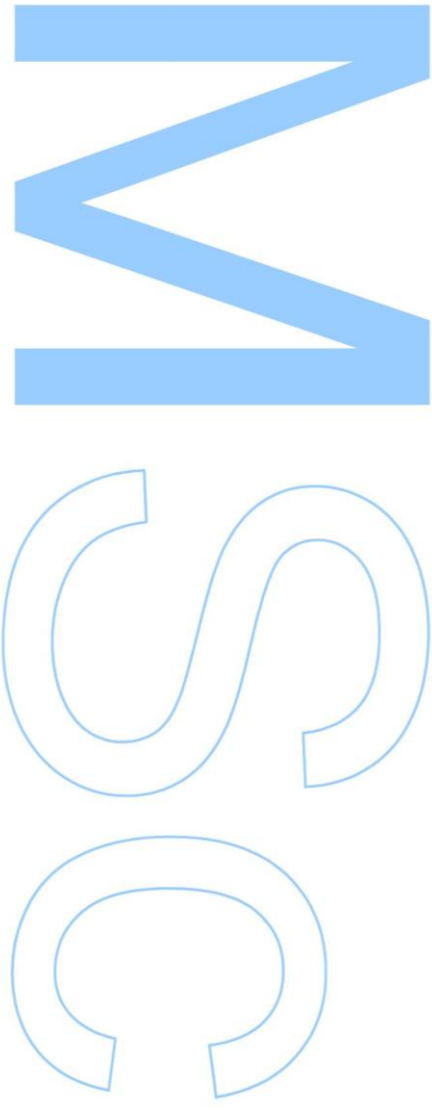
Primitivity of Skew Polynomial Rings

Gjermund Johansen
Matemática
Departamento de Matemática
2018

Orientador
Christian Edgar Lomp, Professor Auxilliar, Faculdade de Ciências



Acknowledgement

First of all I would like to thank God. Without Him there would be no life, and certainly no theses!

I would like to thank my supervisor professor Christian Edgar Lomp of the Department of Mathematics at the University of Porto, Portugal. Prof. Lomp was always available whenever I had a question about my research or writing. He allowed this paper to be my own work while giving me a lot of guidance whenever I needed it. Thanks also to his wife Paula for highly appreciated input. In addition, I would like to thank professor Samuel Lopes from the University of Porto, Portugal and professor André Leroy from the University of Artois, France, for giving feedback and corrections.

I would also thank my children Marielle and William for patiently spending long days missing their father. Hundreds of days during my two years of study they saw me leaving in the morning, knowing that they would only see me again the next morning, as I often came home after their bedtime.

Finally, I would also express my very profound gratitude to my wife Ana-Adriana for graciously providing for our children while I studied. Day in and day out she not only fed and clothed our children, she also gave them the most excellent upraising and added joy and meaning to their lives. Thank you for your unfailing support and continuous encouragement through the process of researching and writing this thesis. This accomplishment would not have been possible without you. Thank you.

October 2018
Gjermund Johansen

Resumo em Português

O objetivo desta tese é construir anéis que são primitivos em apenas num lado, usando os artigos [5] e [6] de Ronald S. Irving como fonte principal. Para o skew anel de plolinómios sobre o anel de polinómios numa variável sobre um corpo algebricamente fechado de característica 0, damos uma descrição completa das condições para a primitividade direita e esquerda. Em particular, descrevemos todos os anéis deste tipo que são primitivos em apenas um lado e exibinos alguns exemplos em concreto. Além disso, mostramos que um certo subanel de um skew anel de polinómios sobre o corpo das funções racionais é primitivo à direita, mas não primitivo à esquerda. Este exemplo foi construído por George M. Bergman em [1].

Abstract in English

The aim of this thesis is to construct rings that are primitive on only one side, following the articles [5] and [6] by Ronald S. Irving as our main source. For the skew polynomial ring over the polynomial ring in one variable over an algebraically closed field of characteristic 0, we give a complete description of the conditions for both right and left primitivity. In particular, we describe all the rings of this type that are primitive on only one side and provide some concrete examples. Furthermore, we show that a certain subring of the skew polynomial ring over the field of rational functions is right primitive but not left primitive. This example was constructed by George M. Bergman in [1].

Keywords

Algebra; ring theory; primitive rings; faithful simple modules; skew polynomial rings.

Contents

Chapter 1

Preliminaries

The following definitions in this chapter, as well as some of the results, are taken from [2], [3], [7], [8], [9], [11], [12], [13], [14] and [15]. Throughout this thesis, we will denote the zero-set $\{0\}$ by 0, and every ring will be unital and associative. We will reserve R and S for commutative rings and A and B for non-commutative rings. Furthermore, K will always denote an algebraically closed field of characteristic 0. For every ring homomorphism $\varphi : A \to B$, we will assume that $\varphi(1_A) = 1_B$. When we omit the word left (resp. right) in front of the word ideal, we mean a two-sided ideal. The **opposite ring** $A^{\mathbf{op}}$ of a ring A is the ring defined on the same abelian group structure $(A, +)$ but with multiplication defined as $a \cdot b := ba$ for all $a, b \in A$.

1.1 Modules and maximal ideals

A **(unital) left A-module** is an abelian group M written additively together with a map

$$A \times M \to M$$
$$(a, m) \mapsto am$$

such that for all $a, b \in A$ and all $m, n \in M$,

(i) $(a + b)m = am + bm$,

(ii) $a(m + n) = am + an$,

(iii) $a(bm) = (ab)m$.

(iv) $1m = m$

A **right A-module** is defined analogously. A subset L of M is called a **submodule** of M if L is a subgroup of M and $al \in L$ for all $a \in A$ and $l \in L$. The following proposition is taken from [14, p. 102].

Proposition 1.1. Let I be a left ideal of a ring A. Then the map

$$A \times A/I \to A/I$$
$$(a, m + I) \mapsto am + I$$

makes the residue class group A/I into a left A-module.

Let M be an Abelian group and A any ring and denote the ring of group endomorphisms of M by $\mathrm{End}(M)$. Then

(i) if $\lambda : A \times M \to M$ defines a left A-module structure on M, then $\varphi : A \to \mathrm{End}(M)$ given by $\lambda(a)(m) = am$ is a ring homomorphism;

(ii) if $\varphi : A \to \mathrm{End}(M)$ is a ring homomorphism, then $\lambda : A \times M \to M$ given by $\lambda(a, m) = \varphi(a)(m)$ defines a left A-module structure on M.

A ring homomorphism $\varphi : A \to \mathrm{End}(M)$ is called a representation of A on M. The kernel of this representation of A is called the **annihilator of** M and as a kernel of a ring homomorphism, the annihilator is a two-sided ideal. More formally, the annihilator of an A-module M is the set

$$\mathrm{ann}_A(M) := \{a \in A : aM = 0\}.$$

If $\mathrm{ann}_A(M) = 0$, then M is said to be a **faithful** module.

Analogously there exists a correspondence between right A-module structures on M and ring homomorphism $\varphi : A \to \mathrm{End}(M)^{\mathrm{op}}$. A **$K$-algebra** is a ring A with a ring homomorphism $i : K \to Z(A)$, where $Z(A)$ is the center of A (see [4, p. xi]). The element $i(1) = 1_A$ is the identity of A and A becomes a K-vector space by $ka := i(k)a$ for all $k \in K$ and $a \in A$. A left (resp. right) module M over a K-algebra is a K-vector space and the endomorphisms of M is the ring of K-linear endomorphisms.

Definition 1.2. A **simple ring** A is a ring where 0 and A are the only two-sided ideals of A.

Example 1.3. $M_n(K)$ is simple, where $M_n(K)$ denotes the $n \times n$-matrix ring over a field K. Just observe that every two-sided ideal of $M_n(K)$ is of the form $M_n(I)$ where I is an ideal

of K. However, 0 and K are the only ideals in K, so 0 and $M_n(K)$ are the only two-sided ideals of $M_n(K)$.

For any non-commutative ring A, we say that a left (resp. right) A-module M is **simple** if $M \neq 0$ and its only submodules are 0 and M. A proper left (resp. right) ideal I of a ring A is said to be **maximal** if, for J any other left (resp. right) ideal of A, we have that $I \subseteq J \subseteq A$ implies that $J = I$ or $J = A$.

Lemma 1.4. Let A be a ring and let M be a left (resp. right) A-module.

(i) M is simple if and only if $M = Am$ (resp. mA) for all nonzero $m \in M$.

(ii) If M is simple, then, for any nonzero $m \in M$, we have that $\text{ann}_A(m) := \{a \in A : am = 0\}$ is a left (resp. right) maximal ideal of A.

(iii) Every simple left (resp. right) A-module is isomorphic to A/I for some maximal left (resp. right) ideal I of A. Conversely, if I is a maximal left (resp. right) ideal of A, then A/I is a simple left (resp. right) A-module.

(iv) Let M be a maximal left (resp. right) ideal of A. Given any nonzero $a \in A \backslash M$, there exists $b \in A$ and $m \in M$ such that

$$1 = ba + m \quad (\text{resp. } 1 = ab + m).$$

Proof. We will only prove the lemma for left modules and left ideals. The proof for right modules and right ideals is analogues.

(i) Assume that M is simple and let $0 \neq m \in M$ be any nonzero element of M. Since $1 \in A$, we have that $0 \neq m = 1 \cdot m \in Am$ and hence Am is a nonzero submodule of M. Since M is simple, we have that $Am = M$.

Conversely, assume that $M = Am$ for all $0 \neq m \in M$. Let N be any nonzero submodule of M. By assumption, $M = An$ for all $0 \neq n \in N$, so

$$M = An \subseteq N \subseteq M.$$

This implies that $N = M$ so that M has no nonzero proper submodules. Hence M is simple.

(ii) By (i), we know that $M = Am$ for any nonzero $m \in M$. Fix one such m and define $\varphi : A \to Am$ by $a \to am$. Since φ is surjective and $\ker(\varphi) = \text{ann}_A(m)$, we have

that $A/\mathrm{ann}_A(m) \cong M$ by the First Isomorphism Theorem. Let I be a left ideal of A such that $\mathrm{ann}_A(m) \subseteq I \subseteq A$. Then $I/\mathrm{ann}_A(m)$ is a submodule of $A/\mathrm{ann}_A(m)$. Since $A/\mathrm{ann}_A(m)$ is simple, it follows that $I/\mathrm{ann}_A(m) = 0$ or $I/\mathrm{ann}_A(m) = A/\mathrm{ann}_A(m)$. Hence $I = \mathrm{ann}_A(m)$ or $I = A$, that is, $\mathrm{ann}_A(m)$ is maximal.

(iii) Let M be a simple left A-module. Then $M = Am$ for any nonzero $m \in M$ by (i). Fix one such m and define the homomorphism $\varphi : A \to Am$ by $a \mapsto am$. Observe that $\ker(\varphi) = \mathrm{ann}_A(m)$ so, since φ is surjective, $A/\mathrm{ann}_A(m) \cong Am$. But $\mathrm{ann}_A(m)$ is maximal by (ii), so M is isomorphic to A/I for the maximal left ideal $I = \mathrm{ann}_A(m)$.

Conversely, let I be a maximal left ideal of A, and let $m \in A\backslash I$. Then $I \subseteq Am + I \subseteq A$ so since I is maximal, we have that $Am + I = A$. Thus

$$\frac{A(m+I)}{I} = \frac{Am+I}{I} = A/I.$$

Hence A/I is simple by (i).

(iv) Define the left ideal $L := Aa + M$. Since $a \in L\backslash M$, we have that $M \subsetneq L$, but M is maximal so $L = A$. Hence $1 \in L$ and there exists $b \in A$ and $m \in M$ such that $1 = ba + m$.

■

Let $I, J, I_1, \ldots, I_n$, where $n \geq 2$ be ideals of the commutative ring R. We say that I and J are **comaximal** precisely when $I + J = R$; also, we say that the family $\{I_i\}_{i=1}^n$ is **pairwise comaximal** if and only if $I_i + I_j = R$ whenever $1 \leq i, j \leq n$ and $i \neq j$. The following proposition is taken from [14, p. 55].

Proposition 1.5. Let $\{I_i\}_{i=1}^n$ for $n \geq 2$ be a pairwise comaximal family of ideals of the commutative ring R. Then

$$I_1 \cap \cdots \cap I_n = I_1 \cdots I_n.$$

1.2 Prime and primary ideals

Let I, J and P be proper ideals of a non-commutative ring A. If $IJ \subseteq P$ implies that $I \subseteq P$ or $J \subseteq P$, we say that P is a **prime ideal**. Equivalently, P is a prime ideal if for $a, b \in A$ such that $aAb \subseteq P$ implies that $a \in P$ or $b \in P$. If the zero ideal of A is prime, we say that A is a **prime ring**. The set of all the prime ideals of R is denoted by $\mathrm{Spec}(R)$.

Lemma 1.6. Let A be a ring and let M be simple left (resp. right) A-module. Then $\mathrm{ann}_A(M)$ is a prime ideal.

Proof. Let $a, b \in A$ be such that $aAb \in \mathrm{ann}_A(M)$. Since $0 \subseteq AbM \subseteq M$ and M is simple, we have that $AbM = 0$ or $AbM = M$. If $AbM = 0$, then $Ab \subseteq \mathrm{ann}_A(M)$ which implies that $1b = b \in \mathrm{ann}_A(M)$. If $AbM = M$, then $aAbM = aM$. But $aAbM = 0$ since $aAb \subseteq \mathrm{ann}_A(M)$, so $aM = 0$ and hence $a \in \mathrm{ann}_A(M)$. It follows that $\mathrm{ann}_A(M)$ is a prime ideal. ■

Lemma 1.7. Let R be a commutative ring and let P be a prime ideal of R. If $X_1, \ldots, X_n$ are non-empty subsets of R for some $n \geq 1$ and

$$\{x_1 x_2 \cdots x_n : x_i \in X_i \text{ for } 1 \leq i \leq n\} \subseteq P,$$

then there exists $1 \leq i \leq n$ such that $X_i \subseteq P$.

Proof. We will prove the lemma by induction on n. The case where $n = 1$ is quite obvious:

$$X_1 = \{x_1 : x_1 \in X_1\} \subseteq P.$$

For the inductive part, assume that the result holds for n and assume that $X_1, \ldots, X_{n+1}$ are non-empty subsets of R such that

$$\{x_1 x_2 \cdots x_{n+1} : x_i \in X_i \text{ for } 1 \leq i \leq n+1\} \subseteq P.$$

Assume now that $X_i \nsubseteq P$ for all $1 \leq i \leq n$. Then

$$\{x_1 x_2 \cdots x_n : x_i \in X_i \text{ for } 1 \leq i \leq n\} \nsubseteq P,$$

by the induction hypothesis. Hence there exist $x_i' \in X_i$ for $1 \leq i \leq n$ such that $x_1' \cdots x_n' \notin P$. Now, for all $x_{n+1} \in X_{n+1}$, we have that $x_1' \cdots x_n' x_{n+1} \in P$. Since P is a prime ideal and since $x_1' \cdots x_n' \notin P$, we must have that $x_{n+1} \in P$ for all $x_{n+1} \in X_{n+1}$. Hence $X_{n+1} \subseteq P$. ■

The **radical** $\sqrt{I}$ of an ideal I over a commutative ring R is defined as

$$\sqrt{I} := \{r \in R : \text{ there exists } n > 0 \text{ for which } r^n \in I\}.$$

We will need the following definition in the next two proofs. Let $(X, \leq)$ be a partially ordered set. A **chain** of elements of a set X is a subset $Y \subseteq X$ of elements of X such that for all $y_1, y_2 \in Y$ we have that either $y_1 \leq y_2$ or $y_2 \leq y_1$.

Lemma 1.8. Let R be a commutative ring and I an ideal. Then

$$\sqrt{I} = \bigcap \{P : P \in \operatorname{Spec}(R) \text{ and } I \subseteq P\}.$$

Proof. Define

$$P^* := \bigcap \{P : P \in \operatorname{Spec}(R) \text{ and } I \subseteq P\}.$$

Let $a \in \sqrt{I}$. By definition there exists $n > 0$ such that $a^n \in I$. For any $P \in \operatorname{Spec}(R)$ with $I \subseteq P$, we have $a^n \in I \subseteq P$ and hence $a \in P$. This shows $\sqrt{I} \subseteq P^*$.

Conversely, let $a \in P^*$. Consider the set of ideals

$$\Omega := \{J \subseteq R : J \text{ is an ideal containing } I \text{ with } a^n \notin J \text{ for all } n > 0\}.$$

Note that $\Omega \neq \emptyset$ if and only if $I \in \Omega$ if and only if $a^n \notin I$ for all $n > 0$. Thus suppose $\Omega \neq \emptyset$, that is, there is no $n > 0$ such that $a^n \in I$. We will apply Zorn's Lemma to obtain a maximal element in Ω. To do so, we equip Ω with the ordinary partial ordering. Let $T \subseteq \Omega$ be a chain of ideals in Ω and set

$$J^* := \bigcup \{J \mid J \in T\}.$$

To see that J^* is an ideal, observe first that $J^* \neq \emptyset$ because $0 \in J^*$. Let $a, b \in J^*$ and $r \in R$. Then there exist ideals $J_1, J_2 \in T$ such that $a \in J_1$ and $b \in J_2$. Since $a \in J_1$, we have that $ra \in J_1 \subseteq J^*$. Furthermore, since T is a chain, either $J_1 \subseteq J_2$ or $J_2 \subseteq J_1$. We assume without loss of generality that $J_1 \subseteq J_2$. Then both $a, b \in J_2$. Since J_2 is an ideal, $a + b \in J_2 \subseteq J^*$.

If $a^n \in J^*$ for some $n > 0$, then there should exist $J \in T$ with $a^n \in J$, which is a contradiction as $J \in \Omega$. Thus $J^* \in \Omega$ and by Zorn's Lemma Ω has a maximal element, say Q. By definition, Q contains I and we will show that Q is a prime ideal, from which we obtain a contradiction, since then $a \in P^* \subseteq Q$ and on the other hand $a \notin Q$. Now take elements $x, y \in R$ with $xy \in Q$. Suppose none of the elements x and y belong to Q. Then the ideals $Q' = Rx + Q$ and $Q'' = Ry + Q$ properly contain Q. By the maximality of Q, we have that $Q', Q'' \notin \Omega$. Hence there exist powers a^n and a^m such that $a^n \in Q'$ and $a^m \in Q''$. But then $a^n = r_1 x + q_1$ and $a^m = r_2 y + q_2$ for some $r_1, r_2 \in R$ and $q_1, q_2 \in Q$. Thus

$$a^{n+m} = (r_1 x + q_1)(r_2 y + q_2) = r_1 r_2 xy + r_1 x q_2 + r_2 y q_1 + q_1 q_2 \in Q,$$

contradicting the assumption that $Q \in \Omega$. Therefore $x \in Q$ or $y \in Q$, i.e. Q is a prime ideal containing I. But then $a \in Q$, which contradicts $a \notin Q$. Therefore $\Omega = \emptyset$ and there must exists $n > 0$ with $a^n \in I$, i.e. $a \in \sqrt{I}$. We conclude that $P^* \subseteq \sqrt{I}$ and thus $\sqrt{I} = P^*$. ∎

Let A be a ring. A left (resp. right) ideal I of A is said to be a **nilpotent left (resp. right) ideal** if there exists $n \in \mathbb{N}$ such that $I^n = 0$ and an element $a \in A$ is said to be a **nilpotent element** if there exists $n \in \mathbb{N}$ such that $a^n = 0$. Note that 0 is nilpotent. An ideal I of A is called **semiprime** if A/I has no nonzero nilpotent ideals and we say that A is **reduced** if it does not contain any nonzero nilpotent elements.

For a commutative ring R, the zero ideal is semiprime if and only if it is reduced, because if a is a nilpotent element, then the ideal $I = Ra$ is nilpotent. And if I is a nilpotent ideal, then any nonzero element of I is nilpotent. It is clear that for any ideal I of R, $\sqrt{I}/I$ contains all nilpotent elements in R/I. Hence an ideal I of R is semiprime if and only if $I = \sqrt{I}$ if and only if I is the intersection of prime ideals, by Lemma 1.8.

A prime ideal P of a ring A is called a **minimal prime ideal** if the only prime ideal that it contains is P itself.

Lemma 1.9. Any prime ideal of a ring A contains a minimal prime ideal [4, p. 44].

A ring A satisfies the **ascending chain condition** for left (resp. right) ideals if for every chain $I_1 \subseteq I_2 \subseteq \ldots I_i \subseteq I_{i+1} \ldots$ of left (resp. right) ideals of A, there exists $n \in \mathbb{N}$ such that $I_n = I_{n+i}$ for all $i \in \mathbb{N}$. A commutative ring R is said to be **noetherian** if and only if it satisfies the following equivalent conditions:

(i) R satisfies the ascending chain condition for ideals;

(ii) every nonempty set of ideals of R has a maximal member with respect to inclusion; and

(iii) every ideal of R is finitely generated.

Lemma 1.10. Any commutative noetherian ring has only a finite number of minimal prime ideals, and a product of some powers of these ideals is zero.

Proof. We will first show that 0 is a product of prime ideals. Let R be a commutative noetherian ring, and let

$$\Omega := \{K \subseteq R : K \text{ is an ideal that does not contain a finite product of prime ideals}\}.$$

If $\Omega = \emptyset$, then every ideal of R contains a finite product of prime ideals. In particular, 0 is a finite product of prime ideals. Our goal is therefore to prove that $\Omega = \emptyset$, and we will do this by showing that the assumption that $\Omega \neq \emptyset$ leads to a contradiction.

Assume $\Omega \neq \emptyset$. Since R is noetherian, Ω has a maximal element K with respect to inclusion. Every nonzero ideal of R/K contains a finite product of prime ideals. As R contains a maximal ideal, it contains a prime ideal. Therefore $R \notin \Omega$, so $K \neq R$ and hence R/K is not a prime ring, that is, $\overline{0}$ is not prime. Thus there exist nonzero ideals $\overline{I} = I/K$ and $\overline{J} = J/K$ of R/K with $\overline{0} = \overline{IJ}$ but where each $\overline{I}, \overline{J}$ contains a finite product of prime ideals, say $\overline{P_1} \cdots \overline{P_n} \subseteq \overline{I}$ and $\overline{Q_1} \cdots \overline{Q_m} \subseteq \overline{J}$. Observe that

$$\overline{P_1} \cdots \overline{P_n Q_1} \cdots \overline{Q_m} \subseteq \overline{IJ} = \overline{0},$$

which implies that

$$P_1 \cdots P_n Q_1 \cdots Q_m \subseteq K,$$

contradicting the fact that $K \in \Omega$. Hence $\Omega = \emptyset$, that is, 0 is a finite product of prime ideals.

We will now prove that a commutative noetherian ring R has only a finite number of minimal prime ideals. We have just proved that there exists prime ideals $P_1, \ldots, P_n$ of R such that $0 = P_1 \cdots P_n$. Let $\min(R)$ denote the set of all minimal prime ideals of R. By Lemma 1.9, $\min(R) \neq \emptyset$. Let $Q \in \min(R)$. Then

$$P_1 \cdots P_n = 0 \subseteq Q,$$

so by Lemma 1.7 there exists $1 \leq i \leq n$ such that $P_i \subseteq Q$. Since Q is minimal, we must have that $P_i = Q$. Since Q was an arbitrary element of $\min(R)$, we conclude that $\min(R) \subseteq \{P_1, \ldots, P_n\}$. Hence R has only a finite number of minimal ideals.

It remains to show that 0 is a product of minimal prime ideals. By Lemma 1.9, there exist minimal prime ideals $P_i' \subseteq P_i$ for each $1 \leq i \leq n$. Hence

$$P_1' \cdots P_n' \subseteq P_1 \cdots P_n = 0,$$

so in fact $0 = P_1' \cdots P_n'$. This proves the lemma. ■

Corollary 1.11. Any semiprime ideal I of a commutative noetherian ring R is the intersection of a finite number of minimal prime ideals over R/I.

Proof. By Lemma 1.8, the zero ideal of $R/\sqrt{I}$ is the intersection of prime ideals. Any of those prime ideals contains a minimal prime ideal by Lemma 1.9. By Lemma 1.10, the set of minimal prime ideals is finite. Hence the zero ideal of $R/\sqrt{I}$ is the intersection of finitely many minimal prime ideals. Thus $\sqrt{I}$ is equal to a finite intersection of minimal prime ideals. ■

Lemma 1.12. Any ideal of a commutative noetherian ring contains a power of its radical.

