kappa$. Then $R/R(X - \alpha)$ is isomorphic to $R/R(X - 1) \Leftrightarrow \alpha = \sigma(\beta)/\beta$ for some $\beta \neq 0$ in κ .*

Proof. $R/R(X - 1) \cong R/R(X - \alpha) \Leftrightarrow \exists \beta \in \kappa \setminus 0$ with $(X - 1)\beta \in R(X - \alpha) \Leftrightarrow \exists \beta \in \kappa \setminus 0$ with $\sigma(\beta)X - \beta \in R(X - \alpha) \Leftrightarrow \exists \beta \in \kappa \setminus 0$ with $\alpha = \beta/\sigma(\beta)$. □

LEMMA B. *Let U and S be modules over some arbitrary ring \mathcal{R} with 1. Assume $S = \mathcal{R}s$ is simple, and U is a uniserial module with a unique composition series $U \supset U_1 \supset U_2 \supset 0$, with $S \cong U_1/U_2$. Then $M = U \oplus S$ is not CS.*

Proof. Let $u + U_2$ map to s in the isomorphism from U_1/U_2 to S , where $u \in U_1$. Since U is uniserial, $\mathcal{R}u$ must have composition length 2, and the same is true for $\mathcal{R}(u + s) = N \subset M$. We observe that $\text{socle}(N) = U_2$ and $N \oplus S$ is the only submodule of M of length 3 containing N . Thus N has no proper essential extensions in M . However, N cannot be

a direct summand of M since M/N is a direct sum of two simple modules whereas the socle of M is $U_2 \oplus S$ and $U_2 \subset N$. □

LEMMA C. *Let \mathcal{R} be a principal left ideal domain, and let p and q generate maximal left ideals of \mathcal{R} . If M is a simple \mathcal{R} -module not divisible by p and $\mathcal{R}/\mathcal{R}p$ is not divisible by q , then \mathcal{R} has a uniserial module $\mathcal{R}u \supset U_1 \supset U_2 \supset 0$ of composition length 3 with $U_1/U_2 \cong \mathcal{R}/\mathcal{R}p$.*

Proof. Let $E = E(M)$ denote an injective hull of M . Let $m \in M \setminus pM$. Then there is an $x \in E$ with $px = m$. Since \mathcal{R} is hereditary, E/M is injective. Then $\mathcal{R}x/(\mathcal{R}x \cap M)$ has an injective hull E' in E/M . In E there is an element $u \notin \mathcal{R}x$ with $u + M \in E'$ and $\mathcal{R}qu + M = \mathcal{R}x + M$. Then $\mathcal{R}u \supset \mathcal{R}x \supset M \supset 0$, and one can easily check that $\mathcal{R}u$ has the required properties. □

THEOREM 2. *Let κ be a field and $R = \kappa[X; \sigma]$. Then the following are equivalent:*

- (1) *For every $q \in R$, R/Rq is CS.*
- (2) *Either σ is the identity or for every $q \in R$ with constant term $\neq 0$, R/Rq is injective.*

Proof. (2) \Rightarrow (1) is reasonably elementary. The ring itself is a uniform module and so CS, and if σ is the identity, other cyclics are CS by the basis theorem for finitely generated Abelian groups. If $p \in R \setminus 0$, $p = qX^j = X^j q'$ for some $j \in \omega$ and $q, q' \in R$ with constant term $\neq 0$. Since R is a pid, $R = RX^j + Rq'$ and R/Rp has a natural map onto $R/RX^j \oplus R/Rq'$. Computing κ -dimensions shows that this map is one to one. We observe that R/RX^j is quasi-injective and R/Rq' is injective and there are no non-zero homomorphisms between submodules of one and submodules of the other. Thus R/Rq is quasi-injective and so CS.

To show that (1) \Rightarrow (2) we may assume that σ is not the identity. Assume R contains a q' with non-zero constant term such that $M = R/Rq'$ is not divisible by $X - 1$. Then since M is a finite dimensional vector space over κ , it is an R -module of finite length, and so has a simple composition factor which is not divisible by $p = X - 1$. Thus we may assume that M is simple. By Theorem 1, $R/R(X - 1)$ cannot be injective or M would be, so $R/R(X - 1)$ is not divisible by some non-zero irreducible polynomial q . By Lemma C, there is an $s \in R$ with $R/Rs \cong Ru$ uniserial of length 3 with middle factor isomorphic to $R/R(X - 1)$. Since

R/Rs has only one maximal submodule, there is at most one $\alpha \in \kappa$ with $R(X - \alpha) \supset Rs$. We are assuming that σ is not the identity, so there is a $\beta \in \kappa$ with $\sigma(\beta) \neq \beta$. Then at least one $\gamma \in \{1, \beta/\sigma(\beta)\}$ satisfies $s \notin R(X - \gamma)$. By Lemma A, $R/R(X - \gamma) \cong R/R(X - 1)$. Then $Rs + R(X - \gamma) = R$, so $R/(Rs \cap R(X - \gamma)) \cong R/Rs \oplus R/R(X - \gamma)$ is not CS by Lemma B.

