Skew Polynomial Rings

John A. Beachy

NIU

November 14, 2018

Bibliography

Beachy, *Introductory Lectures on Rings and Modules*, Cambridge Univ. Press, 1999

Goodearl and Warfield, *An Introduction to Noncommutative Noetherian Rings*, 2nd ed., Cambridge Univ. Press, 2004

Goodearl and Letzter, *Prime Ideals in Skew and Q-Skew Polynomial Rings*, AMS Memoirs, 1994

Kassel, *Quantum Groups*, Springer, 1995

Brown and Goodearl, *Lectures on Algebraic Quantum Groups*, Birkhäuser, 2002

Skew polynomials form a ring

Existence and uniqueness results are given in Theorem I.7.1 in Kassel. Let R be a k-algebra, and let τ be an endomorphism of R. Recall that $\delta : R \to R$ is called τ-derivation if δ is linear and $\delta(ab) = \tau(a)\delta(b) + \delta(a)b$, for all $a, b \in R$.
Uniqueness:

Theorem

Assume that $R[x]$ has an algebra structure such that the inclusion $R \to R[t]$ is an algebra homomorphism, and we have $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$ for any $p(x), q(x) \in R[x]$. Then R as no zero-divisors and there exists a unique one-to-one endomorphism τ of R and a unique τ-derivation δ of R such that

$$xa = \tau(a)x + \delta(a)$$

for all $a \in R$.

Existence

We've already seen the crux of the uniqueness proof: if $a \in R$, then $xa \in Rx + R$ because of the condition on degrees. This gives us τ and δ.

Existence:

Theorem

Let R be an algebra without zero-divisors. Given a one-to-one algebra endomorphism τ of R and a τ-derivation δ of R, there exists a unique algebra structure on $R[x]$ such that the inclusion of R into $R[x]$ is an algebra homomorphism and

$$xa = \tau(a)x + \delta(a)$$

holds for all $a \in R$.

Checking the ring axioms

What follows is a hint of an outline of the proof given by Kassel. To make it easier to check the axioms, we embed R in the endomorphism ring of $R[x]$, viewed as an abelian group. First identify the polynomial $a_0 + a_1 x + a_2 x^2 + \dots$ with the column vector $\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \end{bmatrix}$. To act on these column vectors, the endomorphisms can be identified with the set of countably infinite column-finite matrices, since the image of any basis element e_n (corresponding to x^n) is a polynomial, whose representation has only finitely many nonzero entries.

Multiplication in the endomorphism ring

Multiplication by an element $r \in R$ is given in matrix form by

$$\begin{bmatrix} r & 0 & 0 & \dots \\ 0 & r & 0 & \dots \\ 0 & 0 & r & \dots \\ \vdots & \vdots & \vdots & \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \end{bmatrix} = \begin{bmatrix} ra_0 \\ ra_1 \\ ra_2 \\ \vdots \end{bmatrix}.$$

Call this matrix λ_r.

In the usual matrix ring, multiplying by x on the left is given by

$$\begin{bmatrix} 0 & 0 & 0 & \dots \\ 1 & 0 & 0 & \dots \\ 0 & 1 & 0 & \dots \\ \vdots & \vdots & \vdots & \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \end{bmatrix} = \begin{bmatrix} 0 \\ a_0 \\ a_1 \\ \vdots \end{bmatrix}.$$

In the skew polynomial ring, multiplication by x on the left is given by $x(a_0 + a_1 x + a_2 x^2 + \dots) =$
$\tau(a_0)x + \delta(a_0) + \tau(a_1)x^2 + \delta(a_1)x + \tau(a_2)x^3 + \delta(a_2)x^2 + \dots =$
$\delta(a_0) + (\delta(a_1) + \tau(a_0))x + (\delta(a_2) + \tau(a_1))x^2 + \dots$.

Multiplication by x in the matrix ring

In the matrix ring, the product
$\delta(a_0) + (\delta(a_1) + \tau(a_0))x + (\delta(a_2) + \tau(a_1))x^2 + \dots$ has the form

$$\begin{bmatrix} \delta(a_0) \\ \delta(a_1) + \tau(a_0) \\ \delta(a_2) + \tau(a_1) \\ \vdots \end{bmatrix} = \begin{bmatrix} \delta & 0 & 0 & \dots \\ \tau & \delta & 0 & \dots \\ 0 & \tau & \delta & \dots \\ \vdots & \vdots & \vdots & \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \end{bmatrix}.$$

We identify left multiplication by x with the matrix X that has δ on the main diagonal and τ just below the diagonal. Define a additive mapping $\Phi : R[x] \to M_\infty(R)$ by $\Phi(\sum a_i x^i) = \sum \lambda_{a_i} X^i$. This works since τ and δ are additive. Then Φ can be shown to be one-to-one, and the image of Φ is the subring generated by the matrix X and the matrices of the form λ_r, for $r \in R$. This allows the ring structure of the subring to be transferred back to $R[x]$.
Conclusion: $R[x; \tau, \delta]$ is a ring.

Some miscellaneous results

The next result shows that if τ is an automorphism, then there is some symmetry. We let R^{op} denote the opposite ring of R (defined by reversing the multiplication).

Theorem (Goodearl)

Let $S = R[x; \tau, \delta]$ be a skew polynomial ring in which τ is an automorphism. Then τ^{-1} is an automorphism of R^{op}, and $-\delta\tau^{-1}$ is a τ^{-1}-derivation of R^{op}. There is a ring isomorphism

$$\phi : R[x; \tau, \delta]^{op} \to R^{op}[x; \tau^{-1}, -\delta\tau^{-1}]$$

such that $\phi(x) = x$ and $\phi(a) = a$ for all $a \in R$.