Proof. Since R is noetherian, $\sqrt{I}$ is generated by a finite number of elements, say $a_1, \ldots, a_n$. By the definition of the radical, there exists a number $m_i > 0$ such that $a_i^{m_i} \in I$ for each $1 \leq i \leq n$. Let $m = m_1 + \cdots + m_n$. Then $(r_1a_1 + \ldots + r_na_n)^m \in I$, for any $r_i \in R$. To see this, just observe that each term in the sum $(r_1a_1 + \ldots + r_na_n)^m$ is of the form $ra_1^{j_1} \cdots a_n^{j_n}$, for some $r \in R$ and where $j_1 + \cdots + j_n = m$. If $j_i < m_i$ for all $1 \leq i \leq n$, then $j_1 + \cdots + j_n < m_1 + \cdots + m_n = m$, a contradiction. Hence $j_i \geq m_i$ for at least one i for each of the terms of $(r_1a_1 + \ldots + r_na_n)^m$. Thus each term is contained in I and hence $(r_1a_1 + \ldots + r_na_n)^m \in I$, for any $r_i \in R$. Since $s \in \sqrt{I} \implies s = r_1a_1^{k_1} + \ldots + r_na_n^{k_n}$ for some $r_i \in R$ and some $k_i \in \mathbb{N}$, we conclude that $\left(\sqrt{I}\right)^m \subseteq I$. ∎

Let Q be an ideal of a commutative ring R. We say that Q is a **primary ideal** of R if

(i) Q is a proper ideal of R, and

(ii) whenever $a, b \in R$ with $ab \in Q$ but $a \notin Q$, then there exits $n \in \mathbb{N}$ such that $b^n \in Q$.

One can show that if Q is a primary ideal of R, then $P := \sqrt{Q}$ is a prime ideal of R [14, p. 63]. We say that Q is **P-primary**.

Let I be a proper ideal of the commutative ring R. As in [14, p. 68] we define a **primary decomposition** of I to be an expression for I as an intersection of finitely many primary ideals of R. Such a primary decomposition

$$I = Q_1 \cap \cdots \cap Q_n,$$

with $\sqrt{Q_i} = P_i$ for $1 \leq i \leq n$, of I is said to be a **minimal primary decomposition** of I precisely when

(i) $P_1, \ldots, P_n$ are n different prime ideals of R, and

(ii) for all $1 \leq j \leq n$ we have

$$Q_j \not\supseteq \bigcap_{\substack{i=1 \\ i \neq j}}^{n} Q_i.$$

We say that I is a **decomposable** ideal of R precisely when it has a primary decomposition.

Lemma 1.13. [14, p. 69]. Every decomposable ideal of R has a minimal primary decomposition. Furthermore, if a primary decomposition of I has n terms, then the number of terms in a minimal primary decomposition of I has at most n terms.

Let I be a decomposable ideal of the commutative ring R, and let

$$I = Q_1 \cap \cdots \cap Q_n \qquad \text{with } \sqrt{Q_i} = P_i \text{ for } i = 1, \ldots, n$$

be a minimal primary decomposition of I. Then the n-element set

$$\{P_1, \ldots, P_n\},$$

which is independent of the choice of minimal primary decomposition by Lemma 1.13, is called **the set of associated prime ideals of** I and is denoted $\operatorname{ass}(I)$.

Theorem 1.14 (The Second Uniqueness Theorem for Primary Decomposition)**.** [14, p. 75]. Let I be a decomposable ideal of the commutative ring R, and let $\operatorname{ass}(I) = \{P_1, \ldots, P_n\}$. Let

$$I = Q_1 \cap \cdots \cap Q_n \qquad \text{with } \sqrt{Q_i} = P_i \text{ for } i = 1, \ldots, n$$

and

$$I = Q'_1 \cap \cdots \cap Q'_n \qquad \text{with } \sqrt{Q'_i} = P_i \text{ for } i = 1, \ldots, n$$

be two minimal primary decompositions of I. Then, for each i with $1 \leq i \leq n$ for which P_i is a minimal prime ideal belonging to I, we have

$$Q_i = Q'_i.$$

1.3 Primitive rings

An ideal P of a ring A is said to be a **left (resp. right) primitive ideal** if P is the annihilator of a simple left (resp. right) A-module. Note that, by Lemma 1.6, this implies that every left (resp. right) primitive ideal is prime. If the zero ideal of a ring A is left (resp. right) primitive, we say that A is **primitive on the left (resp. right)**. Equivalently, A is left (resp. right) primitive if it has a faithful simple left (resp. right) A-module M.

Remark 1.15. Every simple ring A is both left and right primitive. To see this, recall that the only two-sided ideals of A are 0 and A, so in particular $\operatorname{ann}_A(M) = 0$ for every nonzero

left (resp. right) A-module M. Hence any left (resp. right) A-module would be faithful. Now, $1 \in A$ implies that there exists a maximal left (resp. right) ideal I of A, and thus A/I is a simple left (resp. right) A-module. We conclude that A is left and right primitive.

Lemma 1.16. A commutative ring R is primitive if and only if it is a field.

Proof. Let R be a field. Then 0 and R are the only ideals. Since $\operatorname{ann}_R(R)$ is an ideal of R, $\operatorname{ann}_R(R) = 0$ or $\operatorname{ann}_R(R) = R$. If $\operatorname{ann}_R(R) = R$, then $rR = 0$ for all $r \in R$. In particular, $1 \cdot R = 0$, a contradiction. Hence $\operatorname{ann}_R(R) = 0$. Since R is a simple faithful module of R, we have that R is primitive.

Conversely, assume that R is a commutative primitive ring. Since R is primitive, it has a faithful simple R-module M. By Lemma 1.4 (iii), $M = R/I$ for some maximal ideal I of R. Since R is commutative, I is two-sided and hence

$$\operatorname{ann}_R(R/I) = \{r \in R : (r+I)(R/I) = 0\} = \{r \in R : rs \in I \text{ for all } s \in R\} \supseteq I.$$

Since I is maximal, and because $\operatorname{ann}_R(R/I) \neq R$ since $1 \notin \operatorname{ann}_R(R/I)$, we conclude that $I = \operatorname{ann}_R(R/I)$. It follows that $I = 0$ because R/I is faithful. But then $M = R/0 = R$, so R itself is simple. Since R is commutative, we conclude that R is a field. ∎

Let X be a set. A **word** in X is a concatenation of some elements of X. We denote the empty word by λ, and we denote the set of all words on X, together with λ, by X^*.

Example 1.17. Let $X = \{x, y, z\}$. Then x, $yzyzx$ and $y^2xyz^5x^2$ are examples of words in X.

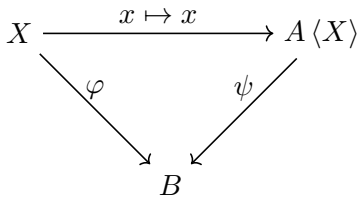
Let A be any ring. The **free algebra** on X over A is denoted by $A\langle X\rangle$ and is defined by

$$A\langle X\rangle = \left\{ \sum_{w \in X^*} a_w w : a_w \in A \right\},$$

where only finitely many a_w are nonzero. For any words $w, u \in X^*$, multiplication is defined as $(a_w w) \cdot (a_u u) = (a_w a_u)\, wu$ and addition is defined as $a_w w + a'_w w = (a_w + a'_w)w$. Thus the free algebra on X over F is the free vector space whose basis are the words in X. The free algebra can also be thought of as non-commutative polynomials since for example x^2zx could be different from x^3z.

Let X be a set, A, B rings, $A\langle X\rangle$ the free algebra on X over A, $\Phi : A \to B$ a ring homomorphism and φ a map from X to B. According to [2, p. 138], φ and Φ can be

extended to a homomorphism ψ from $A\langle X\rangle$ to B, such that $\psi(a) = \Phi(a)$ for all $a \in A$ and such that the following diagram commutes:



This is called the **universal property** of $A\langle X\rangle$.

Example 1.18. The free algebra on $X = \{x_1, \ldots, x_n\}$ over $\mathbb{Z}$ is

$$\mathbb{Z}\langle X\rangle = \left\{ \sum_{i=1}^{n} a_{w_i} w_i : w_i \in X^*, a_{w_i} \in \mathbb{Z}, n \geq 1 \right\}.$$

A commutative factor is

$$\frac{\mathbb{Z}\langle X\rangle}{\langle \{x_i x_j - x_j x_i : 1 \leq i, j \leq n\} \rangle}.$$

Let $N \subseteq \mathbb{N}$ be a subset of the positive integers $\mathbb{N}$. Let $X = \{x_i : i \in N\}$ be a set of indeterminates and let $Z\langle X\rangle$ denote the free algebra on X over the integers $\mathbb{Z}$. Let A be a ring. An element

$$f = \sum_{\sigma \in S_n} k_\sigma x_{\sigma(1)} \cdots x_{\sigma(n)} \in \mathbb{Z}\langle X\rangle, \tag{1.1}$$

where $k_\sigma \in \mathbb{Z}$, is said to be a **multi-polynomial identity** of A if $f(a_1, \ldots, a_n) = 0$ for all $a_1, \ldots, a_n \in A$. We say that A is a **PI-ring** if there exists $f \in \mathbb{Z}\langle X\rangle$ as in (1.1) such that $k_\sigma = 1$ for at least one $\sigma \in S_n$ and f is a multi-polynomial identity of A.

Theorem 1.19 (Kaplansky)**.** [2, p. 185]. A left (resp. right) primitive PI-ring A is a simple algebra finite dimensional over its center.

Lemma 1.20. [10, p. 492]. Let R be a commutative subring of a ring A such that A is a finitely generated left or right R-module. Then A is a PI-ring.

1.4 Dedekind domains

Let K be a field and let F be the field of fractions of an integral domain R. An element $\alpha \in K$ is said to be **integral over** R if an only if α is a zero of a polynomial in $R[y]$ whose leading coefficient is 1. We say that an integral domain R is **integrally closed** if $\alpha \in F$ and α integral over R implies that $\alpha \in R$.

Let R be a commutative integral domain. We say that R is a **Dedekind domain** if and only if

(i) R is noetherian,

(ii) every nonzero prime ideal of R is maximal, and

(iii) R is integrally closed.

Every principal ideal domain is Dedekind and, in particular, $K[y]$ is Dedekind.

The following Corollary is taken from [3, p. 258] and is important for our study of skew polynomial rings in Chapter 3.

Corollary 1.21 (Dedekind)**.** Let R be a Dedekind domain. Every nonzero ideal of R can be written uniquely as the product of prime ideals.

As a consequence of Corollary 1.21 and Lemma 1.7 we have:

Corollary 1.22. Let R be a Dedekind domain, P any prime ideal and I any nonzero ideal of R. Then $I \subseteq P$ if and only if there exists an ideal I' such that $I = PI'$.

Proof. Assume that $I \subseteq P$ for a nonzero ideal I and a prime ideal P, and suppose $I = P_1 \cdots P_n$ is a prime decomposition with prime ideals P_i (not necessarily different). Since $P_1 \cdots P_n = I \subseteq P$, by Lemma 1.7, there exist $1 \leq i \leq n$ such that $P_i \subseteq P$. However P_i is a nonzero prime ideal and any nonzero prime ideal of R is maximal. Thus $P_i = P$ and $I = P_i I'$ where $I' = P_1 \cdots P_{i-1} P_{i+1} \cdots P_n$. The converse is clear. ∎

Let I be an ideal and P a prime ideal in a Dedekind domain R. We say that P **divides** I or that P is a **prime divisor** of I if $I \subseteq P$. The P**-order of** I, denoted $\nu_P(I)$, is the largest $m \geq 0$ such that $I \subseteq P^m$ but $I \nsubseteq P^{m+1}$. This terminology is justified by Corollary 1.22, because if $I \subseteq P$, then $I = PI'$ for some ideal I'. Furthermore if we write the prime decomposition of I as $I = P_1^{\alpha_1} \cdots P_k^{\alpha_l}$ with different primes P_i and numbers $\alpha_i \geq 1$, then the P-order of I is α_i if $P = P_i$ and 0 if P is different from all prime ideals P_i. The P**-order** $\nu_P(r)$ **of an element** $r \in R$ is defined to be $\nu_p(\langle r \rangle)$.

We can generalise Corollary 1.22 as

Corollary 1.23. Let R be a Dedekind domain, I an ideal, P a prime ideal and $m \geq 0$. Then $I \subseteq P^m$ if and only if $\nu_P(I) \geq m$.

Proof. Assume $I \subseteq P^m$. Since $\nu_P(I)$ is the largest integer such that $I \subseteq P^{\nu_P(I)}$, we conclude that $m \leq \nu_P(I)$. Conversely, assume $\nu_P(I) \geq m$. Then $I \subseteq P^{\nu_P(I)} \subseteq P^m$. ■

A consequence of Corollary 1.23 is

Corollary 1.24. Let P be a nonzero prime ideal of a Dedekind domain R and $m > 0$. If I is an ideal of R, such that $P^{m+1} \subseteq I \subseteq P^m$, then $I = P^m$ or $I = P^{m+1}$.

Proof. Since $I \subseteq P^m$, we have that $\nu_P(I) \geq m$ by Corollary 1.23. Decompose $I = P^{\nu_P(I)}Q$ with $\nu_P(Q) = 0$. Then $P^{m+1} \subseteq P^{\nu_P(I)}$ shows that $m + 1 \geq \nu_P(I) \geq m$, which means that $\nu_P(I) = m + 1$ or $\nu_P(I) = m$. In the first case $P^{m+1} \subseteq I = P^{m+1}Q \subseteq P^{m+1}$ which implies that $P^{m+1} = I$. In the latter case one has $P^{m+1} \subseteq I = P^mQ \subseteq P^m$. Since $\nu_P(Q) = 0$, then Q and P are comaximal, i.e. $R = P + Q$. Hence $P^m = P^m(P + Q) = P^{m+1} + I = I$. ■

Corollary 1.25. Let I and J be nonzero ideals of a Dedekind domain R and let P be a prime ideal of R. Then

(i) $\nu_P(IJ) = \nu_P(I) + \nu_P(J)$

(ii) $\nu_P(I + J) \geq \min\{\nu_P(I), \nu_P(J)\}$

As a consequence, $\nu_P(ab) = \nu_P(a) + \nu_P(b)$ and $\nu_P(ab) \geq \min\{\nu_P(a), \nu_P(b)\}$ for any $a, b \in R$.

Proof. Let $\nu_P(I) = m$ and $\nu_P(J) = n$. Then $I = P^mQ_1$ and $J = P^nQ_2$ for some ideals Q_1, Q_2 with $\nu_P(Q_1) = 0$ and $\nu_P(Q_2) = 0$.

(i) We have that $IJ = P^{m+n}Q_1Q_2$. Assume that $\nu_P(Q_1Q_2) > 0$. Then $Q_1Q_2 \subseteq P$. But then, since P is prime, $Q_1 \subseteq P$ or $Q_2 \subseteq P$, contradicting that $\nu_P(Q_1) = 0$ and $\nu_P(Q_2) = 0$. Hence $\nu_P(Q_1Q_2) = 0$ and therefore $\nu_P(IJ) = m + n = \nu_P(I) + \nu_P(J)$, using the uniqueness of the decomposition of I and J as products of primes.

(ii) Assume $n \leq m$; the case where $m \leq n$ can be proven analogously. As above, $I = P^mQ_1$ and $J = P^nQ_2$. Then

$$\nu_P(I + J) = \nu_P\left(P^mQ_1 + P^nQ_2\right) = \nu_P\left(P^n\left(P^{m-n}Q_1 + Q_2\right)\right) \geq n = \min\{\nu_P(I), \nu_P(J)\}$$

■

Definition 1.26. The **least common multiple** of ideals $B_1, \ldots, B_d$ in a Dedekind domain R is defined as follows: Write each ideal as $B_j = P_1^{\alpha_{1j}} \cdots P_n^{\alpha_{nj}}$ where $P_1, \ldots, P_n$ are distinct prime ideals and $\alpha_{ij} \geq 0$ for $1 \leq i \leq n$ and $1 \leq j \leq d$. Then the least common multiple of the ideals $B_1, \ldots, B_d$ is defined by

$$LCM(B_1, \ldots, B_d) := P_1^{\max(\alpha_{11}, \ldots, \alpha_{1d})} \cdots P_n^{\max(\alpha_{n1}, \ldots, \alpha_{nd})}.$$

This means in particular that for any prime ideal P, we have that

$$\nu_P(LCM(B_1, \ldots, B_d)) = \max(\nu_P(B_1), \ldots, \nu_P(B_d)).$$

The **Jacobson radical** of a ring A is the intersection of all left (resp. right) primitive ideals of A and is denoted $\mathrm{rad}(A)$. That is, if Λ is the set of all left primitive ideals of A and Γ is the set of all right primitive ideals of A, then

$$\mathrm{rad}(A) = \bigcap_{I \in \Lambda} I = \bigcap_{I \in \Gamma} I.$$

Since $\mathrm{rad}(A)$ is a two-sided ideal of A, we avoid the term left (resp. right) when referring to the Jacobson radical. We will not prove that $\bigcap_{I \in \Lambda} I = \bigcap_{I \in \Gamma} I$ but instead refer to books like [2] and [8]. The following lemma about the Jacobson radical is taken from [8, p. 50], and will be needed in the proof of Theorem 1.42.

Lemma 1.27. Let A be a ring an let $b \in A$. Then the following statements are equivalent:

(i) $b \in \mathrm{rad}(A)$;

(ii) $1 - ab$ is left-invertible for any $a \in A$;

(iii) $bM = 0$ for any simple left A-module M

The equivalent right version is of course also true.

Lemma 1.28. Let R and S be commutative rings and let $\varphi : S \to R$ be a ring homomorphism. Then for any ideal I of R, the set

$$\varphi^{-1}(I) = \{s \in S : \varphi(s) \in I\}$$

is an ideal of S. In particular, φ induces a map

$$\varphi^* : \mathrm{Spec}(R) \to \mathrm{Spec}(S)$$
$$P \mapsto \varphi^{-1}(P).$$

Proof. Since $\varphi(0) = 0 \in I$, $\varphi^{-1}(I)$ is nonempty. Furthermore, for $a, b \in \varphi^{-1}(I)$, we have that $\varphi(a+b) = \varphi(a) + \varphi(b) \in I$ since φ is a homomorphism and since $\varphi(a), \varphi(b) \in I$. Hence $a+b \in \varphi^{-1}(I)$. Finally, let $a \in \varphi^{-1}(I)$ and $s \in S$. Then $\varphi(as) = \varphi(a)\varphi(s) \in I$ since $\varphi(a) \in I$. Thus $as \in \varphi^{-1}(I)$. This shows that $\varphi^{-1}(I)$ is an ideal of S.

Let now P be a prime ideal. For any $s, t \in S$ with $st \in \varphi^{-1}(P)$ one has

$$\varphi(s)\varphi(t) = \varphi(st) \in \varphi(\varphi^{-1}(P)) \subseteq P.$$

Since P is a prime ideal, $\varphi(s) \in P$ or $\varphi(t) \in P$, which means that $s \in \varphi^{-1}(P)$ or $t \in \varphi^{-1}(P)$. Thus $\varphi^{-1}(P)$ is a prime ideal of S. ■

The following corollary is an immediate consequence of Lemma 1.28.

Corollary 1.29. Let $\varphi : R \to R$ be an endomorphism of a commutative ring R. If P is a prime ideal in R, then, for all $i \geq 0$, $\varphi^{-i}(P) := \{r \in R : \varphi^i(r) \in P\}$ is prime as well.

Let $\varphi : R \to R$ be a ring endomorphism of R. The **φ-orbit** of a prime ideal $P \in \mathrm{Spec}(R)$ is the set

$$\mathrm{orb}_\varphi(P) := \{(\varphi^*)^i(P) : i \geq 0\} = \{\varphi^{-i}(P) : i \geq 0\},$$

where $\varphi^0 = \mathrm{id}$. A prime ideal P is called **φ-periodic** if there exists an integer $n \geq 1$ such that $\varphi^{-n}(P) = P$. In this case $|\mathrm{orb}_\varphi(P)|$ is finite and the least such n is called the **period** of P.

Remark 1.30. If $\mathrm{orb}_\varphi(P)$ is finite, then $\mathrm{orb}_\varphi(P)$ must contain a φ-periodic prime ideal. Moreover, if P is φ-periodic, then

$$\mathrm{orb}_\varphi(P) = \mathrm{orb}_\varphi(\varphi^{-i}(P))$$

for all $i \geq 0$.

A φ-periodic prime ideal P of period n is called **singular** if $\varphi^n(P) \subseteq P^2$.

Example 1.31. Let $R = \mathbb{C}[y]$. Since R is a principal ideal domain, any nonzero prime ideal is maximal and of the form $P = \langle y - a \rangle$ for some $a \in \mathbb{C}$. Let $\varphi : R \to R$ be the endomorphism defined by $\varphi(y) = f(y)$ for some $f \in R$ (see the last paragraph of section 1.5) and denote $f(f(\cdots f(y)\cdots))$ i times by $f^i(y)$. For any $i > 0$ we have that $\varphi^i(y - f^i(a)) = f^i(y) - f^i(a)$. Thus $y = a$ is a root of $\varphi^i(y - f^i(a))$ and hence $\varphi^i(y - f^i(a)) \in P$ which implies that $y - f^i(a) \in \varphi^{-i}(P)$. Since $\langle y - f^i(a) \rangle$ is a maximal ideal contained in $\varphi^{-i}(P)$, we have $\varphi^{-i}(P) = \langle y - f^i(a) \rangle$. In addition, one can show that $\langle \varphi^i(P) \rangle = \langle f^i(y) - a \rangle$.

For a prime ideal $P = \langle y - a \rangle$, we have that $\varphi^{-n}(P) = \langle y - f^n(a) \rangle = P = \langle y - a \rangle$ if and only if $f^n(a) = a$, so we conclude that P is φ-periodic if and only if $f^n(a) = a$.

Let $\varphi(y) = f(y) = y^3$ and $P = \langle y - a \rangle$. Then $\varphi^{-i}(P) = \left\langle y - a^{3^i} \right\rangle$ and $\langle \varphi^i(P) \rangle = \left\langle y^{3^i} - a \right\rangle$. For $a = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$, the eighth root of 1, we have that

$$\varphi^{-2}(P) = \left\langle y - \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \right)^9 \right\rangle = \left\langle y - \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \right) \right\rangle = P,$$

so P is φ-periodic of period 2. Furthermore, one can show that $\langle \varphi^2(P) \rangle = \langle y^9 - a \rangle = \langle y^9 - a^9 \rangle$ has 9 different factors, so the P-order of $\langle \varphi^2(P) \rangle$ is 1. Hence $\varphi^2(P) \nsubseteq P^2$, that is, P is not singular.

Proposition 1.32. Let P be a nonzero φ-periodic prime ideal of period n of a Dedekind domain R with injective ring homomorphism $\varphi : R \to R$. Then P is singular or $\varphi^{-n}(P^m) = P^m$ for any $m \geq 1$.

Proof. Suppose P is not singular. Then for $m = 1$ we have $\varphi^{-n}(P^1) = P^1$ since P is φ-periodic of period n. Suppose $m \geq 1$ and it has already been proven that $\varphi^{-n}(P^m) = P^m$. Then $\langle \varphi^n(P^{m+1}) \rangle \subseteq \langle \varphi^n(P)^{m+1} \rangle \subseteq P^{m+1}$ shows that $P^{m+1} \subseteq \varphi^{-n}(P^{m+1})$. On the other hand, for any $y \in \varphi^{-n}(P^{m+1})$ we have that $\varphi^n(y) \in P^{m+1} \subseteq P^m$ and hence $y \in \varphi^{-n}(P^m) = P^m$. It follows that the ideal $\varphi^{-n}(P^{m+1})$ lies between P^{m+1} and P^m and therefore, by Corollary 1.24, $\varphi^{-n}(P^{m+1}) = P^{m+1}$ or $\varphi^{-n}(P^{m+1}) = P^m$. But the latter case would imply P to be singular, because if $\varphi^{-n}(P^{m+1}) = P^m$ holds, then $\langle \varphi^n(P^m) \rangle \subseteq P^{m+1}$ and therefore, by Corollary 1.23, we have that $m + 1 \leq \nu_P(\langle \varphi^n(P^m) \rangle) = m\nu_P(\langle \varphi^n(P) \rangle)$. Hence $\nu_P(\langle \varphi^n(P) \rangle) \geq 2$ or, in other words, $\varphi^n(P) \subseteq P^2$. But we assumed P not to be singular. By induction we therefore get that $\varphi^{-n}(P^m) = P^m$, for all $m \geq 0$. ∎

Note that both cases in the last proposition cannot occur for the same P, because then both $\varphi^n(P) \subseteq P^2$ and $\varphi^{-n}(P^2) = P^2$. Hence $P \subseteq \varphi^{-n}(P^2) = P^2 \subseteq P$ which implies that $P = P^2$. This is impossible because then $1 = \nu_P(P) = \nu_P(P^2) = 2$.

1.5 Skew polynomial rings

Let A be a ring and $X = \langle x \rangle$ a set of one element. Then the free algebra $A\langle X \rangle$ over A in X is called the **polynomial ring** over A in one variable, and is denoted $A[x]$. Addition and multiplication of two elements of $A[x]$ are defined by

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n,$$

$$\left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} b_n x^n\right) = \sum_{n=0}^{\infty} c_n x^n, \quad \text{where } c_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

Here all but finitely many of the coefficients a_i and b_i are 0. Regarding the associativity, we refer to [10]. In the polynomial ring $A[x]$, we have that $xa = ax$ for all $a \in A$, that is, x and a commute. If we instead require that $xa = \varphi(a)x$, where φ is a ring endomorphism of A, we get

$$(ax^i)(bx^j) = a\varphi^i(b)x^{i+j} \tag{1.2}$$

for all $a, b \in A$. The set of polynomials $\sum_{i=0}^{n} a_i x^i$ endowed with the usual addition and the multiplication determined by (1.2) is called a **skew polynomial ring** [2, p. 20], [10, p. 16]. It is denoted by $A[x, \varphi]$. For an element

$$a = \sum_{i=0}^{n} a_i x^i \in A[x, \varphi]$$

with $a_n \neq 0$, we call $a_n x^n$ the **leading term of** a, a_n the **leading coefficient of** a, and n the **degree of** a. By definition, $A[x, \varphi]$ is a free left A-module with basis $\{x^i : i \geq 0\}$.

