View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

JOURNAL OF ALGEBRA 18, 597–607 (1971)

On Twisted Polynomial Rings

B. L. OSOFSKY*

Department of Mathematics, Rutgers University, New Brunswick, New Jersey 08903

Communicated by I. N. Herstein

Received August 30, 1970

Twisted polynomial rings and localizations thereof have been used as counterexamples to many conjectures. In this paper we extend the results of Cozzens in Ref. [1], who was concerned with the following two properties:

(P_1) Every simple R module is injective.

(P_2) There is only one isomorphism class of simple R modules.

In addition, we look at

(P_3) There exist infinitely many nonisomorphic simple R modules.

By suitably modifying the field of a twisted polynomial ring, we show that P_1 and P_2 are completely independent, and that P_1 and P_3 may simultaneously hold. We also show that P_3 may hold on the right but not on the left.

The following meanings of $p, F, \bar{R}, R$, and σ will be assumed throughout the entire paper.

Let F be a field of characteristic $p > 0$, and let $\sigma : F \to F$ be the endomorphism of F defined by $\sigma(\alpha) = \alpha^p$ for all $\alpha \in F$. Let $\bar{R}$ be the ring of twisted polynomials with coefficients on the left,

$$\bar{R} = F[X; \sigma] = \left\{ \sum_{i=0}^{n} \alpha_i X^i \;\middle|\; \alpha_i \in F, n \in \omega \right\},$$

where addition is polynomial addition, multiplication is defined by the associative and distributive laws, and

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

for all $\alpha \in F$.

$\bar{R}$ is a principal left ideal domain with left Euclidean algorithm with precisely one two-sided ideal, viz., (X). (See Jacobson, Ref. [3]). Moreover,

* The author gratefully acknowledges financial support from the National Science Foundation under grant GP 19856.

for every $r \in \bar{R}$, there exists $s \in \bar{R}$ such that $Xr = sX$, so that one may form $R =$ the left ring of quotients of $\bar{R}$ with respect to X, viz.,

$$R = \left\{ X^{-j} \left(\sum_{i=0}^{n} \alpha_i X^i \right) \middle| j, n \in \omega, \alpha_i \in F \right\}.$$

R is a simple ring, and, being the localization of a principal left ideal domain, is also a principal left ideal domain. Moreover, R may be considered as the localization of the right twisted polynomial ring $(F[X^{-1}; \sigma])_r$ with respect to X^{-1}, so R is also a principal right ideal domain although $\bar{R}$ is not unless F is perfect.

Cozzens shows in Ref. [1] that R has properties P_1 and P_2 if F is algebraically closed. By further analysis of the situation, we show the complete independence of these two properties.

1. Number of Simple Modules

Proposition 1. *Let*

$$r = X^{-j} \left(\sum_{i=0}^{n} \alpha_i X^i \right) \in R.$$

Then $Rr \subseteq R(X - \gamma)$ for some nonzero $\gamma \in F$ if and only if γ is a nonzero root of the polynomial

$$P(Y) = \sum_{k=0}^{n} \alpha_{n-k} Y^{(p^{n-k}-1)/(p-1)}.$$

Proof. $\sum_{i=0}^{n} \alpha_i X^i = (\sum_{i=0}^{n-1} \beta_i X^i)(X - \gamma)$ if and only if

$$(*) \begin{cases} \alpha_n = \beta_{n-1}, & \alpha_0 = -\beta_0 \gamma, \\ \alpha_k = \beta_{k-1} - \beta_k \sigma^k(\gamma) & \text{for} \quad 1 \leqslant k \leqslant n-1. \end{cases}$$

Assume the equations $(*)$ and that

$$\beta_{n-j} = \sum_{k=0}^{j-1} \alpha_{n-k} \gamma^{(\sum_{l=n-j+1}^{n-k-1} p^l)} \qquad \text{for} \quad j \leqslant n-1,$$

where a sum with smaller top than bottom index is equal to zero. This is true if $j = 1$ by the first equation of $(*)$.

