On skew polynomial rings

Lkhangaa Oyuntsetseg
Institute of Mathematics
National University of Mongolia,
Ulaanbaatar, Mongolia
e-mail: oyuntsetseg@smcs.num.edu.mn
oyulkh@yahoo.com

Abstract

In this paper we consider left cyclic modules over a skew polynomial ring R, which are not injective as a left R-module and give on example of skew polynomial rings which homomorphic image is isomorphic to a matrix ring. We hope that this correspondence is useful.

1 Introduction

Let k be a field and σ be an automorphism of k. We define $R = k[x;\sigma] = \{f(x)|f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0,\, a_i \in k, n \in \mathbb{N}\}$, a skew polynomial ring with a usual polynomial addition, and multiplication is defined by the following rule

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

First we consider that R is a principal left ideal domain. We show that R has a left division algorithm. Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

and

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$$

be polynomials of R. We assume that $n \geq m$. Since σ is an automorphism of k we choose the element $c_0 = \sigma^{-m}(a_n b_m^{-1})$ in k then

$$g(x)c_0 x^{n-m} = (b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0)\sigma^{-m}(a_n b_m^{-1})x^{n-m} = a_n x^n + \ldots$$

and if we take $f_1(x) = f(x) - g(x)c_0 x^{n-m}$ then $\deg f_1(x) < \deg f(x)$. If we continue this procedure until $\deg f_k(x) < \deg g(x)$ then we can get $r(x) = f_k(x)$ with $\deg r(x) < \deg g(x)$ and $f(x) = g(x)q(x) + r(x)$. Therefore we conclude that R is a ring with a left division algorithm. So R is a left principal ideal domain (i.e. every left ideal is generated by its non zero polynomial of a minimum degree). We use that a left module M over a left principal ideal domain R is injective if and only if

2 Cyclic modules

We define k as a left R-module with the following multiplication.

$$f(x)\alpha = a_n\sigma^n(\alpha) + a_{n-1}\sigma^{n-1}(\alpha) + \cdots + a_0\alpha,$$

where $\alpha \in k$ and $f(x) = a_nx^n + \cdots + a_0 \in R$. Since k is a field, k can be generated by any nonzero element of k i.e. $R\alpha = k$, $\alpha \in k$, so we call k as a cyclic module over R. First we show that k is isomorphic to $R/R(x-1)$ as a left R-module.

$$\forall f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R$$

$$f_1(x) = f(x) - a_nx^{n-1}(x-1) = (a_n + a_{n-1})x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0$$

If we continue this process, after nth step, we have

$$f_n(x) = a_n + a_{n-1} + \cdots + a_0.$$

This means that

$$f(x) \equiv a_n + a_{n-1} + \cdots + a_0 (modR(x-1)).$$

If we define a module homomorphism φ as

$$\varphi :\ R/R(x-1) \longrightarrow k,$$

$$\overline{f(x)} \mapsto a_n + a_{n-1} + \cdots + a_0,$$

then φ is an R- module isomorphism and we show it.
First we see the case when $g(x) = bx^m$.

$$g(x)f(x) = bx^m(a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0) =$$

$$= b\sigma^m(a_n)x^{n+m} + b\sigma^m(a_{n-1})x^{n+m-1} + \cdots + b\sigma^m(a_0)x^m$$

$$bx^mf(x) \equiv b\sigma^m(a_n) + b\sigma^m(a_{n-1}) + \cdots + b\sigma^m(a_0)(modR(x-1))$$

On the other hand if we see a module multiplication in k, then we have

$$bx^m\varphi(\overline{f(x)}) = bx^m(a_n + a_{n-1} + \cdots + a_0) = b\sigma^m(a_n) + b\sigma^m(a_{n-1}) + \cdots + b\sigma^m(a_0)$$

Thus conclude that

$$\varphi(\overline{bx^mf(x)}) = \varphi(bx^m\overline{f(x)}) = bx^m\varphi(\overline{f(x)}).$$

In general case, if we take $g(x) = b_mx^m + \cdots + b_0$, then by the additive property of φ and above the case, we have

$$\varphi(\overline{g(x)f(x)}) = \varphi(g(x)\overline{f(x)}) = g(x)\varphi(\overline{f(x)}).$$

And we prove that k is isomorphic to $R/R(x-1)$ as a left R-module.