A ring D is called a domain if whenever $ab = 0$, then $a = 0$ or $b = 0$.

Proposition 1.33. Let $A = D[x, \varphi]$ where D is a domain and $\varphi : D \to D$ an injective endomorphism. Then A is a domain.

Proof. Let

$$a = \sum_{i=0}^{n} a_i x^i \text{ and } b = \sum_{j=0}^{n} b_j x^j$$

be two elements of A such that $ab = 0$. We will assume that $a \neq 0$, so the leading coefficient a_n of a is nonzero. Then

$$\begin{aligned} 0 = ab &= \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right) = \sum_{k=0}^{n+m}\left(\sum_{i+j=k} a_i \varphi^i(b_j)\right) x^k \\ &= a_n \varphi^n(b_m) x^{n+m} + \sum_{k=0}^{n+m-1}\left(\sum_{i+j=k} a_i \varphi^i(b_j)\right) x^k \end{aligned}$$

implies that $a_n \varphi^n(b_m) = 0$. Since $a_n \neq 0$ and D is a domain, we must have that $\varphi^n(b_m) = 0$. Since φ is injective, φ^n is injective as well, and therefore $b_m = 0$. Hence $b = 0$, that is, there is no nonzero b such that $ab = 0$. This proves that A is a domain. ■

Remark 1.34. Note that if D is a division ring, then any endomorphism is injective. Since D is a division ring, it is simple. Hence $\ker(\varphi) = 0$ or $\ker(\varphi) = D$. If $\ker(\varphi) = D$, then $\varphi(d) = 0$ for all $d \in D$. This is not possible because D is a division ring and hence unital, so $\varphi(1) = 1 \neq 0$. Hence $\ker(\varphi) = 0$ and φ is injective.

Proposition 1.35. Let $A = D[x, \varphi]$ where D is a division ring and $\varphi : D \to D$ an endomorphism. Then A is a principal left ideal domain.

Proof. Let I be any nonzero left ideal of A and take a nonzero element $g = \sum_{i=0}^{m} s_i x^i \in I$ of minimal degree in I, where $s_i \in D$ and $s_m \neq 0$. Let h be any nonzero element in I. Then $h = \sum_{i=0}^{n} t_i x^i$ for some $t_i \in D$ and $t_n \neq 0$. Note that $n \geq m$. Then

$$\begin{aligned} h - t_n\left(\varphi^{n-m}(s_m)\right)^{-1} x^{n-m} g &= \sum_{i=0}^{n} t_i x^i - t_n\left(\varphi^{n-m}(s_m)\right)^{-1} \sum_{i=0}^{m} x^{n-m} s_i x^i \\ &= \sum_{i=0}^{n} t_i x^i - t_n\left(\varphi^{n-m}(s_m)\right)^{-1} \sum_{i=0}^{m} \varphi^{n-m}(s_i) x^{n-m} x^i \\ &= \sum_{i=0}^{n} t_i x^i - t_n x^{m+n-m} - t_n\left(\varphi^{n-m}(s_m)\right)^{-1} \sum_{i=0}^{m-1} \varphi^{n-m}(s_i) x^{n-m+i}. \end{aligned}$$

The leading term is $t_n x^n - t_n x^{m+n-m} = 0$. Since $h - t_n\left(\varphi^{n-m}(s_m)\right)^{-1} x^{n-m} g$ is of lower degree than h, one can use induction to show that $h = qg + r$ for some $q \in D$ and some $r \in A$ of degree strictly less than the degree of g. Since $g, h \in I$, we have that $r = h - qg \in I$. Since $\deg(r) < \deg(g)$ and the degree of g is minimal, we have that $r = 0$. Hence $h = qg$, and since h was arbitrary chosen, we conclude that $I = Ag$, that is, A is a principal left ideal domain. ■

Let $R = K[y]$ for a field K of characteristic 0, and let $\varphi : R \to R$ be a K-linear ring endomorphism. Define the skew polynomial ring $A := R[x, \varphi] = K[y][x, \varphi]$. Because $xy = \varphi(y)x$ we can write any element in A as

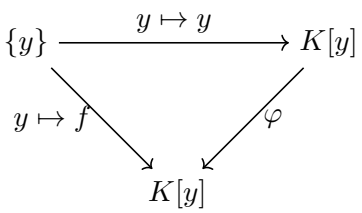
$$\sum_{i=0}^{n} \left(\sum_{j=0}^{m} k_{i,j} y^j \right) x^i$$

for some $k_{i,j} \in K$, that is, the set $\{y^i x^j : i, j \geq 0\}$ forms a K-basis for A. Notice also that A is a free left R-module with basis $\{x^i : i \geq 0\}$ and that every element in A can be uniquely written as $\sum_{i=0}^{n} g_i(y)x^i$, for some $n \in \mathbb{N}$ and $g_i \in R$.

We will now establish that every K-linear endomorphism φ of R is determined by the element $\varphi(y)$. Let $\varphi : R \to R$ be an endomorphism and let $a = \sum_{i=0}^{n} a_i y^i$, where $a_i \in K$, be an element in R. Then

$$\varphi(a) = \varphi\left(\sum_{i=0}^{n} a_i y^i \right) = \sum_{i=0}^{n} a_i \varphi\left(y^i\right) = \sum_{i=0}^{n} a_i \varphi(y)^i,$$

so if φ_1 and φ_2 are ring endomorphisms such that $\varphi_1(y) = \varphi_2(y)$, then $\varphi_1 = \varphi_2$. By the universal property of the free algebra $K\langle y \rangle = K[y]$, for any $f \in K[y]$ there exists a unique ring homomorphism $\varphi : K[y] \to K[y]$ such that the following diagram commutes:



Hence, for every polynomial $f \in R$, there exist a unique ring endomorphism $\varphi : R \to R$ such that $\varphi(y) = f$, that is, there exists a bijection between the K-linear ring endomorphisms of $K[y]$ and the elements of $K[y]$.

1.6 φ-prime ideals

We will in the following define several special ideals that are important for this thesis. Let R be a commutative ring with endomorphism φ. An ideal I of R is called **φ-invariant** if $\varphi^{-1}(I) = I$. Equivalently, I is φ-invariant if

(i) $\varphi(I) \subseteq I$, and

(ii) for all $r \in R$: $\varphi(r) \in I$ implies that $r \in I$.

Remark 1.36. φ is injective if and only if the zero ideal is φ-invariant. To see this, we notice that

$$\varphi \text{ is injective} \iff \ker(\varphi) = 0 \iff \varphi^{-1}(0) = 0 \iff 0 \text{ is } \varphi\text{-invariant.}$$

We call a φ-invariant ideal I **φ-prime** if, given two ideals J and K such that $\varphi(J) \subseteq J$ and $JK \subseteq I$, either $J \subseteq I$ or $K \subseteq I$. If the zero ideal is φ-prime, we say that R is a **φ-prime ring**. An ideal I of R is **φ-cyclic** if $I = P_1 \cap \cdots \cap P_n$, where the P_i are distinct prime ideals of R such that $\varphi^{-1}(P_{i+1}) = P_i$ for all $1 \leq i \leq n-1$ and $\varphi^{-1}(P_1) = P_n$. A ring is called φ-cyclic if the zero ideal is φ-cyclic.

Lemma 1.37. Let R be a commutative domain with endomorphism φ. Then R is a φ-prime ring if and only if φ is injective.

Proof. Let J, K be ideals of R such that $JK = 0$ and assume $J \neq 0$. Then there exists a nonzero element $j \in J$. Since $jk = 0$ for all $k \in K$ and because R is a domain, we must have that $k = 0$ for all $k \in K$, that is, $K = 0$. This shows that 0 is a prime ideal. Hence R is φ-prime if and only if 0 is φ-invariant if and only if φ is injective.

■

Lemma 1.38. Let R be a commutative noetherian ring, φ an endomorphism and I a φ-prime ideal. Then $I = \sqrt{I}$ is semiprime and there exists a φ-periodic prime ideal P of period n such that

$$I = P \cap \varphi^{-1}(P) \cap \cdots \cap \varphi^{-n+1}(P).$$

Proof. Let $a \in \sqrt{I}$. Then there exists $n > 0$ with $a^n \in I$. Hence $\varphi(a)^n = \varphi(a^n) \in \varphi(I) \subseteq I$ which means that $\varphi(a) \in \sqrt{I}$. Hence $\varphi\left(\sqrt{I}\right) \subseteq \sqrt{I}$. By Lemma 1.12, there exists $m \geq 1$ such that $\left(\sqrt{I}\right)^m \subseteq I$. Because I is a φ-prime ideal, we have that $\sqrt{I} \subseteq I$. Hence $\sqrt{I} = I$, that is, I is semiprime.

By Corollary 1.11, I is a finite intersection of minimal prime ideals, say

$$I = P_1 \cap \cdots \cap P_n. \tag{1.3}$$

The representation (1.3) can be considered a minimal primary decomposition of I, when grouping equal prime ideals together. More precisely, suppose that $P_1, \ldots, P_m$ are all the different prime ideals in (1.3) and define $Q_i := \bigcap\{P_j : P_j = P_i\}$ for $1 \leq i \leq m$. Then $I =$

$Q_1 \cap \cdots \cap Q_m$ is a minimal primary decomposition by Lemma 1.13. By the Second Uniqueness Theorem For Primary Decomposition (Theorem 1.14), this decomposition is unique up to the occurring primes P_i. Since I is φ-invariant, we get another decomposition

$$I = \varphi^{-1}(I) = \varphi^{-1}(P_1) \cap \cdots \cap \varphi^{-1}(P_n).$$

For any $1 \leq i \leq n$, we have $\varphi^{-1}(P_1) \cap \cdots \cap \varphi^{-1}(P_n) = I \subseteq P_i$. Hence there exists an index $1 \leq \sigma(i) \leq n$ with $\varphi^{-1}(P_{\sigma(i)}) \subseteq P_i$ by Lemma 1.7. As $\varphi^{-1}(P_{\sigma(i)})$ is a prime ideal contained in the minimal prime ideal P_i , we must have $\varphi^{-1}(P_{\sigma(i)}) = P_i$. Because of the uniqueness of primary decomposition we must have that all prime ideals $\varphi^{-1}(P_j)$ equal one of the prime ideals $P_1, \ldots, P_n$. Hence applying φ^{-1} yields a permutation of the set $\{P_1, \ldots, P_n\}$. Let $\mathrm{Orb}_\varphi(P_1)$ be the φ-orbit of P_1. We can assume that the primes P_i are ordered such that $\mathrm{Orb}_\varphi(P_1) = \{P_1, \ldots, P_k\}$ with $k \leq n$. Suppose $k \neq n$. Set

$$J = P_1 \cap \cdots \cap P_k \quad \text{and} \quad K = P_{k+1} \cap \cdots \cap P_n.$$

Since, for each $1 \leq j \leq k$, we have that $\varphi^{-1}(P_j) = P_i$ for some $1 \leq i \leq k$, we know that $\varphi(P_i) \subseteq P_j$. Thus

$$\varphi(J) \subseteq \varphi(P_1) \cap \cdots \cap \varphi(P_k) \subseteq P_1 \cap \cdots \cap P_k = J.$$

Therefore, since $\varphi(J) \subseteq J$, $JK \subseteq J \cap K = I$ and I is φ-prime, we have $J \subseteq I$ or $K \subseteq I$. Since $I \subseteq J$ and $I \subseteq K$, we have equality. In either case I is written as the intersection of fewer prime ideals as in (1.3), which is a contradiction to our minimality assumption. Hence $n = k$ and

$$I = P_1 \cap \cdots \cap P_n = P \cap \varphi^{-1}(P) \cap \cdots \cap \varphi^{-n+1}(P)$$

for the φ-periodic prime $P = P_1$. ■

Theorem 1.39. Let R be a commutative ring and φ an endomorphism of R. Then $R[x, \varphi]$ is a prime ring if and only if R is a φ-prime ring and φ is injective.

Proof. Assume that R is a φ-prime ring and that φ is injective. Let U and V be ideals of $A = R[x, \varphi]$ such that $VU = 0$. If we can show that $U = 0$ or $V = 0$, then we have shown that A is a prime ring. Hence suppose that $U \neq 0$ and let $f = \sum_{i=0}^{n} a_i x^i \in U$ be any nonzero element with $a_n \neq 0$. For any element $g = \sum_{l=0}^{m} b_l x^l \in V$ and $j \geq 0$ we have $gx^j f \in VU = 0$. Hence

$$0 = gx^j f = \sum_{l=0}^{m} \sum_{i=0}^{n} b_l x^l x^j a_i x^i = \sum_{l=0}^{m} \sum_{i=0}^{n} \varphi^{l+j}(a_i) b_l x^{l+i+j}, \tag{1.4}$$

whose leading coefficient $\varphi^{m+j}(a_n)b_m$ must be zero. Consider the ideals $I = \sum_{j=0}^{\infty} \varphi^{m+j}(a_n)R$ and $J = b_m R$ of R. Then $\varphi(I) \subseteq I$ and by (1.4),

$$IJ = \sum_{j=0}^{\infty} \varphi^{m+j}(a_n)b_m R = 0.$$

As φ is injective and $a_n \neq 0$ we have that $\varphi^m(a_n) \neq 0$. Hence $I \neq 0$ since $\varphi^m(a_n) \in I$. This implies that $J = 0$ since R is a φ-prime ring. Therefore $b_m = 0$. However, this means that the only element in V is the zero element, i.e. $V = 0$.

Conversely, assume $A = R[x;\varphi]$ is a prime ring. Since $I = A\ker(\varphi)A$ is an ideal of A and $Ix = A\ker(\varphi)x = 0$, we must have that $I = 0$, that is, φ is injective. Let I and J be ideals of R such that $\varphi(I) \subseteq I$ and $IJ = 0$. We need to show that $I = 0$ or $J = 0$. Suppose $I \neq 0$. Since $\varphi(I) \subseteq I$, we have that $AI \subseteq IA$, because for any $j \geq 0$, $b \in R$ and $f = \sum_{i=0}^{n} a_i x^i \in I \subseteq R$ we have that

$$bx^j f = b\varphi^j(f)x^j \in IA,$$

since $\varphi^j(f) \in I$ and I is an ideal of R. For the ideals $U = AIA$ and $V = AJA$ of A, the following holds:

$$VU = AJAIA \subseteq AIJA = 0.$$

Since we assumed A to be a prime ring, and since $U \neq 0$ as $0 \neq I \subseteq U$, we conclude that $V = 0$ and therefore $J = 0$. Hence R is a φ-prime ring. ■

Theorem 1.40. Let R be a commutative ring and $\varphi : R \to R$ an endomorphism. If P is a prime ideal of $A = R[x,\varphi]$ not containing x, then $P \cap R$ is a φ-prime ideal of R.

Proof. We will in the proof denote $P \cap R$ by B. The proof has three parts. Parts (i) and (ii) show that B is φ-invariant and together with (iii) this shows that B is φ-prime.

(i) **We will show that $\varphi(B) \subseteq B$.**

Take $b \in B$. Notice that $xb = \varphi(b)x \in P$. For any $f = \sum_{i=0}^{m} a_i x^i \in A$, we have that

$$\varphi(b)fx = \varphi(b)\sum_{i=0}^{m} a_i x^i x = \sum_{i=0}^{m} a_i \varphi(b) x x^i \in P$$

since $\varphi(b)x \in P$. Because f was arbitrary, we have that $\varphi(b)Ax \in P$. Now, P is a prime ideal, so either $x \in P$ or $\varphi(b) \in P$. The former is false by hypothesis, so $\varphi(b) \in P$. Since b was arbitrary, we conclude that $\varphi(B) \subseteq P$. Now, we know that $\varphi(I) \subseteq R$ for any ideal I of R, so we have in fact that $\varphi(B) \subseteq P \cap R = B$.

(ii) **We will show that** $\varphi(r) \in B \implies r \in B$**.**

Suppose $\varphi(r) \in B$ for some $r \in R$. Then $\varphi(r)x = xr \in P$. Let $f \in A$. Then $f = a_0 + \sum_{i=1}^{m} a_i x^i$ and

$$xfr = x\left(a_0 + \sum_{i=1}^{m} a_i x^i\right) r = xa_0 r + x\sum_{i=1}^{m} a_i x^i r = xra_0 + x\sum_{i=1}^{m} a_i x^{i-1} xr \in P$$

because $xr = \varphi(r)x \in P$. Since f was arbitrary, we have that $xAr \in P$. But P is prime and $x \notin P$, so $r \in P$. Since $r \in R$ we have that $r \in B$.

(iii) **We will show that** $JI \subseteq B, \varphi(I) \subseteq I \implies I \subseteq B$ **or** $J \subseteq B$**.**

Let I, J be any two ideals of R such that $JI \subseteq B$ and $\varphi(I) \subseteq I$. Then $xI = \varphi(I)x \subseteq Ix$. By induction, it follows that $x^i I \subseteq Ix^i$ for $i \geq 0$. Let $f \in A$. Then

$$JfI = J\left(\sum_{i=0}^{m} a_i x^i\right) I = \sum_{i=0}^{m} Ja_i x^i I \subseteq \sum_{i=0}^{m} JIa_i x^i = JIf.$$

Hence

$$JAI \subseteq JIA \subseteq BA \subseteq PA \subseteq P.$$

Since P is prime, either $I \subseteq P$ or $J \subseteq P$ and hence, because $I, J \subseteq R$, we have that $I \subseteq B$ or $J \subseteq B$.

■

Theorem 1.41. Let $A = R[x, \varphi]$ for a commutative φ-prime ring R and suppose $\varphi : R \to R$ is not an automorphism of finite order. If P is a prime ideal of A, then either

(i) $P = 0$,

(ii) $x \in P$, or

(iii) $P \cap R \neq 0$.

Proof. Assuming that $P \neq 0$ and that $x \notin P$, we want to show that $P \cap R \neq 0$. Let $B := P \cap R$. By Theorem 1.40, B is a φ-prime ideal. Since $P \neq 0$, we can choose a nonzero element $f \in P$ of the form $\sum_{i=0}^{m} a_i x^i$ for m minimal where $a_i \in R$ and $a_m \neq 0$. If $m = 0$, then $f = a_0$ is nonzero, and $f \in B$ since $a_0 \in R$. Hence $B \neq 0$.

Assume now that $m \geq 1$. Recall that R is a φ-prime ring. In particular, 0 is a φ-invariant ideal and hence φ is injective by Remark 1.36.

Assume for a moment that for all $b \in R$ there exist an $i < m$ such that $\varphi^i(b) = \varphi^m(b)$. Then $\varphi^i(b - \varphi^{m-i}(b)) = 0$ which implies that $b = \varphi^{m-i}(b)$ since φ is injective. It follows that $\varphi^{2(m-i)}(b) = \varphi^{m-i}(\varphi^{m-i}(b)) = \varphi^{m-i}(b) = b$. By induction,

$$\varphi^{m!}(b) = \varphi^{\frac{m!}{m-i}(m-i)}(b) = b.$$

Hence φ has finite order $n \leq m!$. Then $\varphi^n = id$ and $\varphi^{-1} = \varphi^{n-1}$. That is, φ is an automorphism. But φ is not an automorphism of finite order by hypothesis, so our assumption that for all $b \in R$ there exists an $i < m$ such that $\varphi^i(b) = \varphi^m(b)$ must be wrong. We can therefore conclude that there exist $b \in R$ such that $\varphi^i(b) \neq \varphi^m(b)$ for all $i < m$.

Since $f\varphi^j(b) - \varphi^{m+j}(b)f \in P$, we have that

$$\begin{aligned} f\varphi^j(b) - \varphi^{m+j}(b)f &= \sum_{i=0}^{m} a_i x^i \varphi^j(b) - \sum_{i=0}^{m} \varphi^{m+j}(b) a_i x^i \\ &= \sum_{i=0}^{m} \left(\varphi^{i+j}(b) - \varphi^{m+j}(b)\right) a_i x^i \\ &= a_m x^m \cdot 0 + \sum_{i=0}^{m-1} \left(\varphi^{i+j}(b) - \varphi^{m+j}(b)\right) a_i x^i \\ &= \sum_{i=0}^{m-1} \left(\varphi^{i+j}(b) - \varphi^{m+j}(b)\right) a_i x^i \in P. \end{aligned} \tag{1.5}$$

Since the degree of the polynomial in (1.5) is lower than the degree of f, whose degree is minimal, we must have that $\left(\varphi^{i+j}(b) - \varphi^{m+j}(b)\right) a_i = 0$ for all $0 \leq i \leq m$ and all j.

Assume there exists $i < m$ such that $a_i \neq 0$. We will se that this leads to a contradiction. $L := a_i R$ and $K := \sum_j \left(\varphi^{i+j}(b) - \varphi^{m+j}(b)\right) R$ are both left ideals in R. By the last paragraph we know that $LK = 0$. Also,

$$\varphi(K) = \sum_j \left(\varphi^{i+j+1}(b) - \varphi^{m+j+1}(b)\right) R \subseteq K,$$

so either $L = 0$ or $K = 0$ since R is a φ-prime ring. But $K \neq 0$ since $\varphi^i(b) \neq \varphi^m(b)$ for all $i < m$. Hence $L = 0$, that is, $a_i = 0$ for all $i < m$, a contradiction. Therefore that $f = a_m x^m$.

Let $g = \sum_{i=0}^{k} b_i x^i$ be any element of A. Then

$$a_m g x^m = a_m \sum_{i=0}^{k} b_i x^i x^m = \sum_{i=0}^{k} b_i a_m x^m x^i \in P$$

since $a_m x^m = f \in P$. Hence $a_m A x^m \in P$. But P is prime and $x \notin P$, so we have that $a_m \in P$. a_m. We conclude that $B = P \cap R \neq 0$. ■

Theorem 1.42. Let R be a domain and let $A = R[x, \varphi]$, where φ is an injective endomorphism. Then $\operatorname{rad}(A) = 0$.

Proof. Suppose $\operatorname{rad}(A) \neq 0$. Then there exists a nonzero element $s = \sum_{i=0}^{k} s_i x^i \in \operatorname{rad}(A)$ with $s_k \neq 0$. By Lemma 1.27, $1 - s_k s$ has a left inverse $r = \sum_{j=0}^{m} r_j x^j \in A$, where $r_m \neq 0$. Hence

$$1 = r(1 - s_k s) = \sum_{j=0}^{m} r_j x^j - \sum_{j=0}^{m} r_j x^j s_k \sum_{i=0}^{k} s_i x^i.$$

If $k > 0$, the term of degree $m + k$ is zero, that is

$$r_m x^m s_k^2 x^k = r_m \varphi^m \left(s_k^2\right) x^{m+k} = 0.$$

Hence $r_m \varphi^m \left(s_k^2\right) = 0$. Since R is a domain and $r_m \neq 0$, we conclude that $\varphi^m \left(s_k^2\right) = 0$. But as φ is injective $s_k^2 = 0$ and therefore $s_k = 0$ as R is a domain, contradicting that $s_k \neq 0$. Thus $k = 0$ and $s = s_0 \in \operatorname{rad}(A) \cap R$. Since s was an arbitrary nonzero element of $\operatorname{rad}(A)$, we conclude that $\operatorname{rad}(A) \subseteq R$. It follows that

$$\operatorname{rad}(A)x \subseteq R \cap Ax = 0$$

because nonzero elements in Ax have degree at least 1 while nonzero elements in R have degree 0. We conclude that $\operatorname{rad}(A) = 0$. ∎

Chapter 2

Right primitivity of skew polynomial rings

In this chapter we describe the conditions for A to be right primitive according to the degree of $\varphi(y) \in K[y]$ and in chapter 3 we describe the conditions for A to be left primitive. We start with the case where $\varphi(y) \in K$.

2.1 Case: $\varphi(y) \in K$

In this section we will show that $A = K[y][x, \varphi]$ with $\varphi(y) \in K$ is neither right nor left primitive. As it turns out, all we need to do is to prove that φ is not injective. We therefore establish Lemma 2.1.

Lemma 2.1. Let $\varphi : K[y] \to K[y]$ be an endomorphism where K is a field. Then φ is injective if and only if $\deg(\varphi(y)) > 0$.

Proof. Assume that $\varphi(y) = a$ for some $a \in K$. Thus $xy = \varphi(y)x = ax = xa$, so $x(y - a) = 0$. Therefore $\varphi(y - a) = 0$, that is $y - a \in \ker(\varphi)$. Hence φ is not injective.