Then

$$\begin{aligned}\beta_{n-(j+1)} &= \alpha_{n-j} + \beta_{n-j}\gamma^{p^{n-j}} \\ &= \alpha_{n-j} + \sum_{k=0}^{j-1} \alpha_{n-k}\gamma^{(p^{n-j}+\sum_{l=n-j+1}^{n-k-1} p^l)} \\ &= \alpha_{n-j}\gamma^0 + \sum_{k=0}^{j-1} \alpha_{n-k}\gamma^{(\sum_{l=n-(j+1)+1}^{n-k-1} p^l)} \\ &= \sum_{k=0}^{j} \alpha_{n-k}\gamma^{(\sum_{l=n-(j+1)+1}^{n-k-1} p^l)}.\end{aligned}$$

By induction,

$$\beta_0 = \sum_{k=0}^{n-1} \alpha_{n-k}\gamma^{(\sum_{l=1}^{n-k-1} p^l)} = -\alpha_0\gamma^{-1}$$

and multiplying by γ and transposing gives γ is a root of $P(Y)$ since

$$\sum_{l=0}^{m} p^l = (p^m - 1)/(p - 1).$$

If γ is a root of $P(Y)$, define $\beta_{n-1} = \alpha_n$ and β_{n-j} inductively by $(*)$. The above calculations then show the required factorization holds, since β_0 indeed equals $-\alpha_0\gamma^{-1}$.

We make two observations about $P(Y)$.

(i) $P(Y) = P'(Y)Y + \alpha_0$, so $\alpha_0 \neq 0$ implies P has all distinct roots.

(ii) The degree of $P(Y)$ is relatively prime to p since each nonzero exponent of Y is congruent to 1 modulo p.

PROPOSITION 2. *Let* $\alpha, \beta \in F - \{0\}$. *Then*

$$R/R(X - \alpha)X^m \approx R/R(X - \beta)$$

(resp. $\bar{R}/\bar{R}(X - \alpha)X^m \approx \bar{R}/\bar{R}(X - \beta)$) *if and only if there is a* $j \in \omega$ ($m = 0$ *and for* $j = 0$) *such that the polynomial*

$$Q(Y) = Y^{p-1} - \alpha^{p^j}\beta^{-1}$$

has a root in F.

Proof. Any $r \in \bar{R}$ is of the form $r = \rho + q(X - \beta)$ for some $\rho \in F$, $q \in \bar{R}$. Hence $R(X - \beta)$ $(\bar{R}(X - \beta))$ is maximal. $\bar{R}(X - \alpha)X^m$ is maximal if and only if $m = 0$. Moreover, since $R(X - \alpha)$ is a maximal left ideal of R

and since the map $R \to R/R(X-\alpha)$ given by $1 \to X^{-m} + R(X-\alpha)$ has kernel $R(X-\alpha)X^m$, $R/R(X-\alpha)X^m \approx R/R(X-\alpha)$ so we may assume $m = 0$ in this case also.

Now $R/R(X-\alpha) \approx R/R(X-\beta)$ if and only if there exists $j \in \omega$ ($j = 0$ in the case of $\bar{R}$) and $\rho \in F - \{0\}$ such that

$$(X-\alpha)X^{-j}\rho \in R(X-\beta).$$

But $(X-\alpha)X^{-j} = X^{-j}(X - \alpha^{p^j})$, so this holds if and only if

$$(X - \alpha^{p^j})\,\rho \in \bar{R} \cap R(X-\beta) = \bar{R}(X-\beta)$$

if and only if there exists $\tau \in F - \{0\}$ such that

$$\rho^p X - \alpha^{p^j}\rho = \tau X - \tau\beta,$$

or

$$\tau = \rho^p, \qquad \rho(\rho^{p-1}\beta - \alpha^{p^j}) = 0.$$

We observe that, in the case of R, one cannot necessarily assume $j = 0$ unless $p = 2$. For example, let p be odd, F' a purely transcendental extension of $\mathbf{Z}/p\mathbf{Z}$, F'' the separable closure of F', and $F = F''[\alpha^{1/p}]$ for some $\alpha \in F' - \mathbf{Z}/p\mathbf{Z}$. Then $Y^{p-1} - \alpha^{1/p}$ has no root in F, but $Y^{p-1} - \alpha$ does.