Now we are interested in the case k is a simple algebraic extension field of F where $F = inv(\sigma) = \{\alpha \in k | \sigma(\alpha) = \alpha\}$. In this case $k = F(\alpha)$ for some algebraic element α of k over F. Since σ is an element of $Gal(k/F)$, σ has a finite order i.e. $\sigma^n = id$ for some natural number n. If we take

$$f(x) = x^n - 1,$$

then for any β in k we have

$$f(x)\beta = (x^n - 1)\beta = \sigma^n(\beta) - \beta = \beta - \beta = 0.$$

This means a left R-module k is not divisible. And we can conclude that k is not a left injective R-module.

By theorem in [1] we have some examples of left R-modules which are not injective.

Theorem 1. *Let k be a field and σ be an automorphism of k with $F = inv(\sigma) = \{\alpha \in k | \sigma(\alpha) = \alpha\}$. Let k be a finite algebraic extension of F. Then the following modules are not injective.*

(1) A left R-module k;

(2) A left R-module $R/R(x-\alpha)$, where $\alpha \in k$ with $\alpha = \frac{\beta}{\sigma(\beta)}$ for some $\beta \in k$.

Proof. (1) (1) is proved above.

(2) We show that for any α of k with $\alpha = \frac{\beta}{\sigma(\beta)}$ for some $\beta \in k$, $R/R(x-\alpha)$ is isomorphic to $R/R(x-1)$ as a left R-module. Let φ be an R-module isomorphism such that

$$\varphi : R/R(x-1) \to R/R(x-\alpha)$$

and we set $\varphi(1 (\mod R(x-1)) \equiv \beta(\mod R(x-\alpha))$ for some non-zero β then by R-module homomorphism

$$\varphi(f(x)\,(modR(x-1)) \equiv f(x)\varphi(1\,(modR(x-1)) \equiv f(x)\beta(modR(x-\alpha))$$

Since $x - 1 \equiv 0(modR(x-1))$ and by well defined condition of φ we have

$$\varphi(x-1) \equiv (x-1)\varphi(1\,(modR(x-1)) \equiv (x-1)\beta(modR(x-\alpha)).$$

Then

$$(x-1)\beta \equiv 0(modR(x-\alpha)) \Leftrightarrow$$

$$\sigma(\beta)x - \beta = \gamma(x-\alpha) \Rightarrow \alpha = \frac{\beta}{\sigma(\beta)}$$

□

We conclude the following corollary from the above theorem.

Corollary 1. *Let k be a finite field of characteristic 2 and σ be the Frobenius auto morphism of k over $GF(2)$. Then all left R-modules $R/R(x-\alpha)$ are isomorphic for any non-zero α in k.*

Proof. Since $\sigma(\alpha) = \alpha^2$ and $\frac{\alpha}{\sigma(\alpha)} = \frac{\alpha}{\alpha^2} = \alpha^{-1}$ then for any non-zero α in k

$$\alpha = \frac{\alpha^{-1}}{\sigma(\alpha^{-1})}.$$

Therefore by(2) of Theorem 1, a left R-module $R/R(x-\alpha)$ is isomorphic to $R/R(x-1)$ for any non-zero α in k.

□

3 A skew polynomial ring over a finite field

Now we see some particular cases of a skew polynomial ring. Let k be a finite field i.e. $k = GF(p^n)$ and σ be a Frobenius map of k over $GF(p)$. i.e.

$$\sigma : k \longrightarrow k$$

$$\forall \alpha \in k,\ \alpha \mapsto \alpha^p$$

It is well known that $\sigma^n = id$ and n is the minimum number with such property. And it implies that the annihilator of a left R-module k is $R(x^n - 1)$ which is an ideal in R. We take a ring $S = R/R(x^n - 1)$ and $y = \overline{x}$ then $y^n = 1$ and every element s in S has a unique canonic form $s = \alpha_0 + \alpha_1 y + \cdots + \alpha_{n-1} y^{n-1}$. So the number of elements of S is p^{n^2}.