Conversely, assume that φ is not injective. Then $\ker(\varphi) = \langle g \rangle$ for some nonzero polynomial g of degree $d \geq 0$. If $d = 0$, then $\ker(\varphi) = K[y]$ so that $\varphi \equiv 0$. In particular, $\varphi(1) = 0 \neq 1$, a contradiction. Hence $d \geq 1$. Let now $g = \sum_{i=0}^{d} a_i y^i$ with $a_d \neq 0$. Since $g \in \ker(\varphi)$ we have that

$$0 = \varphi(g) = \sum_{i=0}^{d} a_i \varphi(y)^i,$$

so that

$$-a_0 = \left(\sum_{i=1}^{d} a_i \varphi(y)^{i-1} \right) \varphi(y).$$

Assume that $\deg(\varphi(y)) = D \geq 1$. Then the term of highest degree in $\sum_{i=1}^{d} a_i \varphi(y)^{i-1}$ is $a_d y^{(d-1)D}$, and this term is nonzero since $a_d \neq 0$. Hence $\sum_{i=1}^{d} a_i \varphi(y)^{i-1} \neq 0$. Therefore, $\deg(\varphi(y)) = D \geq 1$ and it follows that $\deg(a_0) \geq 1$, a contradiction. Therefore $D = 0$ and hence $\varphi(y) \in K$. ■

We now have the tools we need to analyse the case where $\varphi(y) \in K$.

Corollary 2.2. Let $A = K[y][x, \varphi]$ for a field K and an endomorphism $\varphi : K[y] \to K[y]$ such that $\varphi(y) \in K$. Then A is neither left nor right primitive.

Proof. By Lemma 2.1, φ is not injective. Thus, by Theorem 1.39, A is not a prime ring, that is, the zero-ideal of A is not prime. Since primitive ideals are prime, the zero-ideal of A is not primitive either. Hence A is neither right nor left primitive. ■

2.2 Case: $\varphi(y) = ay + b$

We will now consider the case when $\deg(\varphi(y)) = 1$, that is, $\varphi(y) = ay + b$ for some $a, b \in K$ with a nonzero. We divide our problem into four cases:

2.2.1: a is not a root of unity,

2.2.2: a is a root of unity but $a \neq 1$,

2.2.3: $\varphi = \mathrm{id}$ is the identity, and

2.2.4: $a = 1$ and $b \neq 0$.

Before we can continue, we need the following lemma:

Lemma 2.3. Let $\widehat{y} = dy + c$ for some $c \in K$ and some $0 \neq d \in K$. Then $K[\widehat{y}] = K[y]$ and the powers of $\widehat{y}$ are algebraically independent.

Proof. Assume

$$a_0 + a_1 \widehat{y} + a_2 \widehat{y}^2 + \cdots + a_n \widehat{y}^n = 0$$

for some $a_i \in K$. Then

$$a_0 + a_1(dy + c) + a_2(dy + c)^2 + \cdots + a_n(dy + c)^n = 0 \tag{2.1}$$

for some $c, d \in K$ with d nonzero. The highest degree term in y of the left side of (2.1) must be 0, that is, $a_n d^n = 0$. Since $d \neq 0$ we must have that $a_n = 0$, so that (2.1) is reduced to

$$a_0 + a_1(dy + c) + a_2(dy + c)^2 + \cdots + a_{n-1}(dy + c)^{n-1} = 0.$$

By repeating the same argument, we see that $a_{n-1} = 0$, and by continuing in the same manner we conclude that $a_i = 0$ for all $0 \leq i \leq n$. This shows that the powers of $\widehat{y}$ are algebraically independent.

Clearly $K[\widehat{y}] \subseteq K[y]$. Let $\sum_{i=0}^{n} a_i y^i \in K[y]$. We want to find b_i for $0 \leq i \leq n$ such that $\sum_{i=0}^{n} b_i (\widehat{y})^i = \sum_{i=0}^{n} a_i y^i$. Since

$$\sum_{i=0}^{n} b_i (\widehat{y})^i = \sum_{j=0}^{n} \sum_{i=j}^{n} b_i \binom{i}{j} c^{i-j} d^j y^j = \sum_{i=0}^{n} \left(\sum_{j=i}^{n} \binom{j}{i} b_j c^{j-i} d^i \right) y^j,$$

we need to find b_i for $0 \leq i \leq n$ such that

$$a_i = \sum_{j=i}^{n} \binom{j}{i} b_j c^{j-i} d^i \tag{2.2}$$

for all $0 \leq i \leq n$. The solution is $b_n = d^{-n} a_n$ and, if for some $i \geq 1$ we have that $b_n, \ldots, b_{n-i+1}$ has been defined, then

$$b_{n-i} = d^{i-n} a_{n-i} - \sum_{j=n-i+1}^{n} \binom{j}{n-i} b_j c^{j-n+i}.$$

We will prove this by induction. Since we need

$$a_n = \sum_{j=n}^{n} \binom{j}{n} b_j c^{j-n} d^n = \binom{n}{n} b_n c^{n-n} d^n = b_n d^n,$$

we see that $b_n = d^{-n} a_n$. Furthermore, we need to show that

$$b_{n-i-1} = d^{-n+i+1} a_{n-i-1} - \sum_{j=n-i}^{n} \binom{j}{n-i-1} b_j c^{j-n+i+1}.$$

Using that the conditions in (2.2) must be satisfied, we have that

$$\begin{aligned} a_{n-i-1} &= \sum_{j=n-i-1}^{n} \binom{j}{n-i-1} b_j c^{j-n+i+1} d^{n-i-1} \\ &= \binom{n-i-1}{n-i-1} b_{n-i-1} c^{n-i-1-n+i+1} d^{n-i-1} + \sum_{j=n-i}^{n} \binom{j}{n-i-1} b_j c^{j-n+i+1} d^{n-i-1} \\ &= b_{n-i-1} d^{n-i-1} + \sum_{j=n-i}^{n} \binom{j}{n-i-1} b_j c^{j-n+i+1} d^{n-i-1}. \end{aligned}$$

Hence

$$b_{n-i-1} = d^{-n+i+1}a_{n-i-1} - \sum_{j=n-i}^{n} \binom{j}{n-i-1} b_j c^{j-n+i+1}.$$

This proves the inductive part and we therefore have that $K[y] \subseteq K[\widehat{y}]$. We conclude that $K[\widehat{y}] = K[y]$. ■

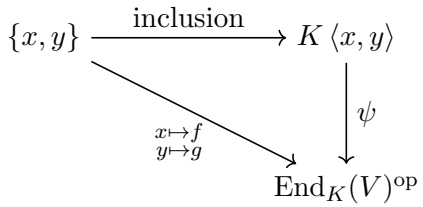
In the first two cases (2.2.1 and 2.2.2), we have that $a \neq 1$. Hence, by Lemma 2.3, we can substitute y with $\widehat{y}$ where $\widehat{y} := y - \frac{b}{1-a}$. Then

$$\begin{aligned}\varphi(\widehat{y}) &= \varphi\left(y - \frac{b}{1-a}\right) = ay + b - \frac{b}{1-a} \\ &= ay + \frac{b - ba - b}{1-a} = ay - a\frac{b}{1-a} = a\left(y - \frac{b}{1-a}\right) = a\widehat{y}.\end{aligned}$$

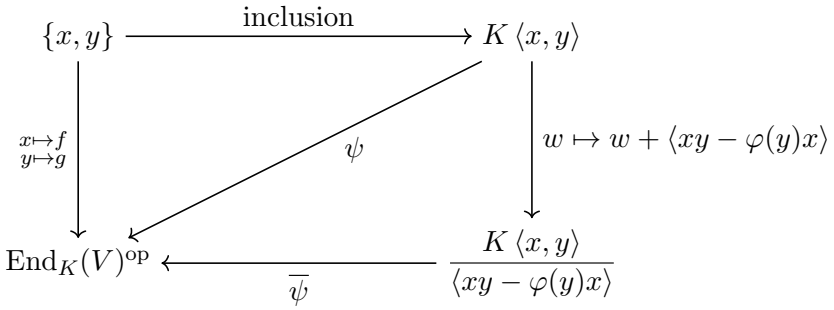
Since $K[\widehat{y}] = K[y]$ by Lemma 2.3, we conclude that we can assume that $b = 0$ in cases 2.2.1 and 2.2.2.

In sections 2.2.1, 2.2.2 and 2.3, we will prove the right primitivity of A by constructing certain right A-modules. We will therefore in the following describe the conditions for a vector space V to be a right A-module.

As seen in the preliminaries, a K-vector space V can be made into a left A-module for any ring homomorphism from A to $\mathrm{End}_K(V)$. Analogously any ring homomorphism from A to the opposite ring $\mathrm{End}_K(V)^{\mathrm{op}}$ defines a right A-module structure on V. Let $f, g \in \mathrm{End}_K(v)$ and let $x \mapsto f$ and $y \mapsto g$ be actions of the set $\{x, y\}$ on elements in V. Then, by the universal property of $K\langle x, y\rangle$, there exist a ring homomorphism $\psi : K\langle x, y\rangle \to \mathrm{End}_K(V)^{\mathrm{op}}$ such that the following diagram commutes:



Hence, by the first isomorphism theorem, there exists a ring homomorphism $\overline{\psi}$ from $\frac{K\langle x,y\rangle}{\langle xy - \varphi(y)x\rangle}$ to $\mathrm{End}_K(V)^{\mathrm{op}}$ such that the following diagram commutes if and only if $\psi(xy - \varphi(y)x) = 0$:



To prove Lemma 2.4, it remains to show that

$$K[y][x,\varphi] \simeq \frac{K\langle x,y\rangle}{\langle xy-\varphi(y)x\rangle}.$$

We will shortly explain why the last isomorphism holds: Suppose φ is an endomorphism of $K[y]$ and let $K\langle a,b\rangle$ denote the free algebra in a and b. We can identify $K[y]$ and $K[b]$ so that it makes sense to write $\varphi(b)$. Let $T = \frac{K\langle a,b\rangle}{\langle ab-\varphi(b)a\rangle}$ and set $\overline{a} = a + \langle ab-\varphi(b)a\rangle$ and $\overline{b} = b + \langle ab-\varphi(b)a\rangle \in T$. By the universal property of the free algebra $K\langle a,b\rangle$ there exists a unique ring homomorphism $\Phi : T \to K[y][x,\varphi]$ with $\Phi(\overline{a}) = x$ and $\Phi(\overline{b}) = y$. One the other hand, we can define a K-linear map $\Theta : K[y][x,\varphi] \to T$ defined on the basis elements by $\Theta(y^i x^j) = \overline{b}^i \overline{a}^j$, which can be shown to be a ring homomorphism as $\Theta(xy-\varphi(y)x) = \overline{ab-\varphi(b)a} = \overline{0}$. Then Θ and Φ are mutual inverses, showing that $T \simeq K[y][x,\varphi]$. We have proved Lemma 2.4.

Lemma 2.4. A K-vector space V is a right A-module if and only if there exist $f, g \in \mathrm{End}_K(V)^{\mathrm{op}}$ where $f(v) := v \cdot x$ and $g(v) := v \cdot y$ such that

$$(v \cdot x) \cdot y - (v \cdot \varphi(y)) \cdot x = 0$$

for all $v \in V$.

2.2.1 Case: a is not a root of unity

We now consider the case where $\varphi(y) = ay + b$ and a is not a root of unity. In particular, $a \neq 1$, so we can assume that $b = 0$ as explained in the introduction to section 2.2. Thus $xy = \varphi(y)x = ayx$. In this case, $A = K[y][x,\varphi]$ is called the "quantum-plane" [7, p. 72].

We will show that A is right primitive by introducing a faithful simple right A-module

V. Let V be a K-vector space with basis $\{v_i : i \in \mathbb{Z}\}$ and define the following map:

$$\begin{aligned} \{x, y\} &\to \mathrm{End}_K(V) \\ x &\mapsto [v_i \mapsto v_{i+1}] \\ y &\mapsto \left[v_i \mapsto a^i v_{i-1}\right]. \end{aligned}$$

Since

$$(v_i \cdot x) \cdot y - (v_i \cdot ay) \cdot x = v_{i+1} \cdot y - a^{i+1} v_{i-1} \cdot x = a^{i+1} v_i - a^{i+1} v_i = 0,$$

we see that $(v \cdot x) \cdot y = (v \cdot \varphi(y)) \cdot x$ for all $v \in V$. By the universal property of $K\langle x, y\rangle$ and the above, we conclude that V is a right A-module by Lemma 2.4.

Before we can prove that V is simple, we need the following lemma.

Lemma 2.5. Let V be the right A-module just defined. Then, for all $n \geq 1$ there exist $c_n \in \mathbb{N}$ such that $v_{-n} = a^{c_n} v_0 y^n$.

Proof. We will give a proof by induction. The base case is easy. Since $v_0 y = v_{-1} = a^0 v_{-1}$ we have that $v_{-1} = a^0 v_0 y$, that is, $c_1 = 0 \in \mathbb{N}$. Assume now that $n \geq 1$ and that there exists c_n such that $v_{-n} = a^{c_n} v_0 y^n$. Then $v_0 y^n = a^{-c_n} v_{-n}$ and hence

$$v_0 y^{n+1} = v_0 y^n y = a^{-c_n} v_{-n} y = a^{-c_n - n} v_{-n-1}.$$

Thus $v_{-n-1} = a^{-c_n - n} v_0 y^{n+1}$ and hence $c_{n+1} = c_n + n \in \mathbb{N}$. This completes the proof. ∎

We will now show that V is simple. By Lemma 1.4 (i), it suffices to show that $wA = V$ for all nonzero $w \in V$. Furthermore, it is enough to show that $v_0 \in wA$ because we claim that $wA = V \iff v_0 \in Aw$. To prove the claim, assume that $wA = V$. Then $v_0 \in V = wA$. Conversely, assume $v_0 \in wA$. Then $v_i = v_0 x^i \in wA$ for all $i \geq 0$ and, by Lemma 2.5, $v_{-i} = a^{d_i} v_0 y^i \in wA$ for some $d_i \in \mathbb{N}$ and all $i \geq 1$. It follows that $V \subseteq wA$, but $wA \subseteq V$ so in fact $wA = V$. This proves the claim.

We now want to prove that for any nonzero $w \in V$ there exist $f \in A$ such that $w \cdot f = v_0$, because then $v_0 \in wA$ and hence V is simple. Since $w = \sum_{i \in \mathbb{Z}} v_i k_i$ with only a finite number of the k_i's being nonzero, we know that

$$w = \sum_{i=m}^{n} v_i k_i$$

for some $m, n \in \mathbb{Z}$ with $m \leq n$, $k_m \neq 0$ and $k_n \neq 0$. Either $m \leq 0$ or $m > 0$. In the case $m \leq 0$, observe that

$$w \cdot x^{|m|} = \sum_{i=m}^{n} v_i k_i \cdot x^{|m|} = \sum_{i=m}^{n} v_{i+|m|} k_i = \sum_{i=0}^{n+|m|} v_i k_{i-|m|}.$$

In the case $m > 0$, observe that

$$w \cdot y^m = \sum_{i=m}^{n} v_i k_i \cdot y^m = \sum_{i=m}^{n} v_{i-m} k_i a^{d_i} = \sum_{i=0}^{n-m} v_i k_{i+m} a^{d_{i+m}},$$

for some $d_i \in \mathbb{N}$ depending on i for $m \leq i \leq n$. It follows that the set

$$\Omega := \{l \in \mathbb{N} : \text{ there exists } \sum_{i=0}^{l} v_i b_i \in wA \text{ with } b_i \in K, b_0 \neq 0 \text{ and } b_l \neq 0\}$$

is nonempty.

Since $\Omega \subseteq \mathbb{N}$ is a well ordered nonempty set, there exists an element

$$u = \sum_{i=0}^{l} v_i b_i \in Aw$$

with l minimal, and where $k_i \in K$, $b_0 \neq 0$ and $b_l \neq 0$. However,

$$\begin{aligned} u \cdot (1 - yx)y &= \left(u - \sum_{i=0}^{l} b_i v_i \cdot yx\right) y = \left(u - \sum_{i=0}^{l} b_i a^i v_{i-1} \cdot x\right) y = \left(u - \sum_{i=0}^{l} b_i a^i v_i\right) y \\ &= \left(\sum_{i=0}^{l} b_i \left(1 - a^i\right) v_i\right) y = \sum_{i=1}^{l} b_i \left(1 - a^i\right) v_i \cdot y = \sum_{i=1}^{l} b_i \left(1 - a^i\right) a^i v_{i-1} \\ &= \sum_{i=0}^{l-1} b_{i+1} \left(1 - a^{i+1}\right) a^{i+1} v_i, \end{aligned}$$

so since l is minimal, we have that $b_i \left(1 - a^i\right) a^i = 0$ for all $1 \leq i \leq l$. Since the degree of $\varphi(y)$ is 1 we know that $a^i \neq 0$. Also, $a^i \neq 1$ since a is not a root of unity. Hence $b_i = 0$ for $1 \leq i \leq l$. In particular, $b_l = 0$ if $l \geq 1$. This is a contradiction, so we conclude that $l = 0$. Therefore $u = v_0 b_0$ so that $v_0 = u b_0^{-1} \in wA$. We conclude that V is simple.

It remains to show that V is faithful. Let $P := \operatorname{ann}_A(V) = \{a \in A : v_i \cdot a = 0 \text{ for all } i\}$. Since V is simple, P is primitive and hence P is a prime ideal. Also, R is a φ-prime ring by Lemma 1.37. We can therefore use Theorem 1.41 to show that $P = 0$. Because $v_i \cdot x = v_{i+1} \neq 0$, we have that $x \notin P$. Let now $g = \sum_{i=0}^{m} b_i y^i \in P \cap K[y]$. Then

$$v_i \cdot g = \sum_{j=0}^{m} b_j v_i \cdot y^j = \sum_{j=0}^{m} b_j a^{d_j} v_{i-j} = 0$$

for some $d_j \in \mathbb{N}$ depending on j for $0 \leq j \leq m$ and where we have used the fact that $g \in P$. But all the v_i's are linearly independent, so $b_j a^{d_j} = 0$ for all $0 \leq j \leq m$. Now, a^{d_j} is nonzero,

so b_j must be 0 for all j. Hence $g = 0$. Since g was arbitrary, it follows that $P \cap K[y] = 0$. We conclude by Theorem 1.41 that $P = 0$, that is, V is a faithful module. We have proved Theorem 2.6:

Theorem 2.6. Let $A = K[y][x, \varphi]$ for an endomorphism $\varphi : K[y] \to K[y]$ such that $\varphi(y) = ay + b$ for some $a, b \in K$ where a is not a root of unity. Then A is right primitive.

2.2.2 Case: a is a root of unity but $a \neq 1$

The main result in this section is Theorem 2.9 that says that if $A = R[x, \varphi]$ where R is a commutative domain and φ is an automorphism of finite order, then A is not right nor left primitive. As we will see in Corollary 2.10, this applies to the case where $\varphi(y) = ay + b$ for some root of unity a where $a \neq 1$. First, we need the following two results.

Proposition 2.7. Let K be a field and $\varphi : K \to K$ be an automorphism. Let $F = \{z \in K : \varphi(z) = z\}$. Then F is a subfield of K.

Proof. Since $\varphi(1) = 1$, we have that $1 \in F$. Let $a, b \in F$. Then $a - b \in F$ because $\varphi(a - b) = \varphi(a) - \varphi(b) = a + b$ and $ab \in F$ because $\varphi(ab) = \varphi(a)\varphi(b) = ab$. Now, observe that $\varphi(a)^{-1} = \varphi\left(a^{-1}\right)$ because

$$1 = \varphi(1) = \varphi\left(aa^{-1}\right) = \varphi(a)\varphi\left(a^{-1}\right).$$

Therefore, $\varphi\left(a^{-1}\right) = \varphi(a)^{-1} = a^{-1}$ which implies that $a^{-1} \in F$. We conclude that F is a subfield of K. ■

The field in Proposition 2.7 is called the **fixed field** of φ and is sometimes denoted K^G for $G = \langle\varphi\rangle$, the subgroup generated by φ. The following theorem is taken from [13, p. 78].

Theorem 2.8. If G is a subgroup of $\mathrm{Aut}(K)$ for a field K, then

$$\left[K : K^G\right] = |G|.$$

Theorem 2.9. Let $A = R[x, \varphi]$ where R is a commutative domain and φ is an automorphism of finite order. Then A is not right nor left primitive.

Proof. Let $H = \{ab^{-1} : a, b \in R, b \neq 0\}$ be the fraction field of R. The endomorphism φ extends to H be defining $\varphi(ab^{-1}) := \varphi(a)\varphi(b)^{-1}$. This is well defined since φ is injective and hence $b \neq 0 \implies \varphi(b) \neq 0$. The subset $F := \{z \in H : \varphi(z) = z\}$ is a subfield of H by Proposition 2.7. Since φ is of finite order, there exists a least $n \geq 1$ such that $\varphi^n = \mathrm{id}$. This implies that $\varphi^{-1} = \varphi^{n-1}$. Let $G = \{\mathrm{id}, \varphi, \varphi^2, \ldots, \varphi^{n-1}\}$. Since G has order n, it follows from Theorem 2.8 that the dimension of H over F is

$$[H : F] = \left[H : H^G\right] = |G| = n.$$

Hence, there exists a basis $\{z_1, z_2, \ldots, z_n\}$ of H as an F-vector space.

Observe that

$$x^n z = x^{n-1}\varphi(z)x = x^{n-2}\varphi^2(z)x^2 = \cdots = \varphi^n(z)x^n = zx^n$$

for all $z \in H$, that is, x^n commutes with every element of H. Furthermore, if $a \in F$, then $xa = \varphi(a)x = ax$, so x commutes with all elements of F. It follows that $F[x^n]$ is central in $H[x, \varphi]$, and since F is a subring of H, we have that $F[x^n]$ is a subring of the center of $H[x, \varphi]$.

$H[x, \varphi]$ is generated as a $F[x^n]$-module by $\{z_i x^j : 1 \leq i \leq n, \quad 0 \leq j \leq n-1\}$. To see this, observe that, for all $z \in H$, there exists $b_1, b_2, \ldots, b_n \in F$ such that $z = b_1 z_1 + b_2 z_2 + \cdots + b_n z_n$. Furthermore, for all $m \geq 0$, $m = qn + k$ where $0 \leq k \leq n-1$, we have

$$zx^m = zx^{qn+k} = (x^n)^q \, zx^k = \sum_{i=1}^{n} b_i \, (x^n)^q \, z_i x^k.$$

Since $b_j \, (x^n)^q \in F[x^n]$, it follows that $zx^m \in \sum_{i=0}^{n-1} \sum_{j=1}^{n} F[x^n] z_j x^i$. But since z and m were arbitrary, we have that

$$H[x, \varphi] = \sum_{i=0}^{n-1} \sum_{j=1}^{n} F[x^n] z_j x^i,$$

that is, $H[x, \varphi]$ is a finitely generated module over the central subring $F[x^n]$. We conclude that $H[x, \varphi]$ is a PI-ring by Lemma 1.20. In particular, the subring $A = R[x, \varphi]$ is a PI-ring as well.

We will now show that A is not simple because $Ax^nA = x^nA$ is a nonzero proper ideal of A. The ideal x^nA is nonzero because $0 \neq x^n \in x^nA$. To see that x^nA is a proper submodule of A, assume otherwise. Then there would exist $a \in A$ such that $x^n a = 1$. Hence x^n, and thus x, is invertible in A. This is impossible because the invertible elements have degree 0.

We have shown that A is a non-simple PI-ring and a finite dimensional algebra over it center. We therefore conclude that A is neither right nor left primitive by Theorem 1.19. ∎

Corollary 2.10. Let $A = K[y][x, \varphi]$ where $\varphi(y) = ay + b$ for some $a, b \in K$ and a is a root of unity but $a \neq 1$. Then A is neither right nor left primitive.

Proof. We proved in the introduction to section 2.2 that we can assume that $b = 0$. Hence $\varphi(y) = ay$. Since a is a root of unity, there exists $N \in \mathbb{N}$ such that $a^N = 1$. Thus $\varphi^N(y) = a^N y = y$, that is, $\varphi^N = \mathrm{id}$ and we conclude that φ is of finite order. We can therefore apply Theorem 2.9. ■

2.2.3 Case: $\varphi = \mathrm{id}$ is the identity

If $\varphi(y) = y$ then $xy = yx$, so the skew polynomial ring $A = K[y][x, \varphi]$ is the same as the commutative polynomial ring $K[x, y]$. Now, since $\langle x \rangle$ is a proper nonzero ideal of $A = K[x, y]$, A is not a field and hence, by Lemma 1.16, A is neither left nor right primitive. We have proved Theorem 2.11:

Theorem 2.11. Let $A = K[y][x] = K[x, y]$. Then A is neither right nor left primitive.

2.2.4 Case: $a = 1$ and $b \neq 0$

Theorem 2.12. Let $A = K[y][x, \varphi]$ where φ is determined by $\varphi(y) = y + b$ for some $0 \neq b \in K$ and K is a field of characteristic 0. Then A is right primitive.

Proof. With $\varphi(y) = y + b$, we have that $xy = \varphi(y)x = (y + b)x$. We will make a shift of variable by defining $\widehat{y} = \frac{1}{b}y$. Then

$$x\widehat{y} = \frac{1}{b}xy = \frac{1}{b}(y + b)x = \left(\frac{1}{b}y + 1\right)x = (\widehat{y} + 1)\,x = \widehat{\varphi}(\widehat{y})x,$$

where $\widehat{\varphi}(\widehat{y}) = \widehat{y} + 1$. Since, by Lemma 2.3, $K[y] = K\left[\frac{1}{b}y\right]$ for all $0 \neq b \in K$, we can assume that $b = 1$.