Just as for P, Q has no multiple roots and degree relatively prime to p.

In order to use the above calculations, we need a way of obtaining particular fields in which polynomials which need roots have them.

Let q be a prime integer, and let K be any field with algebraic closure $\bar{K}$. Let

$$\mathfrak{F} = \{L \mid L \text{ a field, } K \subseteq L \subseteq \bar{K}, \text{ and } l \in L \Rightarrow \text{degree } l \text{ over } K \text{ is relatively prime to } q\}.$$

$K \in \mathfrak{F}$, and $\mathfrak{F}$ is clearly inductive.

Definition. A q-field over K is a maximal element of $\mathfrak{F}$.

Proposition 3. *Let L be a q-field over K, and let $f \in L[X]$ have degree relatively prime to q. Then f has a root in L. If $g \in K[X]$ is irreducible in $K[X]$ and has degree divisible by q, then g has no root in L.*

Proof. Since all of the irreducible factors of f over L cannot have degree divisible by q, one, say f_0, has degree relatively prime to q. Let θ be a root of f_0 in $\bar{K}$, and let $\phi \in L[\theta]$. Then ϕ is contained in $K_0[\theta]$ where K_0 contains all the coefficients of f_0 and is a finite extension of K in L. $K_0[\theta]$ is of K-dimension relatively prime to q since its separable part is generated by a single element of L and dimensions multiply. Then degree ϕ divides $(\deg f_0)(K\text{-dim } K_0)$ which is relatively prime to q. Thus $L[\theta] \in \mathfrak{F}$, and by the maximality of L, $L[\theta] = L$, i.e., $\theta \in L$ is a root of f.

The second part is immediate from the definition of $\mathfrak{F}$. It is possible that g may factor over L, but all such factors must have degree divisible by q.

PROPOSITION 4. *Let K be any field of characteristic $p > 0$, and let F be a p-field over K. Then R has only one isomorphism class of simple left R modules, and $\bar{R}$ has two.*

Proof. Let $X^{-j}(\sum_{i=0}^{n} \alpha_i X^i)X^m$, $\alpha_0 \neq 0$, generate a maximal left ideal of R (for $\bar{R}$, set $j = 0$). Since X^{-j} is a unit in R we may ignore the X^{-j}. By Propositions 3 and 1, $\sum_{i=0}^{n} \alpha_i X^i$ must be linear, so every maximal left ideal of R ($\bar{R}$) is generated by an element of the form $(X - \gamma)X^m$, $\gamma \in F - \{0\}$ (or $= \bar{R}X$). By Propositions 3 and 2, $R/R(X - \gamma)X^m \approx R/R(X - 1)$. (In the case of $\bar{R}$, one has also the possibility $\gamma = 0$ and the unique non-faithful simple $\bar{R}/\bar{R}X$.)

We can also show that roots of all P and Q occurring in Propositions 1 and 2 must exist for R to have only one (and $\bar{R}$ two) isomorphism class of simples.

PROPOSITION 5. *Let $r = \sum_{i=0}^{n} \alpha_i X^i$ generate a maximal ideal of R (or $\bar{R}$) where $\alpha_n \alpha_0 \neq 0$, $n > 1$. Then $R/Rr \not\approx R/R(X - \gamma)$ for any $\gamma \neq 0 \in F$.*

Proof. Any $s \in R$ is of the form $X^{-j}t + qr$, $q \in R$, $j \in \omega$, $t \in \bar{R}$, degree $t \leqslant n - 1$. Then $(X - \gamma)s \in Rr$ if and only if $(X - \gamma^{p^j})t$ is a polynomial of degree $\leqslant n$ in Rr. Since r has constant term $\neq 0$, the only such polynomials are of the form αr, $\alpha \in F$. But then $Rr \subsetneq Rt$, a contradiction.