We conclude that every cyclic CS implies that for all q with constant term $\neq 0$ (and indeed for every non-zero q), R/Rq is divisible by $X - 1$, that is, $(X - 1)R + Rq = R$. But that same equation may be interpreted as saying that the right R -module $R/(X - 1)R$ is divisible by every non-zero $q \in R$, and so injective. By Theorem 1, for every q with constant term $\neq 0$, R/Rq is injective. □

Remark. If every cyclic R -module is CS and σ is not the identity, then for every polynomial q with non-zero constant term, $qR + Rq = R$. In particular, R cannot have any two-sided ideals other than R, RX^m , and 0 . It is well known that the two-sided ideals of R are generated by powers of X and by polynomials in X^n with coefficients in the fixed field of σ , where σ^n is the identity. Thus every cyclic R -module CS and σ of finite order imply that σ is of order 1, i.e. equal to the identity.

To get a feel for what “ σ -polynomial” equations look like, it pays to look at some examples. First, let us assume that κ is a perfect field of characteristic $p > 0$ and σ is the Frobenius map $\alpha \mapsto \alpha^p$. Then the equation

$$\left(\sum_{i=0}^n q_i X^i\right) \cdot \alpha = \beta \quad \text{becomes} \quad \sum_{i=0}^n q_i \alpha^{p^i} = \beta$$

which is an ordinary polynomial equation in α . Note that polynomial is considerably different than the original polynomial in R . Among other things, it has ordinary derivative the constant q_0 so it is separable if $q_0 \neq 0$, and its degree is a power of p . As observed in [O], all such ordinary polynomials may have roots in κ without κ being algebraically closed. If κ is finite, then σ is of finite order so by the above remark, some cyclic R -module, and hence the R -module κ , is not injective. In particular, the annihilator in κ of $X - 1$ is of order p , so the set of elements divisible by $X - 1$ has order $|\kappa|/p$.

The above example may be somewhat misleading, since the operation of an element of R on α gives a polynomial in α . So let us now look at the case that $\kappa = \mathbb{C}$, the field of complex numbers, and $\sigma(z) = \bar{z}$, the

complex conjugate of z . Then σ is of order 2, and $(X - 1) \cdot \mathbf{C} = \mathbf{R}i$. If we wish to extend \mathbf{C} to a field κ_1 in which every equation of the form $(X - 1) \cdot \kappa_1 = \beta$ has a root, adjoin a transcendental τ to \mathbf{C} and extend complex conjugation to $\sigma: (\sum_{j=0}^n q_j \tau^j) \mapsto (\sum_{j=0}^n \bar{q}_j (\tau + 1)^j)$. Clearly σ is an automorphism of $\mathbf{C}[\tau]$ and so of κ_1 . Then κ_1 is an R - \mathbf{R} bimodule, and $(X - 1) \cdot \tau = 1$ so $(X - 1) \cdot \kappa_1 \supseteq \mathbf{R}$. Computations show that applying $(X - 1) \cdot$ to higher powers of τ and i times those powers alternately gives real and imaginary parts of coefficients of every power of τ , so one gets that κ_1 is divisible by $X - 1$. It is not, however, divisible by $X - \tau$. If $q = \sum_{i=0}^n q_i X^i \in R$ has $q_0 q_n \neq 0$, and $q \cdot \alpha = \beta$ has no solution in κ_1 , we may force it to have a solution in an extension of κ_1 by adjoining new transcendentals $\{x_0, \dots, x_{n-1}\}$ to κ_1 and extending σ to this new κ_2 by $\sigma: x_i \mapsto x_{i+1}$ for $0 \leq i \leq n - 2$ and $\sigma: x_{n-1} \mapsto (\beta - \sum_{i=0}^{n-1} q_i x_i) / q_n$. Iterating this procedure carefully will enable us to get a " σ -algebraic closure" of the original field for which the new field is injective over the new R . It will look nothing like the algebraically closed field \mathbf{C} .

We conclude with an obvious conjecture, namely, if some R/R_q is injective with q having non-zero constant term, then so is $R/R(X - 1)$. A computational proof seems very difficult, as not all polynomials appear on the diagonal of the lower triangular \mathbf{L} in equation (**).

REFERENCES

- [C] J. H. Cozzens, Homological properties of the ring of differential polynomials, *Bull. Amer. Math. Soc.*, **76** (1970), 75–79.
- [C-J] J. H. Cozzens and J. L. Johnson, An application of differential algebra to ring theory, *Proc. Amer. Math. Soc.*, **31** (1972), 354–356.
- [J] N. Jacobson, "The theory of rings," American Mathematical Soc., Providence, 1943.
- [O] B. L. Osofsky, On twisted polynomial rings, *J. Algebra*, **4** (1971), 597–607.
- [O-S] B. L. Osofsky and P. F. Smith, Cyclic modules whose quotients have complements direct summands, *J. Algebra*, to appear.
- [R] J. J. Rotman, "An introduction to homological algebra," Academic Press, Inc., Orlando San Diego, 1979.

*Department of Mathematics
Rutgers University
New Brunswick, NJ 08903
U.S.A.*