With $\varphi(y) = y + 1$, we have the relation $xy = (y + 1)x$, or equivalently, $yx = x(y - 1)$. We want to find a simple, faithful A-module on the vector space V with basis $\{v_n : n \geq 0\}$. The action of V, and the proof of it's simplicity, is taken from [11, pp. 9-10]. The action is defined as

$$v_n \cdot y = v_{n+1} \text{ for all } n \geq 0; \text{ and}$$
$$v_n \cdot x = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} v_k.$$

By Lemma 2.4, V is a right A-module if we can prove that $v_n \cdot (yx - x(y-1)) = 0$ for all $n \geq 0$. We will give a proof by induction on n. The base case $n = 0$ is easy:

$$v_0 \cdot (yx - x(y-1)) = v_1 \cdot x - v_0 \cdot (y-1) = -v_0 + v_1 - v_1 + v_0 = 0.$$

Assume that $n \geq 1$ and $v_m \cdot (yx - x(y-1)) = 0$ for all $m \leq n$. Recall that $v_{n+1} = v_n \cdot y$ and that $yx = x(y-1)$. Hence

$$\begin{aligned} v_{n+1} \cdot (yx - x(y-1)) &= v_n \cdot y\,(yx - x(y-1)) = v_n \cdot \left(y^2 x - yx(y-1)\right) \\ &= v_n \cdot (yx(y-1) - yx(y-1)(y-1)) = v_n \cdot (yx - yx(y-1))\,(y-1) \\ &= 0(y-1) = 0 \end{aligned}$$

This proves that $v_n \cdot (yx - x(y-1)) = 0$ for all $n \geq 0$ which implies that V is a right A-module.

To show that V is simple, we first show by induction that $v_n \cdot (1-x)^n = n! v_0$ for all $n \geq 0$. The base case $n = 0$ is trivial: $v_0 \cdot (1-x)^0 = v_0 1 = 0! v_0$.

Let $n \geq 0$ and assume $v_m \cdot (1-x)^m = m! v_0$ for all $m \leq n$. Then, for $l > n \geq m$, we have that

$$v_m \cdot (1-x)^l = m! v_0 \cdot (1-x)^{l-m} = 0 \tag{2.3}$$

because $v_0 \cdot (1-x) = v_0 - v_0 = 0$. Hence

$$\begin{aligned} v_{n+1} \cdot (1-x)^{n+1} &= (v_{n+1} - v_{n+1} \cdot x) \cdot (1-x)^n \\ &= \left(v_{n+1} - \sum_{k=0}^{n+1} (-1)^{n+1-k} \binom{n+1}{k} v_k \right) \cdot (1-x)^n \\ &= \left(v_{n+1} - v_{n+1} - (-1)^{n+1-n} \binom{n+1}{n} v_n - \sum_{k=0}^{n-1} (-1)^{n+1-k} \binom{n+1}{k} v_k \right) \cdot (1-x)^n \\ &= -(-1)^1 \frac{(n+1)!}{n!(n+1-n)!} v_n \cdot (1-x)^n - \sum_{k=0}^{n-1} (-1)^{n+1-k} \binom{n+1}{k} v_k \cdot (1-x)^n \\ &= \frac{(n+1)!}{n!1!} n! v_0 \qquad \text{by (2.3)} \\ &= (n+1)! v_0 \end{aligned}$$

This proves that $v_n \cdot (1-x)^n = n! v_0$ for all $n \geq 0$. Now, let $0 \neq w = \sum_{i=0}^{n} k_i v_i \in V$ be any nonzero element of V with $k_n \neq 0$. Then

$$w \cdot (1-x)^n = \sum_{i=0}^{n} k_i v_i \cdot (1-x)^n = k_n n! v_0,$$

by (2.3). Hence

$$v_0 = \frac{1}{k_n n!} w \cdot (1-x)^n \in wA,$$

that is, v_0 is an element in wA, where we have have used that we can divide by $n!$ because K is of characteristic 0. It follows that $v_m \in wA$ for all $m \geq 0$ because $v_m = v_0 \cdot y^m \in wA$. We conclude that $V = wA$ and hence V is a simple right A-module by Lemma 1.4.

It remains to show that V is faithful. Let $P := \operatorname{ann}_A(V) = \{a \in A : v_n \cdot a = 0 \text{ for all } n\}$. Since V is simple, P is primitive and hence a prime ideal. We can therefore use Theorem 1.41 to show that $P = 0$. Because $v_0 \cdot x = v_0 \neq 0$, we have that $x \notin P$. Let now $g = \sum_{i=0}^m a_i y^i \in P \cap K[y]$. Then

$$0 = v_0 \cdot g = \sum_{i=0}^m a_i v_0 \cdot y^i = \sum_{i=0}^m a_i v_i$$

since $g \in P$. But all the v_i's are linearly independent, so $a_i = 0$ for all $0 \leq i \leq m$. Hence $g = 0$. Since g was arbitrary, it follows that $P \cap K[y] = 0$. We conclude by Theorem 1.41 that $P = 0$, that is, V is a faithful right A-module. We have shown that A is right primitive. ■

2.3 Case: $\deg(\varphi(y)) > 1$

Theorem 2.13. Let $A = K[y][x, \varphi]$ for a field K and a K-linear endomorphism φ be such that $\varphi(y) = f(y) \in K[y]$ has degree $d > 1$. Then A is right primitive.

Proof. Let V be a K-vector space with basis $\{v_i : i \geq 1\}$. Define

$$v_i \cdot y = v_{i+1}$$

for all $i \geq 1$. Furthermore, define

$$v_n \cdot x = 0 \qquad \text{if } n < d$$

$$v_d \cdot x = v_1$$

where d is the degree of $f = \varphi(y) \in K[y]$. By Lemma 2.4, V is a right A-module if we can find an action $v_n \cdot x$ for $n > d$ such that $(v_i \cdot x) \cdot y = (v_i \cdot f(y)) \cdot x$ for all $i \geq 1$. Let $\varphi(y) = \sum_{i=0}^d a_i y^i$. Since $v_1 \cdot x = 0$ we have that $(v_1 \cdot x) \cdot y = 0$. On the other hand

$$(v_1 \cdot x) \cdot y = (v_1 \cdot f(y)) \cdot x = \left(v_1 \cdot \left(\sum_{i=0}^d a_i y^i \right) \right) \cdot x = \sum_{i=0}^d a_i v_{i+1} \cdot x = a_d v_{d+1} \cdot x + a_{d-1} v_1.$$

Hence $v_{d+1} \cdot x = -\frac{a_{d-1}}{a_d} v_1$. Assume now that $v_i \cdot x$ has been defined for all $i < n+d$ for some $n \geq 1$. Then

$$(v_n \cdot x) \cdot y = \left(\sum_{i=0}^{d} a_i v_n \cdot y^i \right) \cdot x = \sum_{i=0}^{d} a_i v_{n+i} \cdot x = a_d v_{n+d} \cdot x + \sum_{i=0}^{d-1} a_i v_{n+i} \cdot x.$$

We therefore define

$$v_{n+d} \cdot x = \frac{1}{a_d} \left((v_n \cdot x) \cdot y - \sum_{i=0}^{d-1} a_i v_{n+i} \cdot x \right). \tag{2.4}$$

It follows that if $n = qd + r$ for $0 < q$ and $0 \leq r < d$, then

$$v_n \cdot x = c_n v_q + w_n \tag{2.5}$$

for some nonzero scalar c_n and $w_n \in \operatorname{span}\{v_i : i < q\}$. We can prove this by induction in the following way. Assume that (2.5) holds for all v_k with $k \leq n + d - 1$. Then

$$\begin{aligned}
v_{n+d} \cdot x &= \frac{1}{a_d} \left((v_n \cdot x) \cdot y - \sum_{i=0}^{d-1} a_i v_{n+i} \cdot x \right) \\
&= \frac{1}{a_d} \left((c_n v_q + w_n) \cdot y - \sum_{i=0}^{d-r-1} a_i \left(c_{n+i} v_q + w_{n+i} \right) - \sum_{i=d-r}^{d-1} a_i \left(c_{n+i} v_{q+1} + w_{n+i} \right) \right) \\
&= \frac{1}{a_d} \left(c_n v_{q+1} + w_{n+1} - \sum_{i=0}^{d-r-1} a_i \left(c_{n+i} v_q + w_{n+i} \right) - \sum_{i=d-r}^{d-1} a_i \left(c_{n+i} v_{q+1} + w_{n+i} \right) \right) \\
&= c_{n+d} v_{q+1} + w_{n+d}
\end{aligned}$$

for $0 \neq c_{n+d} = \frac{c_n}{a_d} \in K$ and

$$w_{n+d} = \frac{1}{a_d} \left(w_{n+1} - \sum_{i=0}^{d-r-i} a_i \left(c_{n+i} v_q + w_{n+i} \right) - \sum_{i=d-r}^{d-1} a_i \left(c_{n+1} v_{q+1} + w_{n+i} \right) \right) \in \operatorname{span} \{ v_i : i < n + d \}.$$

Let $n = d^t$ for some $t > 0$. Then

$$\begin{aligned}
v_{d^t} \cdot x &= c_{d^t} v_{d^t - 1} + w_{d^t}, \\
v_{d^t} \cdot x^2 &= c_{d^t} c_{d^t - 1} v_{d^t - 2} + w_{d^t} \cdot x, \\
&\vdots \\
v_{d^t} \cdot x^t &= \left(\prod_{i=1}^{t} c_{d^i} \right) v_1,
\end{aligned} \tag{2.6}$$

by (2.5), where $\prod_{i=1}^{t} c_{d^i} \neq 0$.

To show that V is simple, we will show that any nonzero submodule of V equals V. Any nonzero submodule of V contains some nonzero $v \in V$, and there exists $m \in \mathbb{N}$ such that

$v = \sum_{i=1}^{m} \lambda_i v_i$ with $\lambda_m \neq 0$. Since $d > 1$, there exist $t \in \mathbb{N}$ such that $d^{t-1} \leq m < d^t$. Thus

$$v \cdot y^{d^t - m} = \sum_{i=1}^{m} \lambda_i v_{i+d^t-m} = \lambda_m v_{d^t} + (\text{lower indexed vectors}).$$

Using (2.5), we se that

$$v \cdot y^{d^t-m} \cdot x = \lambda_m c_{d^t} v_{d^{t-1}} + (\text{lower intexed vectors}).$$

Hence, using (2.6), we have that

$$\left(v \cdot y^{d^t-m}\right) \cdot x^t = cv_1$$

for some nonzero scalar c. It follows, for all $r \geq 1$, that we can write v_r in the following way:

$$v_r = \frac{1}{c} c v_r = \frac{1}{c} c v_1 \cdot y^{r-1} = \frac{1}{c}\left(\left(v \cdot y^{d^t-m}\right) \cdot x^t\right) \cdot y^{r-1}.$$

Thus $vA = V$ and hence V is simple.

It remains to show that V is faithful. Let $P := \operatorname{ann}_A(V) = \{a \in A : v_n \cdot a = 0 \text{ for all } n\}$. Since V is simple, P is primitive and hence a prime ideal. Also, R is a φ-prime ring by Lemma 1.37. We can therefore use Theorem 1.41 to show that $P = 0$. Because $v_d \cdot x = v_1 \neq 0$, we have that $x \notin P$. Let now $g = \sum_{i=0}^{m} \lambda_i y^i \in P \cap K[y]$. Then

$$0 = v_1 \cdot g = \sum_{i=0}^{m} \lambda_i v_1 \cdot y^i = \sum_{i=0}^{m} \lambda_i v_{i+1}$$

since $g \in P$. But all the v_i's are linearly independent, so $\lambda_i = 0$ for all $0 \leq i \leq m$. Hence $g = 0$. Since g was arbitrary, it follows that $P \cap K[y] = 0$. We conclude by Theorem 1.41 that $P = 0$, that is, V is a faithful module. We have shown that A is a right primitive ring.

■

Example 2.14. Let $A = K[y][x, \varphi]$ with $\varphi(y) = f(y)$ where $f(y) = y^2$. Since the degree d of $\varphi(y)$ is $2 > 1$, A is right primitive by Theorem 2.13. Let $V = \operatorname{span}\{v_i : i \geq 1\}$, $v_i \cdot y = v_{i+1}$, $v_1 \cdot x = 0$ and $v_2 \cdot x = v_1$. By (2.4), we have that

$$v_{n+2} \cdot x = \frac{1}{a_2}\left((v_n \cdot x) \cdot y - \sum_{i=0}^{1} a_i v_{n+i} \cdot x\right),$$

but since $f(y) = y^2$, we have that $a_0 = a_1 = 0$ and $a_2 = 1$, and therefore

$$v_{n+2} \cdot x = (v_n \cdot x) \cdot y.$$

It follows by induction that

$$v_{2n+1} \cdot x = 0$$

because $v_1 \cdot x = 0$ and if $v_{2n+1} \cdot x = 0$ has been shown, then $v_{2n+3} \cdot x = (v_{2n+1} \cdot x) \cdot y = 0$. It also follows that

$$v_{2n} \cdot x = v_n$$

because $v_2 \cdot x = v_1$ and if $v_{2n} \cdot x = v_n$ has been shown, then $v_{2n+2} \cdot x = (v_{2n} \cdot x) \cdot y = v_n \cdot y = v_{n+1}$.

2.4 Summary right primitivity

We sum up the results of this chapter in Theorem 2.15:

Theorem 2.15. Let $A = K[y][x, \varphi]$ for an endomorphism $\varphi : K[y] \to K[y]$. Then A is right primitive if and only if φ is injective but not an automorphism of finite order.

Proof. This follows from Corollary 2.2 and theorems 2.6, 2.9, 2.11, 2.12 and 2.13. ■

Chapter 3

Left primitivity of skew polynomial rings

We will now search for the conditions for $A = K[y][x, \varphi]$ to be left primitive. As seen in section 2.1, A is not left primitive when $\varphi(y) \in K$, or equivalently, φ is not injective by Lemma 2.1. Furthermore, in section 2.2.2 we proved that A is not left primitive when φ is of finite order. Therefore, we will in this chapter only consider skew polynomial rings where φ is injective and of infinite order. Our study is divided into three sections:

3.1 Case: There exists only finitely many φ-periodic primes;

3.2 Case: There are infinitely many φ-periodic primes and at least one of them is singular;

3.3 Case: There are infinitely many φ-periodic primes and none of them are singular.

We are primarily interested in the case where the coefficient ring R of our skew polynomial ring $A = R[x, \varphi]$ is $K[y]$, but we will also consider more general coefficient rings. This is because this thesis is largely based on Irving [5] and [6] where he works on Dedekind domains. In particular, this will affect some of our proofs. It will be helpful to keep in mind that the polynomial ring $K[y]$ is a principal ideal domain, every principal ideal domain is Dedekind and that every Dedekind domain is commutative and noetherian.

3.1 Case: There exists only finitely many φ-periodic primes

Let $A = R[x, \varphi]$ for a commutative noetherian domain R and an injective endomorphism φ of infinite order such that there are only finitely many φ-periodic primes in R. We will in

this section prove that A is left primitive. Before we can prove this, we need the following lemma.

Lemma 3.1. Let R be a domain and let I_i for $0 \leq i \leq n$ be a finite set of nonzero ideals in R. Then $\bigcap_{i=0}^{n} I_i \neq 0$.

Proof. Assume $\bigcap_{i=0}^{n} I_i = 0$. Since $\prod_{i=0}^{n} I_i \subseteq \bigcap_{i=0}^{n} I_i$, then $\prod_{i=0}^{n} I_i = 0$ as well. It follows that, given any nonzero $a_i \in I_i$ for $0 \leq i \leq n$, we have that $a_1 \cdots a_n = 0$. But in a domain, this implies that $a_i = 0$ for some i, a contradiction. Hence $\bigcap_{i=0}^{n} I_i \neq 0$. ■

Proposition 3.2. Let $A = R[x, \varphi]$ for a commutative noetherian domain R and an injective endomorphism φ of infinite order. Suppose that there are only finitely many φ-periodic primes in R. Then A is left primitive.

Proof. Let $P_1, P_2, \ldots, P_t$ be all the nonzero φ-periodic primes of R, let

$$B = P_1 \cap P_2 \cap \cdots \cap P_t,$$

and let I be any nonzero left primitive ideal of A. In particular, I is prime. Assume for a moment that $x \notin I$. Then $I \cap R$ is φ-prime by Theorem 1.40. Since R is a φ-prime ring by Lemma 1.37, $I \cap R$ is nonzero by Theorem 1.41 and hence, by Lemma 1.38 there exists a φ-periodic prime ideal P of R such that $I \cap R = P \cap \varphi^{-1}(P) \cap \cdots \cap \varphi^{-n+1}(P)$, where n is the period of P. Since $I \cap R \neq 0$, we have that $\varphi^{-i}(P) \neq 0$ for every $0 \leq i \leq n-1$. Furthermore, every $\varphi^{-i}(P)$ is φ-periodic, because $\varphi^{-n}\left(\varphi^{-i}(P)\right) = \varphi^{-i}\left(\varphi^{-n}(P)\right) = \varphi^{-i}(P)$. Thus $\varphi^{-i}(P) \in \{P_1, \ldots, P_t\}$ for all $0 \leq i \leq n$. We conclude that either $x \in I$ or $B \subseteq I \cap R$ for any nonzero left primitive ideal I of A.

Assume now that 0 is not a left primitive ideal of A, and let $\{I_\lambda : \lambda \in \Lambda\}$ be the set of left primitive ideals of A for some set Λ. Furthermore, let $a \in Bx$ be a nonzero element in Bx. Such an element exists since $B \neq 0$ by Proposition 3.1. Then there exists $b \in B$ such that $a = bx$. Hence $a \in I_\lambda$ for all I_λ containing x, and $a \in I_\lambda$ for all I_λ containing B. Since either $x \in I$ or $B \subseteq I$ for every nonzero primitive left ideal I, we have that $a \in I_\lambda$ for all $\lambda \in \Lambda$. We conclude that

$$Bx \subseteq \bigcap_{\lambda \in \Lambda} I_\lambda = \operatorname{rad}(A).$$

But, by Theorem 1.42, $\operatorname{rad}(A) = 0$, a contradiction since $0 \neq Bx$. Hence 0 is a left primitive ideal of A and thus A is a left primitive ring. ■

Example 3.3. Let $A = K[y][x, \varphi]$ where $\varphi(y) = f(y) = y - 1$. We will show that A is left primitive. Note that φ is injective because $\varphi(y) \notin K$. Furthermore, observe that $\varphi^n(y) = y - n$, so there is no $n \geq 1$ such that $\varphi^n = \mathrm{id}$ since the characteristic of K is 0. Hence φ is of infinite order. Every nonzero prime ideal $P \in K[y]$ is of the form $P = \langle y - a \rangle$ for $a \in K$, and P is φ-periodic if and only if there exists $n \geq 1$ and $a \in K$ such that $f^n(a) = a$. However $f^n(a) = a - n \neq a$, so there is no nonzero φ-periodic prime ideals in $K[y]$; the only φ-periodic prime ideal is the 0-ideal. We conclude by Proposition 3.2 that A is left primitive.

3.2 Case: There are infinitely many φ-periodic primes and at least one of them is singular

Let R be a Dedekind domain and let φ be an injective endomorphism of R. Assume for some φ-periodic prime ideal P of R that $\varphi^n(P) \subseteq P^t$ for some n and some $t > 1$. The aim of this chapter is to prove that $A = R[x; \varphi]$ is left primitive in this case. We need Lemma 3.4 before we can prove this result. Recall the P-order $\nu_P(I)$ from page 13.

Lemma 3.4. Let R be a Dedekind domain and let φ be an injective endomorphism of R. Let P be a φ-periodic prime of R with period n and suppose $\nu_P\left(\varphi^n(P)\right) = t > 1$. Then for any $r \in P$ such that $\nu_P\left(\varphi^n(r)\right) = t$, we have for any $i > 0$ that $\nu_P\left(\varphi^{in}(r)\right) = t^i$.

Proof. We will prove the lemma by induction on i. By hypothesis $\nu_P\left(\varphi^n(r)\right) = t$, so the base case $i = 1$ is clear. For the inductive step, assume $\nu_P(\varphi^{in}(r)) = t^i$ and write $\varphi^{in}(r)R = P^{t^i}U_1 \cdots U_k$ for primes $U_j \neq P$. Then

$$\varphi^{(i+1)n}(r)R = \varphi^n\left(\varphi^{in}(r)R\right)R = \varphi^n(P)^{t^i}\varphi^n\left(U_1\right)\cdots\varphi^n(U_k)R$$

because

$$U_j \neq P \implies U_j \subsetneq \varphi^{-n}(P) \implies \varphi^n(U_j) \subsetneq P \implies \nu_P\left(\varphi^n(U_j)\right) = 0.$$

Moreover, by hypothesis $\varphi^n(P)R = P^t Q_1 Q_2 \cdots Q_s$ for some prime ideals $Q_j \neq P$. Thus

$$\varphi^n(P)^{t^i}R = P^{t^{i+1}}Q_1^{t^i}\cdots Q_l^{t^i}$$

has P-order t^{i+1}. It follows that

$$\varphi^{(i+1)n}(r)R = P^{t^{i+1}}Q_1^{t^i}\cdots Q_l^{t^i}\varphi^n(U_1)\cdots\varphi^n(U_k)R,$$

and hence $\nu_P\left(\varphi^{(i+1)n}(r)R\right) = t^{i+1}$. ∎

Let P be a periodic singular prime of the ring $K[y]$, and let n be its period. If $r \in P\varphi^{-1}(P)\cdots\varphi^{-n+1}(P)$, then the ideal $I := Ap + A(1 - rx^n)$ is a proper ideal. Before we prove this in its generality, we will look at a couple of examples.

Example 3.5 (A φ-periodic singular prime of period 1)**.** Let $R = K[y]$ and φ the K-linear algebra homomorphism determined by $\varphi(y) = y^2$. Consider the skew polynomial ring $A = R[x;\varphi]$ subject to the relation

$$xy = \varphi(y)x = y^2x.$$

Let $P = \langle y\rangle$. Then $\varphi^{-1}(P) = P$, because $\varphi(y) = y^2 \in P$. Thus $P \subseteq \varphi^{-1}(P)$ and as P is maximal, $P = \varphi^{-1}(P)$.

We will now show that $I = Ay + A(1 - yx)$ is a proper left ideal of A. Suppose that I is not proper, that is, suppose $I = A$. We will show that this leads to a contradiction. Since $I = A$, there exist $a, b \in A$ such that $a = \sum_{i=0}^{n} a_i x^i$ and $b = \sum_{j=0}^{m} b_j x^j$ with $a_i, b_j \in K[y]$ and $a_n \neq 0 \neq b_m$ such that

$$1 = ay + b(1 + yx) = \sum_{i=0}^{n} a_i\varphi^i(y)x^i + \sum_{j=0}^{m} b_j x^j - \sum_{j=0}^{m} b_j\varphi^j(y)x^{j+1} \tag{3.1}$$

Since the left hand side has degree 0 in x, all coefficients of powers of x must be zero on the right hand side. In particular $n = m + 1$ as $b_m \neq 0$ and $a_n \neq 0$. We rewrite (3.1) as

$$1 = a_0y + b_0 + \sum_{i=1}^{n-1}\left(a_i\varphi^i(y) + b_i - b_{i-1}\varphi^{i-1}(y)\right)x^i + \left(a_n\varphi^n(y) - b_{n-1}\varphi^{n-1}(y)\right)x^n$$

leading to the system of equations:

$$\begin{aligned} b_0 &= 1 - a_0y \\ b_i &= b_{i-1}\varphi^{i-1}(y) - a_i\varphi^i(y), \quad \text{for all } 1 \leq i \leq n-1 \qquad (3.2)\\ b_{n-1}\varphi^{n-1}(y) &= a_n\varphi^n(y) \qquad (3.3)\end{aligned}$$

Now, from $\varphi(y) = y^2$ one deduces $\varphi^2(y) = y^4, \varphi^3(y) = y^8$ and more generally $\varphi^i(y) = y^{2^i}$. We claim that for all $1 \leq i \leq n-1$, we have that

$$b_i = y^{2^i-1}(1 - c_iy) \tag{3.4}$$

for some c_i. For $i = 1$ we have

$$b_1 = b_0\varphi^0(y) - a_1\varphi^1(y) = (1 - a_0y)y - a_1y^2 = y(1 - (a_0 + a_1)y)$$

Suppose (3.4) for some c_i. Then by (3.2)

$$b_{i+1} = b_i\varphi^i(y) - a_{i+1}\varphi^{i+1}(y) = y^{2^i-1}(1-c_iy)y^{2^i} - a_{i+1}y^{2^{i+1}} = y^{2^{i+1}-1}\left(1-(c_i+a_{i+1})y\right).$$

This proves the claim. However, (3.3) leads to a contradiction:

$$y^{2^n-1}(1-c_{n-1}y) = y^{2^{n-1}-1}(1-c_{n-1}y)y^{2^{n-1}} = b_{n-1}\varphi^{n-1}(y) = a_ny^{2^n},$$

because the right hand side is divisible by y^{2^n}, while the left hand side is only divisible by y^{2^n-1}. Therefore I is a proper left ideal.