Although R has enough symmetry to ensure that there is only one isomorphism class of left simple R modules if and only if there is only one isomorphism class of right simple R modules (if and only if the polynomials $P(Y)$ and $Q(Y)$ in Propositions 1 and 2 always have roots), the situation with $\bar{R}$ is quite different unless F is perfect (so symmetry again holds). Although roots of all P and Q insure only two nonisomorphic simple left $\bar{R}$ modules, it is possible to have infinitely many simple right $\bar{R}$ modules.

PROPOSITION 6. *Let $\{\beta_i \mid i \in \mathscr{I}\}$ be a basis for F over F^p. Then for any $\{\gamma_i \mid i \in \mathscr{I}\} \subseteq F$, $I = \sum \oplus (\beta_i X - \gamma_i)\bar{R}$ is a maximal right ideal of $\bar{R}$.*

Proof. Let $r = \sum_{i=0}^{n} \alpha_i X^i \in \bar{R}$, $\alpha_n \neq 0$, $n \neq 0$. Then $\alpha_n = \sum_{j=1}^{k} \beta_{i_j} \delta_j^p$ for some $\{\delta_j\} \subseteq F$, $\{i_j\} \subseteq \mathscr{I}$, and $r - \sum_{j=1}^{k} (\beta_{i_j} X - \gamma_{i_j}) \delta_j X^{n-1}$ has degree $< n$. Hence $r \in \bar{R}$ is congruent to some constant modulo I. Moreover, $\sum_{j=1}^{k} (\beta_{i_j} X - \gamma_{i_j}) r_j \in F$ with some $r_j \neq 0$ is impossible since the β_{i_j} are linearly independent modulo F^p. Hence I is proper and the sum is direct.

Proposition 7. *Assume that the F^p dimension of F is equal to the cardinality of $F = \aleph$, and that $\mathscr{I}$ is the first ordinal with cardinality $\aleph$. Then $\bar{R}$ has at least $\aleph$ nonisomorphic simple right $\bar{R}$ modules.*

Proof. Set $\gamma_{i,0} = 0$, $I_0 = \sum (\beta_i X - \gamma_{i,0})\bar{R}$. Let $j < \mathscr{I}$, and assume for all $k < j$, $I_k = \sum (\beta_i X - \gamma_{i,k})\bar{R}$ has been defined such that $R/I_k \approx R/I_{k'}$ if and only if $k = k'$. Let $i \to \alpha_i$ be a one-one indexing of $F - \{0\}$ by $\mathscr{I}$. Let $\alpha_i\beta_i = \sum_{l \in S_i} \beta_l \delta_{l,i}^p$, where S_i is some finite subset of $\mathscr{I}$. Then

$$\left\{ \sum_{l \in S_i} \alpha_i^{-1}\gamma_{l,m}\delta_{l,i} \,\middle|\, m < j \right\}$$

has cardinality $< \aleph$. Let $\gamma_{i,j}$ be any element of F not in this set. Then for all $m < j$,

$$\alpha_i(\beta_i X - \gamma_{i,j}) - \Big(\sum_{l \in S_i} (\beta_l X - \gamma_{l,m}) \Big) \delta_{l,i} = \alpha \neq 0 \in F$$

so $\alpha_i(\beta_i X - \gamma_{i,j}) \notin I_m$.

Set $I_j = \sum (\beta_i X - \gamma_{i,j})\bar{R}$. Then no nonzero $\alpha_i \in F$ sends I_j into I_k for $k < j$ so $R/I_j \not\approx R/I_k$ for $k < j$. Transfinite induction completes the proof.

Corollary. *Let F be a p field over a purely transcendental extension K of $\mathbf{Z}/p\mathbf{Z}$, where K has infinite transcendence degree. Then $\bar{R}$ has precisely two nonisomorphic simple left modules but an infinite number of simple right modules.*

2. Divisibility of Simple Modules

For a commutative ring, every simple is injective if and only if the ring is regular (see Ref. [7]). Cozzens showed this was not true in the noncommutative case since the ring of differential polynomials over a universal differential field and the ring R for F algebraically closed have this property. We will use this second result to study precisely when every simple R module is injective.