Some miscellaneous results

Theorem (Goodearl)

Let (τ, δ) be a skew derivation on a ring R, and let u, v be elements in a polynomial ring $R[x]$. Then (τ, δ) extends to a skew derivation on $R[x]$ such that $\tau(x) = u$ and $\delta(x) = v$ if and only if $u\tau(r) = \tau(r)u$ and $vr - \tau(r)v = (y - u)\delta(r)$ for all $r \in R$.

The "skew" Hilbert basis theorem:
If R is a commutative Noetherian ring, then so is the polynomial ring $R[y]$. This is usually known as the Hilbert basis theorem. We would like to extend the result to include the more general case of a skew polynomial ring $R[x; \tau, \delta]$ over R, in which the defining endomorphism τ is an automorphism. In this case the ring is generated by R and x, and $xR + R = Rx + R$. This motivates the general statement of the next theorem.

The skew Hilbert basis theorem

Theorem

Let R be a subring of the ring S, and suppose that S is generated as a ring by R and an element $y \in S$ for which $yR + R = Ry + R$. If R is left Noetherian, then so is S.

Proof: By assumption, each element $s \in S$ has the form $s = \sum_{i=0}^{n} a_i y^i$, for some integer $n \geq 0$ and some elements $a_0, \ldots, a_n \in R$. Since $yR \subseteq Ry + R$, we can prove by induction that $y^n R \subseteq \sum_{i=0}^{n} Ry^i$. Thus we can also assume that each element $s \in S$ has the form $s = \sum_{i=0}^{n} y^i a_i$, for some integer $n \geq 0$ and some elements $a_0, \ldots, a_n \in R$. We say that this expression for s has degree n, and that its leading coefficient is a_n.

Proof–continued

We will show that if S is not left Noetherian, then R is not left Noetherian. In particular, we suppose that there exists a left ideal I of S that is not finitely generated, and we use this left ideal to construct an infinite ascending chain of left ideals of R. Among nonzero elements of I, choose an element s_1 with an expression $s_1 = \sum_{i=0}^{n} y^i a_{1i}$ of minimal degree. Then $I \neq Ss_1$ since I is not finitely generated, so we can choose an element s_2 with an expression $s_2 = \sum_{i=0}^{m} y^i a_{2i}$ whose degree is minimal among the elements in I but not in Ss_1. If such elements have already been chosen for $1 \leq i \leq k-1$, let s_k be an element whose degree is minimal among the elements in I but not in $(\sum_{i=1}^{k-1} Ss_i)$.

Proof–continued

Let $n(i)$ denote the degree of s_i. By our choice of the elements $\{s_i\}$, we see that if $i < j$, then $n(i) \leq n(j)$. Let a_i be the leading coefficient of s_i. We claim that the left ideals $Ra_1 \subseteq Ra_2 + Ra_2 \subseteq \ldots$ form a strictly ascending chain of left ideals of R. If $\sum_{i=1}^{k-1} Ra_i = \sum_{i=1}^{k} Ra_i$, then $a_k = \sum_{i=1}^{k-1} r_i a_i$, for some $r_1, \ldots, r_{k-1} \in R$. Since $y^{n(i)} R \subseteq \sum_{j=0}^{n(i)} Ry^j$, we can write $y^{n(i)} r_i = r_i' y^{n(i)} + t_i$, where t_i has an expression with degree less than $n(i)$.

Proof–continued

Now consider the element $s = s_k - \sum_{i=1}^{k-1} y^{n(k)-n(i)} r_i' s_i$. To compute the leading coefficient of the term $y^{n(k)-n(i)} r_i' s_i$, we have

$$\begin{aligned} y^{n(k)-n(i)} r_i' s_i &= y^{n(k)-n(i)} r_i' y^{n(i)} a_i \\ &= y^{n(k)-n(i)} (y^{n(i)} r_i - t_i) a_i \\ &= y^{n(k)} r_i a_i + t_i' \ , \end{aligned}$$

where the degree of t_i' is less than $n(k)$. It follows that the degree s is less than $n(k)$, since the coefficient of $y^{n(k)}$ is $a_k - \sum_{i=1}^{k-1} r_i a_i = 0$. This contradicts the choice of s_k, since $s \in I$ but $s \notin (\sum_{i=1}^{k-1} S s_i)$, but s has lower degree than s_k. □

The theorem and an example

As a corollary of the previous theorem, we have the following.

Theorem (Hilbert basis theorem)

Let R be a left Noetherian ring. If τ is an automorphism of R, then the skew polynomial ring $R[x;\tau,\delta]$ is left Noetherian.

If R is also right Noetherian, then so is $R[x;\tau,\delta]$.

Example

Let $R = k(t)$ be a rational function field over a field k, and let τ be the k-algebra endomorphism of R defined by $\tau(f(t)) = f(t^2)$. (Chosen so that τ is not an automorphism of the field.) Then $R[x;\tau]$ is a principal left ideal domain, but not a principal right ideal domain. Moreover, $R[x;\tau]$ is not right Noetherian.

Recall the following definition.

Definition

Let F be a field, and let $R = F[x_1, x_2, \ldots, x_n]$. The iterated differential operator ring

$$R[y_1, \ldots, y_n; \frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n}]$$

is called the n*th Weyl algebra over* F, and is denoted by $A_n(F)$.

A ring is said to be *simple* if it has no nonzero proper ideals.

Theorem

The Weyl algebra $A_n(k)$ is a simple Noetherian ring if k is a field.

Prime ideals

Recall that an ideal P of a ring is said to be *prime* if $AB \subseteq P$ implies $A \subseteq P$ or $B \subseteq P$, for all ideals A, B of R. An ideal is called *primitive* if it is the annihilator of a simple module. Prime and primitive ideals are important; one of the next steps in studying skew polynomial rings is to study them.

That's all for now!