Example 3.6 (A φ-periodic singular prime of period 2)**.** As before let $R = K[y]$ where K is a field of characteristic 0. Let φ be defined by $\varphi(y) = y^2 - 1$. Consider the skew polynomial ring $A = R[x;\varphi]$ subject to the relation

$$xy = \varphi(y)x = \left(y^2-1\right)x.$$

Let $P = \langle y\rangle$. Then $\varphi^{-1}(P) = \langle y+1\rangle$, because $\varphi(y+1) = y^2-1+1 = y^2 \in P$. Thus $\langle y+1\rangle \subseteq \varphi^{-1}(P)$ and as $\langle y+1\rangle$ is maximal, $\langle y+1\rangle = \varphi^{-1}(P)$. Furthermore, since $\varphi(y) = y^2-1 = (y-1)(y+1) \in \langle y+1\rangle$, we have that $y \in \varphi^{-1}\left(\langle y+1\rangle\right)$ and hence $P = \langle y\rangle \subseteq \varphi^{-1}\left(\langle y+1\rangle\right)$, but as $\langle y\rangle$ is maximal, we have that $P = \varphi^{-1}(\langle y+1\rangle)$. So P is a φ-periodic prime ideal of period 2 and

$$P = \langle y\rangle, \quad \varphi^{-1}(P) = \langle y+1\rangle \quad \text{and} \quad \varphi^{-2}(P) = P.$$

Since

$$\varphi^2(y) = \varphi(\varphi(y)) = \varphi\left(y^2-1\right) = \left(y^2-1\right)^2 - 1 = y^4 - 2y^2 + 1 - 1 = y^2\left(y^2-2\right) \subseteq \left\langle y^2\right\rangle \subseteq P^2,$$

we have that P is singular.

By Lemma 3.4, for all $i \geq 0$, we have that $\varphi^{2i}(y)$ is divisible by y^{2^i}, but not by y^{2^i+1}. Furthermore, $\varphi^{2i}(y+1)$ is not divisible by y, as otherwise $y+1 \in \varphi^{-2i}(P) = P = \langle y\rangle$, which is absurd, and $\varphi^{2i+1}(y+1)$ is not divisible by $y+1$ analogously. Then $I = Ay + A\left(1-y(y+1)x^2\right)$ is a proper left ideal of A because if we suppose $I = A$, then there exist $a = \sum_{i=0}^n a_ix^i, b = \sum_{j=0}^m b_jx^j \in A$, with $a_i, b_j \in K[y]$ and $a_n \neq 0 \neq b_m$ such that

$$1 = ay + b\left(1+y(y+1)x^2\right) = \sum_{i=0}^n a_i\varphi^i(y)x^i + \sum_{j=0}^m b_jx^j - \sum_{j=0}^m b_j\varphi^j(y(y+1))x^{j+2}.$$

Since the left hand side has degree 0 in x, all coefficients of x must be zero on the right hand side. In particular $n = m+2$ as $b_m \neq 0$ and $a_n \neq 0$. Rewriting the last equation as

$$1 = a_0y + b_0 + \left(a_1\varphi(y) + b_1\right)x + \sum_{i=2}^{n-2}\left(a_i\varphi^i(y) + b_i - b_{i-2}\varphi^{i-2}(y(y+1))\right)x^i$$
$$+ \left(a_{n-1}\varphi^{n-1}(y) - b_{n-3}\varphi^{n-3}(y(y+1))\right)x^{n-1} + \left(a_n\varphi^n(y) - b_{n-2}\varphi^{n-2}(y(y+1))\right)x^n$$

leads to the system of equations:

$$\begin{aligned} b_0 &= 1 - a_0 y \\ b_1 &= -a_1\varphi(y) = -a_1(y^2-1) \\ b_i &= b_{i-2}\varphi^{i-2}(y)\varphi^{i-2}(y+1) - a_i\varphi^i(y), \quad \text{for all } 1 \le i \le n-2 \end{aligned}$$

$$b_{n-3}\varphi^{n-3}(y(y+1)) = a_{n-1}\varphi^{n-1}(y) \tag{3.5}$$

$$b_{n-2}\varphi^{n-2}(y(y+1)) = a_n\varphi^n(y) \tag{3.6}$$

We claim that

Claim: b_{2i} is nonzero and divisible by y^{2^i-1} but not by y^{2^i} for $2i \le n-2$.

Proof of claim. For $i = 0$ we have $b_0 = 1 - a_0 y$ is not divisible by $y = y^{2^0}$, but by $1 = y^0 = y^{2^0-1}$. For $i = 1$ we had already noted that $\varphi^2(y) = y^2(y^2-2)$. Hence

$$\begin{aligned} b_2 &= b_0 y(y+1) - a_2\varphi^2(y) = (1-a_0 y)y(y+1) - a_2 y^2\left(y^2-2\right) \\ &= y\left(y\left(1 - a_0\left(y+1\right) - a_2\left(y^2-2\right)\right) + 1\right) \end{aligned}$$

is divisible by $y = y^{2^1-1}$ but not by $y^2 = y^{2^1}$. Suppose b_{2i} is divisible by y^{2^i-1} but not by y^{2^i}.

$$b_{2(i+1)} = b_{2i}\varphi^{2i}(y)\varphi^{2i}(y+1) - a_{2(i+1)}\varphi^{2(i+1)}(y).$$

Since $\varphi^{2i}(y)$ is divisible by y^{2^i} but not by y^{2^i+1}, and since b_{2i} is divisible by y^{2^i-1} but not by y^{2^i} by induction hypothesis, we have that $b_{2i}\varphi^{2i}(y)$ is divisible by $y^{2^{i+1}-1}$ but not by $y^{2^{i+1}}$. Therefore $b_{2(i+1)}$ is divisible by $y^{2^{i+1}-1}$ but not by $y^{2^{i+1}}$. This proves the claim.

If $n = 2i$ is even, then (3.6) leads to

$$b_{n-2}\varphi^{n-2}(y)\varphi^{n-2}(y+1) = a_n\varphi^n(y)$$

where the left hand side is nonzero and divisible by $y^{2^{n-2}+2^{n-2}} = y^{2^{n-1}}$, but not divisible by y^{2^n} while the right hand side is divisible by y^{2^n}. This is a contradiction.

Otherwise, if $n = 2i+1$ is odd, then $n-1 = 2i$ is even and we can use equation (3.5)

$$b_{n-3}\varphi^{n-3}(y)\varphi^{n-3}(y+1) = a_{n-1}\varphi^{n-1}(y)$$

where the left hand side is nonzero and divisible by $y^{2^{n-3}+2^{n-3}} = y^{2^{n-2}}$, but not divisible by $y^{2^{n-1}}$ while the right hand side is divisible by $y^{2^{n-1}}$. In either case we get a contradiction, so our assumption that $I = A$ must be false. Hence I is a proper left ideal of A.

This completes our second example, and also in this case, as we will see, we can conclude that A is left primitive. Before we can prove this in general, we will generalise the two examples in Theorem 3.7 (i) and (ii).

Theorem 3.7. Let $A = R[x, \varphi]$ for some injective endomorphism $\varphi : R \to R$ of infinite order and R a principal left ideal domain. Let P be a φ-periodic prime of period n and assume there exists $t \geq 2$ such that $\nu_P(\varphi^n(P)) = t$. Since R is a principal left ideal domain, there exist irreducible elements $p, p_1, \ldots, p_{n-1} \in R$ such that $P = \langle p \rangle, \varphi^{-1}(P) = \langle p_1 \rangle, \ldots, \varphi^{-n+1}(P) = \langle p_{n-1} \rangle$. Let $r := pp_1 \cdots p_{n-1}$. Then

(i) p^{t^i} is the largest power of p that divides $\varphi^{ni}(r)$ and $\varphi^{ni}(p)$ for any $i \geq 0$.

(ii) The ideal $B := Ap + A(1 - rx^n)$ is a proper left ideal of A.

(iii) Let M be a maximal left ideal containing B, who's existence is assured by (ii). Then A/M is a faithful simple left A-module.

Proof. (i) Since $\nu_P(\varphi^n(P)) = t$, we have in particular that $\nu_P(\varphi^n(p)) = t$ since $\langle p \rangle = P$. If there exists $1 \leq i \leq n-1$ such that $\nu_P(\varphi^n(p_i)) > 0$, then $\langle \varphi^n(p_i) \rangle = \langle p \rangle = P$, a contradiction. Hence $\nu_P(\varphi^n(p_i)) = 0$ for all $1 \leq i \leq n-1$, so we also have that $\nu_P(\varphi^n(r)) = t$. The result now follows from Lemma 3.4.

(ii) We will assume that $B = A$ and show that this leads to a contradiction. Since $B = A$, there exists $a = \sum_{i=0}^{m} a_i x^i, b = \sum_{i=0}^{l} b_i x^i \in A$ with $a_m \neq 0$, $b_l \neq 0$ and $a_i, b_i \in R$ such that

$$1 = ap + b(1 - rx^n). \tag{3.7}$$

Since the left hand side has degree 0 in x, all coefficients of x must be zero on the right hand side. In particular $l = m - n$ as $b_m \neq 0$ and $a_n \neq 0$. We rewrite (3.7) as

$$\begin{aligned}
1 &= \sum_{i=0}^{m} a_i x^i p + \sum_{i=0}^{l} b_i x^i - \sum_{i=0}^{l} b_i x^i r x^n \\
&= \sum_{i=0}^{m} a_i \varphi^i(p) x^i + \sum_{i=0}^{l} b_i x^i - \sum_{i=0}^{l} b_i \varphi^i(r) x^{i+n} \\
&= \sum_{i=0}^{m} a_i \varphi^i(p) x^i + \sum_{i=0}^{m-n} b_i x^i - \sum_{i=n}^{m} b_{i-n} \varphi^{i-n}(r) x^i \\
&= \sum_{i=0}^{n-1} \left(a_i \varphi^i(p) + b_i \right) x^i + \sum_{i=n}^{m-n} \left(a_i \varphi^i(p) + b_i - b_{i-n} \varphi^{i-n}(r) \right) x^i + \sum_{i=m-n+1}^{m} \left(a_i \varphi^i(p) - b_{i-n} \varphi^{i-n}(r) \right) x^i
\end{aligned}$$

leading to this system of equations:

$$1 = a_0 p + b_0 \tag{3.8}$$

$$0 = a_i \varphi^i(p) + b_i, \quad \text{for all } 1 \leq i \leq n-1$$

$$b_i = b_{i-n}\varphi^{i-n}(r) - a_i \varphi^i(p), \quad \text{for all } n \leq i \leq m-n \tag{3.9}$$

$$b_{i-n}\varphi^{i-n}(r) = a_i \varphi^i(p), \quad \text{for all } m-n+1 \leq i \leq m \tag{3.10}$$

Since $m \geq n$, there exists $j \geq 1$ and $0 \leq s < n$ such that $m = nj + s$.

Claim : For all $0 \leq i \leq j$, the largest power of p that divides b_{nj} is $p^{\frac{t^i-1}{t-1}}$.

To prove the claim, consider first the case where $i = 0$. From (3.8), we see that p cannot divide b_0 because otherwise p would have been invertible and hence $P = R$. Therefore, the largest power of p that divides b_0 is $1 = p^0 = p^{\frac{t^0-1}{t-1}}$.

For the inductive step, suppose $p^{\frac{t^i-1}{t-1}}$ is the largest power of p that divides b_{ni} for some $0 \leq i \leq j$. Then, by (3.9) and part (i) of this lemma, we have that

$$b_{n(i+1)} = b_{ni}\varphi^{ni}(r) - a_{n(i+1)}\varphi^{n(i+1)}(p) = p^{\frac{t^i-1}{t-1}} u p^{t^i} v - a_{n(i+1)} p^{t^{i+1}} w = p^{\frac{t^{i+1}-1}{t-1}} uv - a_{n(i+1)} p^{t^{i+1}} w,$$

for some $u, v, w \in R$ not divisible by p. Since

$$\frac{t^{i+1}-1}{t-1} \leq t^{i+1} - 1 < t^{i+1},$$

we see that $b_{n(i+1)}$ is divisible by $p^{\frac{t^{i+1}-1}{t-1}}$. Suppose $b_{n(i+1)}$ is divisible by $p^{\frac{t^{i+1}-1}{t-1}+1}$. Then, as $\frac{t^{i+1}-1}{t-1} < t^{i+1}$, we have that $\frac{t^{i+1}-1}{t-1} + 1 \leq t^{i+1}$. Then $\varphi^{n(i+1)}(p)$, and hence $b_{ni}\varphi^{ni}(r)$ as well, are both divisible by $p^{\frac{t^{i+1}-1}{t-1}+1}$. But $b_{ni}\varphi^{ni}(r) = p^{\frac{t^{i+1}-1}{t-1}} uv$ with uv not divisible by p, so we have a contradiction. We conclude that $b_{n(i+1)}$ is not divisible by $p^{\frac{t^{i+1}-1}{t-1}+1}$. This proves the inductive step, and hence the claim.

Notice that $m - n + 1 \leq nj \leq m - s \leq m$, so by (3.10) we have that

$$b_{n(j-1)}\varphi^{n(j-1)}(r) = a_{nj}\varphi^{nj}(p).$$

By the claim, $p^{\frac{t^{j-1}-1}{t-1}}$ is the largest power of p that divides $b_{n(j-1)}$, and by part (i), $p^{t^{j-1}}$ is the largest power of p that divides $\varphi^{n(j-1)}(p)$. Hence $p^{\frac{t^{j-1}-1}{t-1}} p^{t^{j-1}} = p^{\frac{t^j-1}{t-1}}$ is the largest power that divides $b_{n(j-1)}\varphi^{n(j-1)}(r) = a_{nj}\varphi^{nj}(p)$. This is a contradiction since p^{t^j} divides $\varphi^{nj}(p)$ by (i). We conclude that our assumption that $B = A$ is false, that is, B is a proper ideal of A.

(iii) Let $I := \operatorname{ann}_A(A/M)$. By Lemma 1.6, I is a prime ideal. Hence, either $I = 0$, $x \in I$ or $I \cap R$ is a nonzero φ-prime ideal of R by Theorem 1.41. We want to rule out the last two possibilities in order to show that $I = 0$.

If $x \in I \subseteq M$, then M contains rx^n since M is a left ideal. Now, from the definition of B, we know that $1 - rx^n \in B \subseteq M$. Since $rx^n \in M$ we have that $1 = (1 - rx^n) + rx^n \in M$. Thus $M = A$, a contradiction since M is proper. Hence $x \notin I$.

Assume now that $I \cap R$ is a nonzero φ-prime ideal. Consider the ideal $P + I \cap R$. Clearly

$$P \subseteq P + I \cap R \subseteq R.$$

Since P is prime, P is maximal because R is a principal ideal domain. Hence $P + I \cap R = P$ or $P + I \cap R = R$. If $P + I \cap R = R$, then $AP + A(I \cap R) = AR = A$, but $AP \subseteq M$ and $A(I \cap R) \subseteq I \subseteq M$, and hence $M = A$, a contradiction. If $P = P + I \cap R$, then $I \cap R \subseteq P$. Now, by Lemma 1.38,

$$I \cap R = Q \cap \varphi^{-1}(Q) \cap \cdots \cap \varphi^{-m+1}(Q),$$

for some φ-periodic prime ideal Q with period m. However, since Q is prime and nonzero, $\varphi^{-i}(Q)$ is prime and nonzero as well by Lemma 1.28, and thus maximal. Assume there exists $0 \leq i, j \leq m-1$ with $i \neq j$ such that $\varphi^{-i}(Q) \subseteq \varphi^{-j}(Q)$. Then $\varphi^{-i}(Q) = \varphi^{-j}(Q)$ since they are maximal, but then the φ-period of Q would be at most $m-1$, a contradiction. Hence $\varphi^{-i}(Q) \nsubseteq \varphi^{-j}(Q)$ for all $0 \leq i, j \leq m-1$ with $i \neq j$, and thus $\varphi^{-i}(Q) + \varphi^{-j}(Q) = R$ for all $0 \leq i, j \leq m-1$ with $i \neq j$ by the maximality. We conclude that $\{\varphi^{-i}(Q)\}_{i=0}^{m-1}$ is a pairwise comaximal family of ideals of R. It follows by Proposition 1.5 that

$$I \cap R = Q\varphi^{-1}(Q) \cdots \varphi^{-m+1}(Q).$$

Therefore,

$$Q\varphi^{-1}(Q) \cdots \varphi^{-m+1}(Q) \subseteq P.$$

Since P is a prime ideal, we have that $\varphi^{-i}(Q) \subseteq P$ for some i by Lemma 1.7. Since $\varphi^{-i}(Q)$ is maximal and P is proper we have that $\varphi^{-i}(Q) = P$. Then

$$\varphi^{-i}(Q) = P = \varphi^{-n}(P) = \varphi^{-n-i}(Q),$$

so $n \geq m$. On the other hand,

$$\varphi^{-m}(P) = \varphi^{-m-i}(Q) = \varphi^{-i}(Q) = P,$$

so $m \geq n$. We conclude that $m = n$ and that $\{Q, \varphi^{-1}(Q), \ldots, \varphi^{-m+1}(Q)\}$ is a permutation of $\{P, \varphi^{-1}(P), \ldots, \varphi^{-n+1}(P)\}$. Thus

$$I \cap R = Q\varphi^{-1}(Q) \cdots \varphi^{-m+1}(Q) = P\varphi^{-1}(P) \cdots \varphi^{-n+1}(P),$$

so we have that $r \in I \cap R \subseteq I \subseteq M$ and hence $rx^n \in M$. As we have seen, this leads to the contradiction that $M = A$. Hence our assumption that $I \cap R$ is a nonzero φ-prime ideal is false. We conclude that $I = 0$ by Theorem 1.41, that is, A/M is faithful.

■

An immediate consequence of Theorem 3.7 (iii) is Corollary 3.8:

Corollary 3.8. Let $A = R[x, \varphi]$ for some injective endomorphism $\varphi : R \to R$ of infinite order and a principal left ideal domain R. Let P be a φ-periodic prime of period n and assume there exists $t \geq 2$ such that $\nu_P(\varphi^n(P)) = t$. Then $A = R[x, \varphi]$ is left primitive.

Corollary 3.8 applies to both of the examples just before Theorem 3.7 so that A is left primitive in these examples.

3.3 Case: There are infinitely many φ-periodic primes and none of them are singular.

Let $A = K[y][x, \varphi]$ be the skew polynomial ring where $\varphi : K[y] \to K[y]$ is an injective endomorphism, and suppose that there are infinitely many φ-periodic primes in $K[y]$. The aim of this section is to show that, in this case, A is left primitive if and only if there is a singular φ-periodic prime ideal in $K[y]$.

So, define $f(y) := \varphi(y) \in K[y]$ and let P be a nonzero prime ideal of $K[y]$, that is, $P = \langle y - a \rangle$ for some $a \in K$. If a is φ-periodic, there exists $n \geq 1$ such that the set of primes

$$\{P, \varphi^{-1}(P), \varphi^{-2}(P), \ldots, \varphi^{-n+1}(P)\}$$

is closed under taking φ^{-1}. Define

$$Q := \prod_{i=0}^{n-1} \varphi^{-1}(P) = \prod_{i=0}^{n-1} \langle y - f^i(a) \rangle = \langle q \rangle,$$

where $q = (y - a)(y - f(a)) \cdots \left(y - f^{n-1}(a)\right)$. We will show that $\varphi(Q) \subseteq Q$. Note that $\varphi(y - f^i(a)) = f(y) - f^i(a)$. If $i \geq 1$, then $f^{i-1}(a)$ is a root of $f(y) - f^i(a)$ and hence

$y - f^{i-1}(a)$ divides $\varphi(y - f^i(a))$. Otherwise, in the case $i = 0$, we observe that $f^{n-1}(a)$ is a root of $f(y) - a = f(y) - f^n(a)$ and hence $y - f^{n-1}(a)$ divides $\varphi(y - a)$. Thus $\varphi(q) \in Q$ and hence $\varphi(Q) \subseteq Q$. It follows that

$$xQ \subseteq \varphi(Q)x \subseteq Qx. \tag{3.11}$$

Let $K(y) := \{gh^{-1} : g, h \in K[y], h \neq 0\}$ denote the field of fractions of $K[y]$. φ extends to a ring homomorphism of $K(y)$ by defining $\varphi(gh^{-1}) := \varphi(g)\varphi(h)^{-1}$. Note that $\varphi(h) \neq 0$ because $h \neq 0$ and φ is injective. Define $B := K(y)[x, \varphi]$. Furthermore, note that, since K is algebraically closed, given any $n \geq 0$, the polynomial $f^n(y) - y$ has n roots. That is, there exists $a_1, a_2, \ldots, a_n \in K$ such that $f^n(a_i) = a_i$ for all $0 \leq i \leq n$.

Lemma 3.9. Let $R = K[y]$ with the injective endomorphism $\varphi : R \to R$, and let $A = R[x, \varphi]$ such that there are infinitely many φ-periodic primes. Assume there exists a simple faithful left A-module $E = Av$. Then $\operatorname{ann}_A(v) \cap R \neq 0$.

Proof. Define $M := \operatorname{ann}_A(v)$. By Lemma 1.4 (ii), M is a maximal left ideal of A, and by Proposition 1.35, the ideal BM of $B := K(y)[x, \varphi]$ is generated by some element $g \in B$. However, observe that any element of B is of the form

$$\sum_{i=0}^{n} h_i s_i^{-1} x^i = s^{-1} \left(\sum_{i=0}^{n} r_i x^i \right),$$

where $r_i, s_i, s \in A$ and s is a common denominator of the fractions $h_i s_i^{-1}$. It follows that we can assume that $BM = Bg$ for some $g \in A$. Write

$$g = r_0 + r_k x^k + r_{k+1} x^{k+1} + \cdots + r_m x^m,$$

where $r_i \in R$ and k is the smallest integer strictly greater than 0 such that $r_k \neq 0$.

If $BM = B$, then $1 \in BM$, that is, $1 = \sum_{i=0}^{n} s^{-1} a_i$ for $a_i \in M$ and $0 \neq s \in R$. Hence $0 \neq s = \sum_{i=0}^{n} a_i \in M \cap R$ and thus $M \cap R \neq 0$. We will therefore in the following assume that BM is a proper ideal of B.

We will assume that $M \cap R = 0$ and see that this leads to a contradiction. Note that $m > 0$ because BM is proper. We claim that there exists a φ-periodic prime $P = \langle y - a \rangle$ of period u such that for all $0 \leq j \leq m$ with $r_j \neq 0$ and all $0 \leq i < u$, we have that $r_j \notin \varphi^{-i}(P)$. To justify the claim, note first that

$$r_j \in \varphi^{-i}(P) \iff y - f^i(a) \text{ divides } r_j \iff f^i(a) \text{ is a root of } r_j.$$

Since there are only finitely many nonzero polynomials r_j, there are only finitely many roots of the r_j's, but by assumption there are infinitely many φ-periodic elements $a \in K$. Hence there exists a φ-periodic element a such that $f^i(a)$ is not a root of r_j for all $0 \leq i < u$ and all nonzero r_j. This proves the claim, in fact, it shows that there are infinitely many such primes.