Therefore k is a left faithful irreducible S-module then S is a primitive ring. It is well known that S is a direct sum of simple artinian rings i.e. matrix rings over a field. The following proposition tells us that S has no nonzero proper ideal.

Proposition 1. *S is a simple ring.*

Proof. We assume that I is a nonzero ideal of S. Let s be a nonzero element of I and $s = y^r + \beta_{r-1} y^{r-1} + \cdots + \beta_0$ with minimum degree r. And we assume that $n > r > 0$. Let β_{r-i} be the first nonzero coefficient from left i.e. $\beta_{r-1} = \cdots = \beta_{r-i+1} = 0$ but $\beta_{r-i} \neq 0$. Since $\sigma \in Gal(GF(p^n)/GF(p))$ and has the order of n, there is an element $\alpha \in k$ such that $\sigma^r(\alpha) \neq \sigma^{r-i}(\alpha)$. If we take $s' = \sigma^r(\alpha)s - s\alpha$, then

$$s' = (\sigma^r(\alpha)y^r + \sigma^r(\alpha)\beta_{r-i}y^{r-i} + \dots) - (\sigma^r(\alpha)y^r + \sigma^{r-i}(\alpha)\beta_{r-i}y^{r-i} + \dots) =$$

$$(\sigma^r(\alpha) - \sigma^{r-i}(\alpha))\beta_{r-i}y^{r-i} + \cdots \neq 0 \in I.$$

s' is a nonzero element in I with degree less than of s. It contradicts to our choice. This means I contains an element of degree zero i.e. $I = S$. Thus we prove S has no nonzero proper ideal. $\square$

At last we conclude the above consideration in the following theorem.

Theorem 2. *Let $k = GF(p^n)$ be a finite field and σ be the Frobenius map of k.*

$$\sigma : k \longrightarrow k$$

$$\alpha \longmapsto \alpha^p.$$

Let $R = k[x;\sigma]$ be a skew polynomial ring and $S = R/(x^n - 1)R$ be a factor ring. Then S is a simple artinian ring i.e. S is isomorphic to $M_n(GF(p))$.

From this theorem, we can conclude the following property of a full matrix ring.

Proposition 2. *The full matrix ring over $GF(p)$ can be generated by two elements.*

We consider the following example.
$GF(4) = \{0, 1, \alpha, \alpha + 1 | \alpha^2 + \alpha + 1 = 0\}$. $\sigma \in Gal(GF(4)/GF(2))$ and $\sigma(\alpha) = \alpha^2 = \alpha + 1$. $R = GF(4)[x;\sigma]$ is a skew polynomial ring with a multiplication that $x \cdot 1 = x$, $\quad x \cdot \alpha = (\alpha + 1)x$ and $x \cdot (\alpha + 1) = \alpha x$. Let $S = R/R(x^2 - 1)$ be a factor ring and $y = \overline{x}$. Then $y^2 = 1$ and $S = \{\beta_0 + \beta_1 y | \beta_0, \beta_1 \in GF(4), y^2 = 1\}$. The number of elements of S is 16. By the above theorem it implies that S is isomorphic to $M_2(GF(2))$. Let f be an isomorphism from S to $M_2(GF(2))$. Since S is generated by $\{\alpha, y\}$, it is enough to define homomorphic image of α and y.

$$f : S \longrightarrow M_2(GF(2))$$

$$\alpha \longmapsto \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad y \longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

In this case we see k as a left S-module with multiplication $y\alpha = \sigma(\alpha) = \alpha + 1$.

Acknowledgements. I would like to thank Prof. A.Mekei for his great advice on this paper.

References

[1] B. L. Osofsky , Injective module over twisted polynomial rings. Nagoya Math. J. Vol. 119 (1990) 107-114

[2] Nathan Jacobson, Lectures in Abstract Algebra, II, III.

[3] I.N.Herstein, Noncommutative rings