We first observe that since R is a principal left ideal domain, divisibility is equivalent to injectivity. Thus a cyclic R module R/Rb is injective if and only if for all $a \neq 0 \in R$, $aR + Rb = R$. The same remark holds for $\bar{R}$, but in that ring it is clear that $X\bar{R} + \bar{R}X \neq \bar{R}$, so $\bar{R}/\bar{R}X$ cannot be injective.

Let $a' = X^{-k}a$, $b' = X^{-l}b$, $a, b \in \bar{R}$. Then $a'R + Rb' = R$ if and only if $X^k a'R + X^k Rb = X^k R$ if and only if $aR + Rb = R$. Moreover, if $a\bar{R} + \bar{R}b = \bar{R}$ for all $a, b \in \bar{R}$ with nonzero constant terms, then for all $X^{-l}c \in R$, let $c = a'r_1 + r_2 b$ where $aX^{-l} = X^{-l}a'X^k$. Then

$$X^{-l}c = X^{-l}a'r_1 + X^{-l}r_2 b = aX^{-l-k}r_1 + X^{-l}r_2 b \in aR + Rb$$

so every proper cyclic R module is divisible if

$$a\bar{R} + \bar{R}b = \bar{R}$$

for every $a, b \in \bar{R} - \bar{R}X$.

For completeness we include the following minor modification of Cozzen's result [1].[1] We will need the second portion of this in what follows.

PROPOSITION 8. *Let F be separably closed. Then every simple R module is injective. Moreover, so is every proper cyclic R module.*

Proof. By Proposition 1, every $r \in \bar{R}$ is a product of linear factors. Hence R/Ra is divisible if and only if it is divisible by every $(X - \gamma)$, $\gamma \neq 0$. Now for $\gamma, \alpha \in F - \{0\}$,

$$(X - \gamma)\bar{R} + \bar{R}(X - \alpha) = \bar{R}$$

if and only if for all $\beta \in F$ there exists ρ and $\tau \in F$ such that

$$(X - \gamma)\rho + \tau(X - \alpha) = \beta$$

if and only if $\tau = \rho^p$ and $-\gamma\rho - \rho^p\alpha = \beta$. Since $\gamma \neq 0$ and F is separably closed, this equation has a root in F.

We give an alternate proof of the injectivity of all simple modules using a criterion attributed to Villamayor that every simple is injective if and only if every proper ideal is an intersection of maximals. Clearly R is Jacobson semisimple so zero is an intersection of maximals. Let $r \neq 0 \in \bar{R} - \bar{R}X$. By Proposition 1, there are precisely $(1 - p^{\text{degree} r})/(1 - p)$ distinct maximal ideals $R(X - \gamma)$ containing Rr, and their intersection is generated by an element giving rise to a P having all the γ's as roots, i.e., r. For ideals RrX^m, one uses the fact that postmultiplication by X^m is an isomorphism to express them as an intersection of ideals $R(X - \gamma)X^m$.

Now for $r \in \bar{R} - \bar{R}X$, R/RrX^m and $\bar{R}/\bar{R}r$ have composition series (obtained by expressing r as a product of irreducible elements of $\bar{R}$). Since a simple $(\neq \bar{R}/\bar{R}X)$ is divisible by all $r \in \bar{R} - \bar{R}X$, $\bar{R}/\bar{R}r$ and R/RrX^m are also so divisible, and so R/RrX^m is injective.

If F does not contain a root of every polynomial $P(Y)$ in Proposition 1, the above analysis is inedequate to show that every simple is injective since we must look at more than linear polynomials.

[1] *Added in Proof.* As a matter of fact, this is not really a modification. Indeed, $R = K[X; \sigma]$ where $K = U_{n=0}^{\infty} X^{-n}FX^n$ is the perfect closure of F, and if F is separably closed, so is K. Replacing F by K would also eliminate the necessity of looking at ideals of the form pX^m in R, since any element $\neq 0$ in $K[X; \sigma]$ is of the form $X^m p'$ where p' has constant term $\neq 0$.