Let now $P = \langle y - a \rangle$ be such a prime ideal and let $u + 1$ be the period of a, that is, $\varphi^{-u-1}(a) = a$. Define

$$Q := \prod_{i=0}^{u} \varphi^{-i}(P) = \prod_{i=0}^{u} \langle y - f^i(a) \rangle = \langle q \rangle ,$$

where $q = (y - a)(y - f(a)) \cdots (y - f^u(a))$. From (3.11) we know that $xQ \subseteq Qx$. It follows that the two-sided ideal AQA of A is contained in QA. In particular, every element of AQA can be written in the form $\sum_{i=0}^{n} t_i x^i$ for $t_i \in Q$. Since M is a left ideal that does not contain any two-sided ideal, we know in particular that $AQA \nsubseteq M$. It follows that M is properly contained in $M + AQA$. But M is a maximal ideal of A, se we conclude that $M + AQA = A$. It therefore exist $m \in M$ and $t_i \in Q$ with $t_d \neq 0$ such that $m - \sum_{i=0}^{d} t_i d x^i = 1$, or equivalently,

$$1 + \sum_{i=0}^{d} t_i x^i = m \in M.$$

Since $M \subseteq BM = Bg$, there exists $0 \neq s \in R$ and $\sum_{j=0}^{n} s_j x^j \in A$ such that

$$1 + \sum_{i=0}^{d} t_i x^i = s^{-1} \left(\sum_{j=0}^{n} s_j x^j \right) g = s^{-1} \sum_{j=0}^{n} \sum_{i=0}^{m} s_j x^j r_i x^i = s^{-1} \sum_{j=0}^{n} \sum_{i=0}^{m} s_j \varphi^j(r_i) x^{i+j}.$$

Multiplying the above with s yields

$$s + s \sum_{i=0}^{d} t_i x^i = \sum_{j=0}^{n} \sum_{i=0}^{m} s_j \varphi^j(r_i) x^{i+j}. \tag{3.12}$$

Let N be the greatest integer such that $s \in P^N$ but $s \notin P^{N+1}$. Note that $d = n + m$ is the degree of both sides of (3.12), and consider the coefficient of the highest degree term of (3.12):

$$s t_{m+n} = s_n \varphi^n(r_m).$$

Since $t_{m+n} \in Q \subseteq P$, we have that $s t_{n+m} \in P^{N+1}$ and therefore $s_n \varphi^n(r_m) \in P^{N+1}$ as well. However, because $r_m \notin \varphi^{-i}(P)$ for all i, we have in particular that $r_m \notin \varphi^{-n-i}$ for all i, that is, $\varphi^n(r_m) \notin \varphi^{-i}(P)$ for all i. Therefore, $\varphi^n(r_m) \notin Q \subseteq P$, and we conclude that $s_n \in P^{N+1}$. By considering the second highest term of (3.12),

$$s t_{m+n-1} = s_n \varphi^n(r_{m-1}) + s_{n-1} \varphi^{n-1}(r_m),$$

and using the last discovery that $s_n \in P^{N+1}$, we can argue in the same manner that $s_{n-1} \in P^{N+1}$. We can continue in the same way until we consider the coefficient of the term with degree k:

$$st_k = s_k\varphi^k(r_0) + s_0\varphi^0(r_k) = s_k\varphi^k(r_0) + s_0 r_k. \tag{3.13}$$

Since $t_k \in P$ and $s \in P^N$, we have that $st_k \in P^{N+1}$. The right hand side of (3.13) must therefore also be an element in P^{N+1}. Now, neither $\varphi^k(r_0)$ nor $\varphi^0(r_k)$ are in P, but $s_k \in P^{N+1}$, hence we have that $s_0 \in P^{N+1}$. We finally consider the coefficient of the term of degree 0:

$$s + st_0 = s_0 r_0.$$

We have that $st_0 \in P^{N+1}$ and $s_0 r_0 \in P^{N+1}$. It follows that $s \in P^{N+1}$, a contradiction. We conclude that our assumption that $M \cap R = 0$ is false. This completes the proof. ■

Lemma 3.10. Let $R = K[y]$ with injective endomorphism $\varphi : R \to R$ and let $A = R[x, \varphi]$ such that there are infinitely many φ-periodic prime ideals. Assume there exists a simple faithful left A module $E = Av$. Then $I = \mathrm{ann}_A(v) \cap R$ has a nonzero φ-periodic prime divisor.

Proof. Let $M := \mathrm{ann}_A(v)$. By Lemma 3.9, $I \neq 0$. Therefore, I has a unique prime ideal decomposition:

$$I = P_1 P_2 \cdots P_n$$

for some $n \geq 1$. Let $J := AxA$. Since $xa = \varphi(a)x$ for all $a \in R$, we have that $xA \subseteq Ax$. But then $AxA \subseteq Ax \subseteq AxA$, so in fact, $J = AxA = Ax$.

If $Jv = 0$, then $J \subseteq \mathrm{ann}_A(v)$ and hence $J \subseteq \mathrm{ann}_A(E) = 0$, but J is nonzero because $x \in J$. Since Jv is a submodule of the simple module E, it follows that $Jv = E = Av$. In particular, $v \in Jv$, and therefore

$$v = \sum_{i=1}^{t+1} r_i x^i v$$

for some $t \geq 0$ and $r_i \in R$. Thus

$$\left(1 - \sum_{i=1}^{t+1} r_i x^i\right) v = 0,$$

that is,

$$\left(1 - \sum_{i=1}^{t+1} r_i x^i\right) \in M \tag{3.14}$$

Furthermore, for all

$$s \in \prod_{i=1}^{t+1} \varphi^i(I),$$

we have that $s = \varphi(c_1)\varphi^2(c_2)\cdots\varphi^{t+1}(c_{t+1})$ for $c_i \in I$. Therefore, for all $0 \leq i \leq t+1$, we must have that

$$sx^i = \varphi(c_1)\varphi^2(c_2)\cdots\varphi^{t+1}(c_{t+1})x^i = \prod_{j\neq i} \varphi^j(c_j)\varphi^i(c_i)x^i = \prod_{j\neq i} \varphi^j(c_j)x^i c_i \in AI = A\left(M \cap R\right) \subseteq M.$$

Since $sx^i \in M$, we have, using (3.14), that

$$s = s\left(1 - \sum_{i=1}^{t+1} r_i x^i\right) + \sum_{i=1}^{t+1} r_i s x^i \in M.$$

We conclude that

$$\prod_{i=1}^{t+1} \varphi^i(I) \subseteq M \cap R = I = P_1 \cdots P_n \subseteq P_j$$

for $1 \leq j \leq n$.

We will now show that, given any $P \in \{P_1, \ldots, P_n\}$, there exists $1 \leq i \leq t+1$ such that $\varphi^{-i}(P)$ is a φ-periodic prime divisor of I, and thus prove the lemma. Let $P := P_{j_1}$ for some $1 \leq j_1 \leq n$. Since P is prime, there exists by Lemma 1.7 some $1 \leq i_1 \leq t+1$ such that $\varphi^{i_1}(I) \subseteq P$. Therefore, $I \subseteq \varphi^{-i_1}(P)$. By Corollary 1.29, this means that $\varphi^{-i_1}(P)$ is a prime divisor of I, in fact, $\varphi^{-i_1}(P)$ is one of the primes $P_1, \ldots, P_n$. Since $\varphi^{-i_1}(P) = P_{j_2}$ for some $1 \leq j_2 \leq n$, we can apply the same argument again, but this time on P_{j_2}. The result is another prime divisor of I:

$$\varphi^{-i_2}\left(\varphi^{-i_1}(P)\right) = \varphi^{-i_1-i_2}(P) \in \{P_1, \ldots, P_n\}.$$

If we continue in this way, we obtain a series of prime ideals

$$P, \varphi^{-i_1}(P), \varphi^{-i_1-i_2}(P), \varphi^{-i_1-i_2-i_3}(P), \ldots,$$

all contained in the finite set $\{P_1, \ldots, P_n\}$. This implies that there exists i_k, i_l such that $\varphi^{-i_l}\left(\varphi^{-i_k}(P)\right) = \varphi^{-i_k}(P)$. Hence $\varphi^{-i_k}(P)$ is a φ-periodic prime divisor of I. ■

As we will see in the next lemma, I does not only have one φ-periodic prime divisor, but every divisor of I is a φ-periodic prime.

Lemma 3.11. Let $R = K[y]$ with the injective endomorphism $\varphi : R \to R$ and let $A = R[x, \varphi]$ be such that there are infinitely many φ-periodic prime ideals. Assume there exists a simple faithful left A-module $E = Av$. Then $I = \operatorname{ann}_A(v) \cap R$ is a product of nonzero φ-periodic primes.

Proof. We will give a proof by induction on the number of different primes dividing I, where in the base case we have that $I = P_1 \cdots P_n = P^n$, that is, $P = P_i$ for all $1 \leq i \leq n$. By Lemma 3.10, we have that P is φ-periodic. Hence I is a product of φ-periodic primes.

For the inductive part, assume that for every simple faithful left A-module $E = Av$, and whenever $I = \operatorname{ann}_A(v) \cap R$ can be written as a product of less than or equal to $m \geq 1$ different primes, we have that I is a product of φ-periodic primes. Let $E = Av$ be a simple faithful left A-module such that I has $m+1$ different prime divisors. By Lemma 3.10, I has at least one φ-periodic prime divisor. Let $n \leq m+1$ be the number of different φ-periodic prime divisors of I. That is,

$$I = P_1 \cdots P_n P_{n+1} \cdots P_{m+1},$$

where none of the primes $P_{n+1} \cdots P_{m+1}$ are φ-periodic. We want to prove that $n = m+1$.

Assume first that $sv = 0$ for all $s \in P_1 \cdots P_n$. Then

$$s \in \operatorname{ann}_A(v) \cap R = I = P_1 \cdots P_n P_{n+1} \cdots P_{m+1},$$

so we have that

$$P_1 \cdots P_n \subseteq P_1 \cdots P_n P_{n+1} \cdots P_{m+1}.$$

But then, since $P_1 \cdots P_n P_{n+1} \cdots P_{m+1} \subseteq P_1 \cdots P_n$, we have that $n = m+1$, using the uniqueness of the product into prime ideals.

Assume now that there exists $s \in P_1 \cdots P_n$ such that $sv \neq 0$ and define $I_s := \operatorname{ann}_A(sv) \cap R$. Since R is a Dedekind domain, we know that $I_s = Q_1 \cdots Q_u$ for some $u \geq 1$ and where Q_i are prime ideals. Since $sv \neq 0$, we see that $Asv = Av = E$, and since E is a simple faithful left A-module, we know by Lemma 3.10 that there exist $1 \leq i \leq u$ such that Q_i is a φ-periodic prime ideal. Because $P_{n+1} \cdots P_{m+1} sv \subseteq P_1 \cdots P_{m+1} v = Iv = 0$, we have that $P_{n+1} \cdots P_{m+1} \subseteq I_s$ and hence $P_{n+1} \cdots P_{m+1} \subseteq Q_i$. By Lemma 1.7, there exist $n+1 \leq j \leq m+1$ such that $P_j \subseteq Q_i$. Since every nonzero prime ideal in R is maximal, we have in fact that $P_j = Q_i$. But Q_i is φ-periodic so P_j is φ-periodic. This is a contradiction unless $n = m+1$. ∎

Lemma 3.12. Let $R = K[y]$, φ an injective endomorphism of R and $A = R[x, \varphi]$ such that there are infinitely many φ-periodic prime ideals. Suppose that M is a maximal left ideal of A that does not contain any nonzero two-sided ideals. Then $M \cap R$ has a singular φ-periodic prime divisor.

Proof. By Lemma 3.11, all the prime divisors of $I := M \cap R$ are φ-periodic. Take any prime divisor, say P, of I and consider its φ-orbit

$$\mathrm{orb}_\varphi(P) = \{P, \varphi^{-1}(P), \ldots, \varphi^{-u}(P)\},$$

where $u+1$ is the period of P. Suppose that P is the prime yielding the largest P-order $\nu_P(I) = m \geq 1$ among all elements $\varphi^{-j}(P) \in \mathrm{orb}_\varphi(P)$. We can make this assumption without loss of generality because, if $\varphi^{-j}(P)$ is not a prime divisor of I, then $\nu_{\varphi^{-j}(P)}(I) = 0 < \nu_P(I)$ and if $\nu_{\varphi^{-j}(P)}(I) > \nu_P(I)$, then we can replace P by $\varphi^{-j}(P)$, which is a prime divisor of I and is also φ-periodic.

Now, if P is singular we are done. We will therefore in the remaining assume that P is not singular. Let Q be the product of all the ideals in $\mathrm{orb}_\varphi(P)$, i.e.

$$Q = P\varphi^{-1}(P)\cdots\varphi^{-u}(P).$$

As $\varphi\left(\varphi^{-i}(P)\right) \subseteq \varphi^{-i+1}(P)$ for all $i < n$ and $\varphi(P) \subseteq \varphi^{-u}(P)$, because $\varphi^{u+1}(P) \subseteq P$, we conclude that $\varphi(Q) \subseteq Q$. Hence $AQA \subseteq QA$. Since $Q \neq 0$, we have that AQA is a nonzero two-sided ideal and hence not included in the maximal left ideal M. Therefore $M \subset M + AQA$, but M is maximal, so $M + AQA = A$. Thus M contains an element of the form

$$1 + \sum_{i=0}^{d} t_i x^i \in M, \qquad t_0, \ldots, t_d \in Q. \tag{3.15}$$

For any $0 \leq i \leq d$ consider the ideal generated by the image $\varphi^i(I)$, which we denote by L_i, i.e. $L_i = \langle \varphi^i(I) \rangle = R\varphi^i(I)$. Let $\Lambda_i = \{j : L_i \subseteq \varphi^{-j}(P)\}$. Since $j \in \Lambda_i$ if and only if $\nu_{\varphi^{-j}(P)}(L_i) \neq 0$, we have that $C_i = \prod_{j\in\Lambda_i} \varphi^{-j}(P)$ is a divisor of L_i and hence, using the fact that R is a Dedekind domain, there exist an ideal B_i with $L_i = B_i C_i$. Then

$$C_i B_i x^i = R\varphi^i(I)x^i = Rx^i I \subseteq AI = A(M \cap R) \subseteq M.$$

Take the least common multiple $N = LCM(B_0, \ldots, B_d)$ of the ideals B_i as in Definition 1.26. Then since $Q \subseteq C_i$ we also have for all $0 \leq i \leq d$:

$$NQx^i \subseteq C_i B_i x^i \subseteq M.$$

In particular $n\sum_{i=0}^{d} t_i x^i \in M$, for any $n \in N$ and any $t_i \in Q$ from equation (3.15). It follows that for any $n \in N$:

$$n = n\left(1 + \sum_{i=0}^{d} t_i x^i\right) - n\sum_{i=0}^{d} t_i x^i \in M.$$

Hence $N \subseteq I$.

Using that $N = LCM(B_0, \ldots, B_d) \subseteq I \subseteq P^m$, where $m = \nu_P(I)$, we have by Corollary 1.23 that

$$m \leq \nu_P(N) = \max\left(\nu_P(B_0), \nu_P(B_1), \ldots, \nu_P(B_d)\right).$$

Hence there exist $0 \leq i \leq d$ such that $m \leq \nu_P(B_i)$ and therefore $B_i \subseteq P^m$, again by Corollary 1.23. Fix this i. Then $\left\langle \varphi^i(I) \right\rangle = C_i B_i \subseteq P^m \subseteq P = \varphi^{-0}(P)$. Therefore $0 \in \Lambda_i$ and hence $C_i \subseteq P$. Thus

$$\left\langle \varphi^i(I) \right\rangle = C_i B_i \subseteq P P^m = P^{m+1}$$

or equivalently

$$\nu_P\left(\left\langle \varphi^i(I) \right\rangle\right) \geq m + 1. \tag{3.16}$$

In general, we do not know whether i is less than $u+1$, but we can reduce it modulo $u+1$. There are non-negative integers q and r such that $i = q(u+1) + r$ with $0 \leq r \leq u$. Since we suppose that P is not singular, $\varphi^{-(u+1)}(P^{m+1}) = P^{m+1}$ by Proposition 1.32. In particular

$$\varphi^{-i}(P^{m+1}) = \varphi^{-r}\left(\varphi^{-q(u+1)}(P^{m+1})\right) = \varphi^{-r}(P^{m+1}).$$

Together with equation (3.16) we conclude that

$$\left\langle \varphi^i(I) \right\rangle \subseteq P^{m+1} \Rightarrow I \subseteq \varphi^{-i}\left(P^{m+1}\right)) = \varphi^{-r}(P^{m+1}) \Rightarrow \langle \varphi^r(I) \rangle \subseteq P^{m+1}.$$

Therefore we can replace i by $r = i(\mathrm{mod} u+1)$ and we will assume that $i < u+1$.

Let $s = \nu_{\varphi^{-i}(P)}(I)$ which is less than $m+1$ as m was chosen to be the maximal P-order of prime divisors of I. Then $I = J\varphi^{-i}(P)^s$ for some ideal J with $\nu_{\varphi^{-i}(P)}(J) = 0$. Applying φ^i yields:

$$\left\langle \varphi^i(I) \right\rangle = \left\langle \varphi^i(J) \right\rangle \left\langle \varphi^i\left(\varphi^{-i}(P)^s\right) \right\rangle$$

Since $\nu_{\varphi^{-i}(P)}(J) = 0$, we have $J \not\subseteq \varphi^{-i}(P)$. By definition $\varphi^i(J) \not\subseteq P$ and hence also $\left\langle \varphi^i(J) \right\rangle \not\subseteq P$. But this means again that $\nu_P\left(\left\langle \varphi^i(J) \right\rangle\right) = 0$. Together with Corollary 1.25 and equation (3.16) we conclude:

$$\begin{aligned}
\nu_P\left(\left\langle \varphi^i\left(\varphi^{-i}(P)^s\right) \right\rangle\right) &= \nu_P\left(\left\langle \varphi^i(J) \right\rangle\right) + \nu_P\left(\left\langle \varphi^i\left(\varphi^{-i}(P)^s\right) \right\rangle\right) \\
&= \nu_P\left(\left\langle \varphi^i(J) \right\rangle \left\langle \varphi^i\left(\varphi^{-i}(P)^s\right) \right\rangle\right) \\
&= \nu_P\left(\left\langle \varphi^i(I) \right\rangle\right) \\
&\geq m + 1.
\end{aligned}$$

Therefore $\varphi^i\left(\varphi^{-i}(P)^s\right) \subseteq P^{m+1}$ and hence, again by Corollary 1.25, we have that

$$s < m+1 \leq \nu_P\left(\varphi^i\left(\varphi^{-i}(P)^s\right)\right) = s\nu_P\left(\varphi^i\left(\varphi^{-i}(P)\right)\right).$$

This shows that $\nu_P\left(\varphi^i\left(\varphi^{-i}(P)\right)\right) \geq 2$, that is,

$$\varphi^i\left(\varphi^{-i}(P)\right) \subseteq P^2,$$

but then, using that $i < u+1$ and $\varphi^{u+1-i}(P) \subseteq \varphi^{-i}(\varphi^{u+1}(P))$, we obtain that

$$\varphi^{u+1}(P) = \varphi^i\left(\varphi^{u+1-i}(P)\right) \subseteq \varphi^i\left(\varphi^{-i}\left(\varphi^{u+1}(P)\right)\right) \subseteq \varphi^i\left(\varphi^{-i}(P)\right) \subseteq P^2.$$

We conclude that P is singular, which is a contradiction. Hence our assumption that P was not singular is false, so we conclude that P is in fact singular. ■

Theorem 3.13. Let $A = K[y][x,\varphi]$ where $\varphi : K[y] \to K[y]$ is an injective endomorphism. Suppose that there are infinitely many φ-periodic primes in $K[y]$. Then A is left primitive if and only if there is a singular φ-periodic prime ideal in $K[y]$.

Proof. Assume there is a singular φ-periodic prime ideal P in $K[y]$ of period n. Then $\varphi^n(P) \subseteq P^2$, so by taking $t = 2$ in Theorem 3.7, we conclude that A is left primitive by Corollary 3.8.

Conversely, assume A is left primitive. Then there exists a simple faithful left A-module E. Since E is simple, $E = Av$ for some $v \in E$ by Lemma 1.4 (i). Let $I = \operatorname{ann}_A(v) \cap K[y]$. Since I is maximal, $K[y]$ has a singular φ-periodic prime ideal by Lemma 3.12. ■

3.4 Summary left primitivity

We sum up our results for left primitivity in Theorem 3.14:

Theorem 3.14. Let $A = K[y][x,\varphi]$ for an endomorphism $\varphi : K[y] \to K[y]$. Then A is left primitive if and only if φ is injective and of infinite order and

(i) there are only finitely many φ-periodic primes of $K[y]$, or

(ii) $K[y]$ has a singular φ-periodic prime ideal.

Proof. If φ is of finite order, then A is not left primitive by Theorem 2.9, so assume that the order of φ is infinite. Then A is left primitive if $K[y]$ has only finitely many φ-periodic primes by Proposition 3.2. Otherwise, if there are infinitely many φ-periodic prime ideals,

then A is left primitive if and only if $K[y]$ has a singular φ-periodic prime ideal by Theorem 3.13. ■

Chapter 4

Examples of rings that are primitive on only one side

We will need Proposition 4.1 in the following discussion.

Proposition 4.1. Let K be an algebraically closed field and let $\varphi : K[y] \to K[y]$ be an endomorphism such that $\deg(\varphi(y)) > 1$. Then there are infinitely many φ-periodic prime ideals in $K[y]$.

Proof. We know that $\varphi(y) = f(y)$ for some polynomial $f \in K[y]$. Define

$$\Omega := \{a \in K : \text{ there exists a prime number } p \text{ and } a \text{ is a root of } f^p(y) - y\}.$$

For every $a \in \Omega$, the prime ideal $P := \langle y - a\rangle$ of $K[y]$ is φ-periodic because $\varphi^{-p}(P) = \langle y - f^p(a)\rangle = \langle y - a\rangle = P$. Note that if $a, b \in \Omega$ is such that $a \neq b$, then $\langle y - a\rangle \neq \langle y - b\rangle$. Thus the number of φ-periodic primes is at least the cardinality of Ω. Since K is algebraically closed, there exists at least one root $a \in K$ of $f^p(y) - y$ for every prime number p. Hence $|\Omega|$ is greater than or equal to the number of prime numbers. We conclude that there are infinitely many φ-periodic prime ideals in $K[y]$. ■

Let $A = K[y][x, \varphi]$ for some endomorphism φ of $K[y]$. We will now search for conditions on φ such that A is primitive only on one side. By Remark 1.15 and Theorem 1.19, we can exclude simple rings and primitive rings that are PI-rings. We can also exclude skew polynomial rings where $\varphi(y) \in K$ or φ is of finite order by Corollary 2.2 and Theorem 2.9.

Assume there are only finitely many φ-periodic primes of $K[y]$. Then A is left primitive by Proposition 3.2. By Proposition 4.1, we have that $\deg(\varphi(y)) \leq 1$. Hence $\varphi(y) = f(y) = ay+b$

for some $a, b \in K$. In this case $\varphi^2(y) = a^2y + ab + b = a^2y + \left(\frac{a^2-1}{a-1}\right) b$. In general,

$$\varphi^n(y) = a^n y + \left(\frac{a^n - 1}{a - 1}\right) b.$$

Let $P = \langle y - c \rangle$, where $c \in K$, be a φ-periodic prime of $K[y]$. Then there exists $n \in N$ such that $f^n(c) = c$. Hence P is φ-periodic if and only if $a^n c + \left(\frac{a^n-1}{a-1}\right) b = c$, that is, if and only if $c = \frac{b}{1-a}$, assuming $a^n \neq 1$. Hence there is only one φ-periodic prime ideal, namely $P = \left\langle y - \frac{b}{1-a} \right\rangle$, where $a \neq 1$.

If a is a root of unity, then either A is not primitive by Corollary 2.10 and Theorem 2.11, or right (and left) primitive by Theorem 2.12. There are therefore no skew polynomial rings $A = K[y][x, \varphi]$ that are primitive on only one side under the assumption that there are only finitely many φ-periodic primes of $K[y]$. As shown in the previous paragraph, if there are infinitely many φ-periodic prime ideals of $K[y]$, the degree of $\varphi(y)$ cannot be 1 and hence we can exclude this case as well from our search for rings primitive on only one side.

If $\deg(\varphi(y)) > 1$, then A is right primitive by Theorem 2.13, so we will look for conditions for A not to be left primitive. Since there are infinitely many φ-periodic primes by Proposition 4.1, we need to look for endomorphisms φ such that $K[y]$ has no singular φ-periodic prime ideals by Theorem 3.14. This leads to Corollary 4.3 below. Before we can prove Corollary 4.3, we need the general formula for the chain rule in derivation, which we state and prove here:

Proposition 4.2. Let $f(y)$ be a function. Then

$$\frac{df^n(y)}{dy} = \prod_{i=0}^{n-1} f'(f^i(y)). \tag{4.1}$$

for all $n \geq 1$.

Proof. We will prove the formula by induction. The base case $n = 1$ is trivial:

$$\frac{df^1(y)}{dy} = \prod_{i=0}^{1-1} f'(f^i(y)) = f'(f^0(y)) = f'(y).$$

For the inductive step, assume that (4.1) has been proven for n. Then

$$\frac{df^{n+1}(y)}{dy} = f'(f^n(y))\frac{df^n(y)}{dy} = f'(f^n(y)) \prod_{i=0}^{n-1} f'(f^i(y)) = \prod_{i=0}^{n} f'(f^i(y)),$$

where we have used the chain rule $\frac{d(h(g(y)))}{dy} = h'(g(y))g'(y)$. ∎

Corollary 4.3. Let $A = K[y][x, \varphi]$ for an algebraically closed field K of characteristic 0 and an injective endomorphism φ such that $\deg(\varphi(y)) > 1$. Then A is right primitive, and A is left primitive if and only if there exists $a \in K$ such that $P := \langle y - a \rangle$ is φ-periodic and $f'(a) = 0$, where $f(y) := \varphi(y)$.

Proof. A is right primitive by Theorem 2.13. Since $\deg(\varphi(y)) > 1$, there are infinitely many φ-periodic primes in $K[y]$. Thus, by Theorem 3.14, A is left primitive if and only if $K[y]$ has a singular φ-periodic prime ideal. We claim that

> **Claim:** $K[y]$ has a singular φ-periodic prime ideal if and only if there exists $a \in K$ such that $P = \langle y - a \rangle$ is φ-periodic and $f'(a) = 0$.

To prove the claim, assume $K[y]$ has a singular φ-periodic prime ideal Q. Then $Q = \langle y - b \rangle$ for some $b \in K$ such that $f^n(b) = b$ where n is the φ-period of Q. Since Q is singular, we have that

$$\varphi^n(Q) \subseteq Q^2 = \langle y - b \rangle^2 = \left\langle (y - b)^2 \right\rangle.$$

On the other hand, $\langle \varphi^n(Q) \rangle = \langle \varphi^n(y - b) \rangle = \langle \varphi^n(y) - \varphi^n(b) \rangle = \langle \varphi^n(y) - b \rangle$. Hence $(y - b)^2$ divides $\varphi^n(y) - b$, that is, b is a root of $\varphi^n(y) - b$ of multiplicity at least 2. Thus $y - b$ divides $\frac{d(\varphi^n(y) - b)}{dy}$ and therefore $f'\left(f^i(b)\right) = 0$ for some i by the general chain rule (4.1). Let $a = f^i(b)$. Then a is a root of $f'(y)$, and the prime $\langle y - a \rangle$ is φ-periodic because $\varphi^{-n}\left(\langle y - a \rangle\right) = \left\langle y - f^{n+i}(b) \right\rangle = \left\langle y - f^i(b) \right\rangle = \langle y - a \rangle$.