PROPOSITION 9. *Let F be a field such that every polynomial of degree p^i has a root in F (e.g., take a q-field over a field K for some $q \neq p$). Let $b \neq 0 \in \bar{R} - \bar{R}X$. Then R/Rb is injective ($\bar{R}/\bar{R}b$ is injective if F is perfect).*

Proof. Let $a = \sum_{i=0}^{n} \alpha_i X^i$, $b = \sum_0^m \beta_j X^j$, $\alpha_0 \neq 0$. Without loss of generality $m = n$. Then $a\bar{R} + \bar{R}b = \bar{R}$ if and only if for all $c = \sum_{i=0}^{n-1} \gamma_i X^i \in \bar{R}$, there exists $r = \sum_{i=0}^{n-1} \rho_i X^i \in \bar{R}$ such that $c \in ar + Rb$ if and only if there exists $t = \sum_{i=0}^{n-1} \tau_i X^i \in \bar{R}$ such that $c = ar + tb$. The problem then reduces to solving for the ρ_i and τ_i. If

$$\Big(\sum_{i=0}^{n} \alpha_i X^i\Big)\Big(\sum_{i=0}^{n-1} \rho_i X^i\Big) + \Big(\sum_{i=0}^{n-1} \tau_i X^i\Big)\Big(\sum_{i=0}^{n} \beta_i X^i\Big) = \sum_{i=0}^{n-1} \gamma_i X^i$$

and $\gamma_l = 0$ for all $n \leqslant l \leqslant 2n - 1$, by equating coefficients we get

$$\sum_{i+j=k} \alpha_i \sigma^i(\rho_j) + \sum_{i+j=k} \tau_i \sigma^i(\beta_j) = \gamma_k$$

for $0 \leqslant k \leqslant 2n - 1$. These equations may be written as

$$\begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}\begin{pmatrix} \rho \\ \tau \end{pmatrix} = \begin{pmatrix} \gamma \\ 0 \end{pmatrix},$$

where the A_i are matrices over $F[\sigma; \sigma]$ ($\approx \bar{R}$ under $\sigma \leftrightarrow X$) and ρ, τ, and γ are the appropriate column matrices. Now A_1 and A_2 are the lower triangular matrices

$$A_1 = \begin{pmatrix} \alpha_0 & & & & \\ \alpha_1\sigma & \alpha_0 & & 0 & \\ & \alpha_1\sigma & \alpha_0 & & \\ \vdots & \vdots & & & \\ \alpha_{n-1}\sigma^{n-1} & \alpha_{n-2}\sigma^{n-2} & \cdots & \alpha_1\sigma & \alpha_0 \end{pmatrix},$$

$$A_2 = \begin{pmatrix} \beta_0 & & & & \\ \beta_1{}^p & \beta_0 & & 0 & \\ & \beta_1{}^p & \beta_0 & & \\ \vdots & \vdots & & & \\ \beta_{n-1}^{p^{n-1}} & \beta_{n-1}^{p^{n-1}} & \cdots & \beta_1{}^p & \beta_0 \end{pmatrix},$$

and since $\beta_0 \neq 0$, A_2 has an inverse over F. Then

$$\tau = -A_2^{-1}A_1\rho + A_2^{-1}\gamma,$$

i.e., we can solve for the τ_i in terms of polynomials in the ρ_i all of whose exponents are powers of p. Then

$$A_3\rho + A_4(-A_2^{-1}A_1\rho + A_2^{-1}\gamma) = 0$$

so $(A_3 - A_4A_2^{-1}A_1)\rho = -A_4A_2^{-1}\gamma$. Set $B = A_3 - A_4A_2^{-1}A_1 \in (F[\sigma; \sigma])_{n,n}$, $A = -A_4A_2^{-1}$.

We now apply some linear algebra and the Euclidean algorithm in R. The standard commutative argument goes through except that we have no right algorithm. Let

$$\mathfrak{A} = \{UBV \mid U \text{ and } V \text{ invertible in } (F[\sigma; \sigma])_{n,n}\}.$$

We observe that permutation matrices and elementary matrices of the form $I_n + rE_{ij}$, $i \neq j$ are invertible and premultiplication by one of them performs the row operation used to obtain them from I_n, whereas postmultiplication performs the column operation.

LEMMA. *There exists $B' \in \mathfrak{A}$ such that B' is upper triangular, i.e., $(B')_{i,j} = 0$ for $i < j$.*

Proof. If $B = 0$ or $n = 1$ there is nothing to prove. Now assume $B \neq 0$ and $n > 1$. Let $C \in \mathfrak{A}$ possess a nonzero entry r of smallest degree in σ. Pre- and post-multiplication by appropriate permutation matrices will bring r to the 1, 1 position. Subtracting multiples of row one from succeeding rows will make every entry in column one either 0 or of degree less than that of r by the Euclidean algorithm in $F[\sigma; \sigma]$. By minimality of degree r, there is a $C' \in \mathfrak{A}$ of the form

$$C' = \begin{pmatrix} r & \text{---} \\ 0 & C'' \end{pmatrix}.$$

By induction on n, there exist U' and V' invertible in $(F[\sigma; \sigma])_{n-1,n-1}$ such that $U'C''V'$ is triangular. Then for

$$U'' = \begin{pmatrix} 1 & 0 \\ 0 & U' \end{pmatrix}, \qquad V'' = \begin{pmatrix} 1 & 0 \\ 0 & V' \end{pmatrix},$$

we have

$$B' = U''C'V'' = UBV$$

is triangular, where U and V are invertible.

Returning to the proof of Proposition 9, we note that $B\rho = A\gamma$ if and only if $B'(V^{-1}\rho) = UA\gamma$, where B' is the triangular matrix of the Lemma.

Set $r_i = (B')_{i,i}$. One can then find a set of ρ_i that will show divisibility provided one can successively solve the equations $r_n\rho_n = (UA)_n$, $r_k\rho_k + f_k(\rho_{k+1}, ..., \rho_n) = (UA)_k$ for the appropriate polynomials f_k. If these equations are compatable (any zero r_i corresponds to a zero $(UA)_i$), then one has a series of polynomials of degree a power of p, and every such polynomial has a root in F. But over the separable closure of F these equations have a solution by Proposition 8 since every cyclic over the corresponding localized twisted polynomial ring is divisible. Hence one can find ρ and τ in F such that $ar + tb = c$. Divisibility of $\bar{R}/\bar{R}b$ by X follows from the perfectness of F.

EXAMPLES. (a) Let $K = \mathbf{Z}_p(x)$, x an indeterminant, p odd, $q = 2$. Let F be a two-field over K and $\{\pi_i \mid i \in \omega\}$ the (infinite) set of primes of $\mathbf{Z}_p[x]$. Then $R/R(X - \pi_i) \approx R/R(X - \pi_k)$ for $i \neq k$ if and only if for some $j \geqslant 0$ there is an $\alpha \in F$ such that

$$\alpha^{p-1} - \pi_i^{p^j}/\pi_k = 0.$$

But the polynomial $\pi_k Y^{p-1} - \pi_i^{p^j}$ is irreducible over K since

$$\pi_i^{p^j}\left(\frac{1}{Y}\right)^{p-1} - \pi_k \in F\left[\frac{1}{Y}\right]$$

is by Eisenstein's criterion, and so cannot have a root in F. Then R satisfies P_1 and P_3.

(b) Let $K = \mathbf{Z}_2$, F a two-field over K. By a minor modification of the proof of Proposition 8, $(x - 1)R + R(x - 1) = R$ if and only if for all $\beta \in F$ the polynomial $Y^2 + Y + \beta$ has a root in F. But that polynomial is irreducible over $\mathbf{Z}_2$ for $\beta = 1$, and hence has no root in F. Thus R satisfies P_2 but not P_1.

Although Proposition 8 shows that the condition P_1 on R says nothing about perfectness of F, the situation in the case of $\bar{R}$ is significantly different. For a separably closed F, every simple $\bar{R}$ module is divisible by any polynomial with constant term $\neq 0$ by Proposition 8 and the observation that $\bar{R}/\bar{R}X$ is so divisible. However, we have

PROPOSITION 10. *Let $a = \sum_{i=0}^{n} \alpha_i X^i \in \bar{R}$, a not a unit in $\bar{R}$. Then if $\bar{R}/\bar{R}a$ is divisible by X, F must be perfect.*

Proof. Since $\bar{R}$ is not divisible by X, $a \neq 0$. Without loss of generality, $\alpha_n = 1$, $n > 0$. Then for all $\sum_{i=0}^{n-1} \gamma_i X^i$, there exists $\sum_{i=0}^{n-1} \rho_i X^i$ and τ such that

$$X\left(\sum_{i=0}^{n-1} \rho_i X^i\right) + \tau\left(\sum_{i=0}^{n} \alpha_i X^i\right) = \sum_{i=0}^{n-1} \gamma_i X^i.$$

But then $\rho_{n-1}^p + \tau = 0$, so $\tau \in F^p$, and all $\gamma_0 \in F$ are in $\alpha_0 F^p$, i.e., $F = F^p$.

We have observed that, conversely, if $\alpha_0 \neq 0$ and F is perfect, then $\bar{R}/\bar{R}a$ is always divisible by X since $X\bar{R} = \bar{R}X$. By Propositions 1 and 8, if F is algebraically closed, then every simple $\bar{R}$ module except $\bar{R}/\bar{R}X$ is injective.

Remarks. Although P_1 and P_2 hold for F separably closed and P_1 and P_3

hold for F a two-field over a rational function field and $p > 2$, it is difficult to envision a field for which R has P_1 but neither P_2 nor P_3. One not only has to worry about polynomials of the same degree yielding a finite set of simples, but one must also consider polynomials of different degrees. Thus for $p = 2$, simples of the form $R/R(X - \alpha)$ are all isomorphic, but there may well be other distinct unfactorable polynomials of different degrees yielding other simples. If one could have at least one root for each polynomial P of Proposition 1 without simultaneously having roots for all Q of Proposition 2, then one might be able to have only a finite number ($\neq 1$) of nonisomorphic simples, but this seems difficult also.

In the case of differential polynomials, Cozzens in his thesis characterizes the situation when all simples are injective and isomorphic. It seems much more difficult to get a nice description for twisted polynomials. The problem is that not every separable polynomial is a P or Q or of the form $f(\sigma)(Y) + \alpha$, $f \in F[\sigma; \sigma]$, $\sigma(Y) = Y^p$.

In the simple ring case (R rather than $\bar{R}$) one can ask whether R may have both injective and noninjective simples. This seems highly unlikely. For example, if $R/R(X - \alpha)$ is divisible, one obtains roots for all equations of the form $f(\sigma)(Y) + \beta = 0$, so all simples are injective.

It is also of interest to ask if, for a noninjective simple R module M, the injective hull of M can have finite length. This also seems to be a difficult problem.

References

1. J. Cozzens, Homological properties of the ring of differential polynomials, *Bull. Amer. Math. Soc.* **76** (1970), 75–79.
2. C. Faith, "Lectures on Injective Modules and Quotient Rings," Springer-Verlag, Berlin, 1967.
3. N. Jacobson, "The Theory of Rings," Amer. Math. Soc. Math. Surveys, Vol. 2, Amer. Math. Soc., Providence, R. I., 1943.
4. I. Kaplansky, "Fields and Rings," University of Chicago Press, Chicago, Ill., 1969.
5. S. Lang, "Algebra," Addison-Wesley, Reading, Mass., 1965.
6. S. Perlis, "Theory of Matrices," Addison-Wesley, Reading, Mass., 1952.
7. A. Rosenberg and D. Zelinsky, On the finiteness of the injective hull, *Math. Z.* **70** (1959), 372–380.