Conversely, assume $a \in K$ is such that $P = \langle y - a \rangle$ is φ-periodic of period n and that $f'(a) = 0$. Then $f^n(a) = a$ and

$$\frac{d\left(f^n(a) - a\right)}{dy} = \prod_{i=0}^{n-1} f'(f^i(a))$$

by (4.1). Since $f'(a) = 0$, we have that $\frac{d(f^n(a) - a)}{dy} = 0$, that is, $y - a$ divides $\frac{d(f^n(a) - a)}{dy}$. Hence a is a root of $f^n(y) - a$ of multiplicity at least 2. Thus

$$\varphi^n(P) = \langle f^n(y) - a \rangle \subseteq \left\langle (y - a)^2 \right\rangle = P^2.$$

We conclude that P is singular. This prove the claim, and the corollary. ∎

Example 4.4. Let $A = \mathbb{C}[y][x, \varphi]$ with φ an endomorphism of $\mathbb{C}[y]$ such that $\varphi(y) = f(y) = y^2 + 1$. Then $\deg(\varphi(y)) > 1$. By Lemma 2.1 φ is injective. Hence A is right primitive by Corollary 4.3.

Since $f'(y) = 2y$, 0 is the only element of $\mathbb{C}$ such that $f'(0) = 0$. However, $f^n(0) \in \mathbb{R}$ and $f^n(0) > 0$ for all $n > 0$. We will prove this using induction on n. First $f(0) = 1 > 0$. Assume now that $f^k(0) \in \mathbb{R}$ and $f^k(0) > 0$ for some $k \geq 1$. Then $f^{k+1}(0) = f\left(f^k(0)\right) = \left(f^k(0)\right)^2 + 1 > 0^2 + 1 > 0$ and $f^{k+1}(0) \in \mathbb{R}$. This shows that $f^n(0) \in \mathbb{R}$ and $f^n(0) > 0$ for all $n > 0$. In particular, there exists no $n > 0$ such that $f^n(0) = 0$, so we conclude that $P := \langle y \rangle$ is not φ-periodic. Hence A is not left primitive by Corollary 4.3.

Example 4.5. Let $A = \mathbb{C}[y][x, \varphi]$ with φ an endomorphism of $K[y]$ such that $\varphi(y) = f(y) = y^2 - 2y + 1$. As in Example 4.4, A is right primitive. Since $f'(y) = 2y - 2$, the only zero of the derivative of f is $y = 1$. However, $f(1) = 0$ and $f^2(1) = 1$, so $P = \langle y - 1 \rangle$ is φ-periodic with period 2. Hence A is left primitive as well by Corollary 4.3.

4.1 A skew polynomial ring over the field of rational functions

We will here present the first known example of a ring primitive on only one side, constructed by George Bergman in 1964 [1].

Let $\varphi : \mathbb{Q}(y) \to \mathbb{Q}(y)$ be the same homomorphism as in Example 3.5, that is, $\varphi\left(r(y)\right) = \varphi\left(r\left(y^2\right)\right)$. Then $\mathbb{Q}[y][x, \varphi]$ is both right and left primitive by Theorem 2.13 and Corollary 3.8. In this section we will se that if we instead of the coefficient ring $\mathbb{Q}[y]$ go to the field of rational functions $\mathbb{Q}(y)$, we can find a subring B of $A := \mathbb{Q}(y)[x, \varphi]$ that is right primitive but not left primitive. Since every field is also an integral domain, and since φ is injective, A is without zero divisors by Proposition 1.33 and every left ideal of A is principal by Proposition 1.35.

Lemma 4.6. For any $r \in \mathbb{Q}(y)$ there is a unique $r^* \in \mathbb{Q}(y)$ such that

$$\frac{r(y) + r(-y)}{2} = r^*\left(y^2\right). \tag{4.2}$$

Proof. To see this, let $r(y) = \dfrac{f(y)}{g(y)}$ where $f, g \in \mathbb{Q}[y]$, and write $f(y) = f_0(y) + yf_1(y)$ such that f_0 is the sum of all the terms of f with even power in y and yf_1 is the sum of all the terms of f with odd powers in y. Similarly, write $g(y) = g_0(y) + yg_1(y)$. Since $(-y)^n = y^n$

for even n, we have that

$$\begin{aligned}\frac{r(y)+r(-y)}{2} &= \frac{\frac{f(y)}{g(y)}+\frac{f(-y)}{g(-y)}}{2} = \frac{f(y)g(-y)+f(-y)g(y)}{2g(y)g(-y)} \\ &= \frac{(f_0(y)+yf_1(y))(g_0(y)-yg_1(y))+(f_0(y)-yf_1(y))(g_0(y)+yg_1(y))}{2(g_0(y)+yg_1(y))(g_0(y)-yg_1(y))} \\ &= \frac{2f_0(y)g_0(y)-2y^2f_1(y)g_1(y)}{2g_0(y)^2-2y^2g_1(y)^2} = \frac{f_0(y)g_0(y)-y^2f_1(y)g_1(y)}{g_0(y)^2-y^2g_1(y)^2} := r^*\left(y^2\right)\end{aligned}$$

■

Lemma 4.7. For every $r, s \in \mathbb{Q}(y)$, define $r \cdot s := rs$ and $r \cdot x := r^*$, with r^* as defined in (4.2). With this structure, $\mathbb{Q}(y)$ is a right A-module.

Proof. Regarding (i), (ii) and (iv) in the definition of a module on page 1, there is nothing to prove. To prove (iii), it suffice to verify that for any $r, s \in \mathbb{Q}(y)$ we have that $(r \cdot x) \cdot s = (r \cdot \varphi(s)) \cdot x$ or equivalently that $r^*s = (r\varphi(s))^*$. Observe that

$$\varphi(s)(y) = s\left(y^2\right) = s\left((-y)^2\right) = \varphi(s)(-y).$$

Hence

$$(r^*s)\left(y^2\right) = r^*\left(y^2\right)s\left(y^2\right) = \frac{r(y)+r(-y)}{2}s\left(y^2\right) = \frac{r(y)\varphi(s)(y)+r(-y)\varphi(s)(-y)}{2} = (r\varphi(s))^*\left(y^2\right),$$

This proves that $r^*s = (r\varphi(s))^*$ and therefore $\mathbb{Q}(y)$ is a right A-module. ■

Lemma 4.8. Let $n, m \geq 0$. Then

$$y^n \cdot x^m = \begin{cases} y^{\frac{n}{2^m}} & \text{if } n \text{ is divisible by } 2^m, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We will give a proof by induction on m. The case $m = 0$ is trivial: $y^n \cdot x^0 = y^n$ as it should since $2^0 = 1$ divides n for any $n \geq 0$. We will divide the inductive step into three cases. In all three cases, we will assume the inductive hypothesis

$$y^n \cdot x^{m-1} = \begin{cases} y^{\frac{n}{2^{m-1}}} & \text{if } n \text{ is divisible by } 2^{m-1}, \\ 0 & \text{otherwise} \end{cases}$$

for $m \geq 1$.

(i) In the case n is not divisible by 2^{m-1}, we have that $y^n \cdot x^m = \left(y^n \cdot x^{m-1}\right) \cdot x = 0 \cdot x = 0$.

(ii) In the case n is divisible by 2^{m-1} but not by 2^m, observe that

$$y^n \cdot x^m = \left(y^n \cdot x^{m-1}\right) \cdot x = y^{\frac{n}{2^{m-1}}} \cdot x = \left(y^{\frac{n}{2^{m-1}}}\right)^* \tag{4.3}$$

because $r \cdot x = r^*$ for all $r \in \mathbb{Q}(y)$. Since $\frac{n}{2^{m-1}}$ is an odd integer we have that $(-y)^{\frac{n}{2^{m-1}}} = -y^{\frac{n}{2^{m-1}}}$ and therefore

$$\left(y^{\frac{n}{2^{m-1}}}\right)^* \left(y^2\right) = \frac{y^{\frac{n}{2^{m-1}}} + (-y)^{\frac{n}{2^{m-1}}}}{2} = \frac{y^{\frac{n}{2^{m-1}}} - y^{\frac{n}{2^{m-1}}}}{2} = 0.$$

Since $y^n \cdot x^m = \left(y^{\frac{n}{2^{m-1}}}\right)^*$ by (4.3), we conclude that $y^n \cdot x^m = 0$.

(iii) In the case where n is divisible by 2^m, we have that $\frac{n}{2^{m-1}}$ is an even integer so that $(-y)^{\frac{n}{2^{m-1}}} = y^{\frac{n}{2^{m-1}}}$. Thus

$$\left(y^{\frac{n}{2^{m-1}}}\right)^* \left(y^2\right) = \frac{y^{\frac{n}{2^{m-1}}} + (-y)^{\frac{n}{2^{m-1}}}}{2} = \frac{y^{\frac{n}{2^{m-1}}} + y^{\frac{n}{2^{m-1}}}}{2} = y^{\frac{n}{2^{m-1}}}.$$

Hence, by (4.3), we have that

$$y^n \cdot x^m = \left(y^{\frac{n}{2^{m-1}}}\right)^* = \left(y^{\frac{n}{2^{m-1}}}\right)^{1/2} = y^{\frac{n}{2^m}}.$$

This completes the proof. ■

Theorem 4.9. Let $A = \mathbb{Q}(y)[x, \varphi]$ where $\varphi : \mathbb{Q}(y) \to \mathbb{Q}(y)$ takes $r(y)$ to $r\left(y^2\right)$ for every $r \in \mathbb{Q}(y)$. Then any subring $B \subseteq A$ containing x and y is right primitive.

Proof. Let $M = \mathbb{Q}(y)$ with the right A-module structure defined in Lemma 4.7. By restricting the scalars, M is also a right B-module. We will prove that B is right primitive by showing that M is simple and faithful.

In order to prove that M is simple, we will prove that $M \neq 0$ and that the only submodules of M are 0 and M. Since M generated by y, we have that $y \in M$ and hence $M \neq 0$. Let $0 \neq \frac{p}{q} \in M$ be a nonzero element in M, where $p, q \in \mathbb{Q}[y]$. Choose $a \in \mathbb{N}$ such that $2^a > \deg(p)$. Let $c :=$ the leading coefficient of p. Then

$$\frac{p}{cq} \cdot qy^{2^a - \deg(p)} = \frac{p}{c} y^{2^a - \deg(p)}.$$

The element on the right is a polynomial with leading term y^{2^a} and constant term zero. Hence

$$\begin{aligned}\frac{p}{c}y^{2^a-\deg(p)}\cdot x^a &= \left(y^{2^a}+\text{lower terms}\right)\cdot x^a\\ &= y^{2^a}\cdot x^a + (\text{lower terms})\cdot x^a\\ &= y^{\frac{2^a}{2^a}}+0 \quad \text{by Lemma 4.8}\\ &= y.\end{aligned}$$

This shows that given any nonzero $m \in M$ we can find $a \in A$ such that $ma = y$. But y generates M, so 0 and M are the only submodules of M. Hence M is simple.

We will now prove that M is faithful. Let $0 \neq b = \sum r_i(y)x^i \in B$ be a nonzero element of the subring B, where $r_i(y) \in \mathbb{Q}(y)$. Choose a polynomial $p \in \mathbb{Q}[y]$ such that $r_i := pr_i \in \mathbb{Q}[y]$ for all i. If $r_i = \frac{f_i}{g_i}$, then $p = \prod_i g_i$ would work. Since b is arbitrary, in order to show that M is faithful it is sufficient to find one element $a \in M$ such that $a \cdot b \neq 0$. To achieve this, we will look for an element $m \in M$ such that $mp \cdot b = m\sum r_i \cdot x^i \neq 0$. Let j be the least integer such that $r_j \neq 0$ and let

$$d = \max_i(\deg r_i - \deg r_j),$$

where we use the convention that the degree of the 0-polynomial is $-\infty$. Choose $n > j$ so that $2^n \geq \deg R_j$ and $2^{n-j-1} \geq d$. Let $m = y^{2^n-\deg r_j}$ and consider

$$y^{2^n-\deg r_j}\cdot\sum r_i(y)x^i.$$

Using Lemma 4.8, we see that the exponent of y in the highest-power term of $y^{2^n-\deg r_j}\cdot r_i x^i$ is

$$\frac{2^n-\deg r_j+\deg r_i}{2^i} \tag{4.4}$$

or zero if (4.4) is not an integer. The denominator 2^i is a result of the action of x^i. For $i = j$, (4.4) is just $2^{n-i} = 2^{n-j}$. For $i > j$,

$$\begin{aligned}\frac{2^n-\deg r_j+\deg r_i}{2^i} = \frac{2^n+(\deg r_i-\deg r_j)}{2^i} &\leq \frac{2^n+d}{2^i} = 2^{n-i}+\frac{d}{2^i}\\ &< 2^{n-(j+1)}+d \leq 2^{n-j-1}+2^{n-j-1} = 2^{n-j}\end{aligned}$$

So only the jth term r_j contributes to the coefficient of $y^{2^{n-j}}$. Because $r_j \neq 0$ we conclude that $y^{2^n-\deg r_j}\cdot r_j(y)x^j \neq 0$ and hence $y^{2^n-\deg r_j}\cdot\sum r_i(y)x^i \neq 0$. This proves that M is faithful and we conclude that B is right primitive. ■

Having proved that B is right primitive, we will search for restrictions on B such that B is not left primitive. For a prime number p, the polynomial

$$\Phi_p(y) = \frac{y^p - 1}{y - 1} = y^{p-1} + y^{p-2} + \cdots + y^2 + y + 1 \in \mathbb{Q}[y]$$

is called the p^{th} **cyclotomic polynomial** and is irreducible according to [13, p. 42]. If $w \in \mathbb{C}\backslash\{1\}$ is a root of $\Phi_p(y)$ and $i < p$, then

$$\Phi_p\left(w^i\right) = \frac{\left(w^i\right)^p - 1}{w^i - 1} = \frac{\left(w^p\right)^i - 1}{w^i - 1} = 0 \tag{4.5}$$

because

$$\Phi_p(w) = 0 \iff \frac{w^p - 1}{w - 1} = 0 \iff w^p - 1 = 0 \iff w^p = 1.$$

Let $1 \leq i \leq p - 1$. Then there exists j such that $ij \equiv 1 \bmod p$. If $w \in \mathbb{C}\backslash\{1\}$ is a root of $\Phi_p(y)$, then $\left(w^i\right)^j = w$. Therefore, if $g \in \mathbb{Q}[y]$, we have that

$$g\left(w^i\right) = 0 \iff \Phi_p(y) \text{ divides } g\left(y^i\right) \iff g\left(\left(w^i\right)^j\right) = 0 \iff g(w) = 0. \tag{4.6}$$

Let $P = \langle q \rangle$ be the prime ideal generated by an irreducible polynomial $q \in K[y]$. Just as on page 13, we define the P-order of a polynomial $f \in \mathbb{Q}[y]$, denoted $\nu_P(f)$, to be the largest $m \geq 0$ such that $\langle f \rangle \subseteq P^m$ and $\langle f \rangle \not\subseteq P^{m+1}$. Equivalently, $\nu_P(f) = m$ if q^m is the largest power of q that divides f. Clearly, if q^m divides f, then $f \in \langle q^m \rangle = \langle q \rangle^m = P^m$. If $\left\langle q^{m+1} \right\rangle$ would divide f, then f would belong to P^{m+1}. On the other hand, if $\langle f \rangle \subseteq P^m$, then $f \in P^m = \langle q^m \rangle$ and hence f is a multiple of q^m.

For $r \in \mathbb{Q}(y)$, we define

$$\nu_P(r) := \nu_P(f) - \nu_P(g),$$

where $r = \frac{f}{g}$ for some $f, g \in \mathbb{Q}[y]$. To simplify notation, define $v_p := \nu_{\langle \Phi_p(y) \rangle}$, that is, v_p is the $\langle \Phi_p(y) \rangle$-order where $\langle \Phi_p(y) \rangle$ is the prime ideal generated by the p^{th} cyclotomic polynomial.

Example 4.10. Let $p = 3$. Then the cyclotomic polynomial is $\Phi_3(y) = y^2 + y + 1$, and if

$$r = \frac{\left(y^2 + y + 1\right)^4 \left(3y^3 - 4y + 2\right)}{3y^3 + 3y^2 + 3y} = \frac{f}{g} \in \mathbb{Q}(y),$$

then $v_3(r) = v_3\left(\frac{f}{g}\right) = v_3(f) - v_3(g) = 4 - 1 = 3$.

Lemma 4.11. Let the endomorphism $\varphi : \mathbb{Q}[y] \to \mathbb{Q}[y]$ be defined by $\varphi(y) = \varphi\left(y^2\right)$ and let $r \in \mathbb{Q}(y)$. Then $v_p\left(r\left(y^2\right)\right) = v_p(r(y))$ for any prime number $p > 2$.

Proof. Since $p > 2$, we have, for any root $w \in \mathbb{C}\backslash\{1\}$ of $\Phi_p(y)$, that $\Phi_p\left(w^2\right) = 0$ by (4.5). It follows that w is a root of $\varphi\left(\Phi_p(y)\right)$ and therefore $\Phi_p(y)$ divides $\Phi_p\left(y^2\right)$, that is,

$$\Phi_p\left(y^2\right) = \Phi_p(y)\tilde{\Phi}(y)$$

for some $\tilde{\Phi} \in \mathbb{Q}[y]$. If fact, $\tilde{\Phi}(y) = \frac{y^p+1}{y+1}$ because

$$\Phi_p\left(y^2\right) = \frac{\left(y^2\right)^p - 1}{y^2 - 1} = \frac{\left(y^p - 1\right)\left(y^p + 1\right)}{(y-1)(y+1)} = \Phi_p(y)\tilde{\Phi}(y).$$

Note that since p is odd, -1 is not a root of $\Phi_p(y)$ because $\Phi_p(-1) = \frac{(-1)^p-1}{y-1} = \frac{-2}{-2} = 1 \neq 0$. Thus any root $w \in \mathbb{C}\backslash\{1\}$ of $\Phi_p(y)$ is different from -1 and

$$\tilde{\Phi}(w) = \frac{w^p + 1}{w + 1} = 0 \iff w^p + 1 = 0 \iff w^p = -1,$$

but $\Phi_p(w) = 0 \implies w^p = 1 \implies 1 = -1$, a contradiction. Thus the roots of $\tilde{\Phi}(y)$ are all different from the roots of $\Phi_p(y)$. Hence $\Phi_p(y)$ does not divide $\tilde{\Phi}(y)$ and therefore

$$v_p\left(\varphi\left(\Phi_p(y)\right)\right) = v_p\left(\Phi_p\left(y^2\right)\right) = v_p\left(\Phi_p(y)\tilde{\Phi}(y)\right) = 1. \tag{4.7}$$

For any $f \in \mathbb{Q}[y]$ with $n = v_p(f)$ there exists a nonzero $g \in \mathbb{Q}[y]$ such that $f(y) = \Phi_p(y)^n g(y)$ and $\Phi_p(y)$ does not divide $g(y)$. Assume $\Phi_p(y)$ divides $g(y^2)$ and let $w \in \mathbb{C}\backslash\{1\}$ be a root of $\Phi_p(y)$. Then $g(w) = 0$ by (4.6) and hence $\Phi_p(y)$ divides $g(y)$. This is a contradiction, so we conclude that $\Phi_p(y)$ does not divide $g\left(y^2\right) = \varphi(g(y))$. It follows that

$$v_p\left(\varphi\left(f(y)\right)\right) = v_p\left(\varphi\left(\Phi_p(y)\right)^n \varphi\left(g(y)\right)\right) = nv_p\left(\varphi\left(\Phi_p(y)\right)\right) + v_p\left(\varphi\left(g(y)\right)\right) = n = v_p(f(y))$$

where we used (4.7). Hence

$$v_p(f(y)) = v_p\left(\varphi\left(f(y)\right)\right).$$

Let now $r = \frac{f}{g} \in \mathbb{Q}(y)$ be any element in $\mathbb{Q}(y)$ such that $f, g \in \mathbb{Q}[y]$. Then

$$v_p(r) = v_p\left(\frac{f}{g}\right) = v_p(f) - v_p(g) = v_p(\varphi(f)) - v_p(\varphi(g)) = v_p\left(\frac{\varphi(f)}{\varphi(g)}\right) = v_p\left(\varphi\left(\frac{f}{g}\right)\right) = v_p(\varphi(r)).$$

■

For a field K, the function $v : K \to \mathbb{R} \cup \{\infty\}$ is called a **valuation** if it satisfies

(i) $v(a) = \infty$ if and only if $a = 0$;

(ii) $v(ab) = v(a) + v(b)$; and

(iii) $v(a + b) \geq \min\{v(a), v(b)\}$ with equality if $v(a) = v(b)$.

for all $a, b \in K$.

Proposition 4.12. Let v be a valuation on a field K. Then $v(1) = v(-1) = 0$.

Proof. $v(1) = v(1 \cdot 1) = v(1) + v(1)$. Subtracting $v(1)$ from both sides yields $0 = v(1)$. Furthermore,

$$0 = v(1) = v((-1)(-1)) = v(-1) + v(-1) = 2v(-1),$$

so $v(-1) = 0$. ■

Just as in Corollary 1.25, we can show that, for a prime number p, the $\Phi_p(y)$-order v_p induced by the cyclotomic polynomial $\Phi_p(y)$ is a valuation on $\mathbb{Q}(y)$. Given any such valuation v and a nonzero element $a = \sum a_i x^i \in A = \mathbb{Q}(y)[x, \varphi]$, we say that a is of **relativized v-degree** j, denoted $\delta_v(a) = j$, if

(i) $v(a_j) = \min_i (v(a_i))$, and

(ii) for all $0 \leq i \leq n$ we have that $v(a_i) = v(a_j)$ implies that $i \leq j$.

Proposition 4.13. Let v be a valuation on $\mathbb{Q}(y)$ that satisfies $v(\varphi(r)) = v(r)$ for all $r \in \mathbb{Q}(y)$. Then v is extended to a valuation on $A = \mathbb{Q}(y)[x, \varphi]$ by the definition $v\left(\sum a_i x^i\right) = \min_i v(a_i)$. Furthermore, $\delta_v(fg) = \delta_v(f) + \delta_v(g)$ for all $f, g \in A$.

Proof. To show that the valuation can be extended to A, we show that the three items in the definition of a valuation are satisfied:

(i) $v\left(\sum_i a_i x^i\right) = \infty \iff \min_i v(a_i) = \infty \iff a_i = 0$ for all $i \iff \sum_i a_i y^i = 0$.

(ii) Let $f, g \in A$ where $f = \sum_{i=0}^{n} a_i x^i$ and $g = \sum_{j=0}^{m} b_j x^j$ and suppose $v(f) = k_1$, $v(g) = k_2$, $\delta_v(f) = i_1$ and $\delta_v(g) = i_2$. Then $v(a_{i_1}) = k_1 \leq v(a_i)$ for all $i \neq i_1$ and $v(a_i) > v(a_{i_1})$ for all $i > i_1$. Similarly, $v(b_{i_2}) = k_2 \leq v(b_i)$ for all $i \neq i_2$ and $v(b_i) > v(b_{i_2})$ for all $i > i_2$. Since

$$fg = \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right) = \sum_{i=0}^{n}\sum_{j=0}^{m} a_i \varphi^i(b_j)\, x^{i+j} = \sum_{l=0}^{m+n}\left(\sum_{i=0}^{l} a_i \varphi^i(b_{l-i})\right) x^l,$$

the coefficient of $x^{i_1+i_2}$ in fg is $\sum_{i=0}^{i_1+i_2} a_i \varphi^i(b_{i_1+i_2-i})$. For all $0 \leq i < i_1$, we have that $i_1 + i_2 - i > i_2$ and hence

$$v\left(\varphi^i(b_{i_1+i_2-i})\right) = v(b_{i_1+i_2-i}) > v(b_{i_2}),$$

where we have used that $v(\varphi(r)) = v(r)$ for all $r \in \mathbb{Q}(y)$. Also, $v(a_i) \geq v(a_{i_1})$. Therefore

$$v\left(a_i\varphi^i\left(b_{i_1+i_2-i}\right)\right) = v(a_i) + v\left(\varphi^i\left(b_{i_1+i_2-i}\right)\right) > v\left(a_{i_1}\right) + v\left(b_{i_2}\right).$$

If $i > i_1$, then $v(a_i) > v(a_{i_1})$ and $v\left(\varphi^i\left(b_{i_1+i_2-i}\right)\right) \geq v(b_{i_2})$, so

$$v\left(a_i\varphi^i\left(b_{i_1+i_2-i}\right)\right) > v\left(a_{i_1}\right) + v\left(b_{i_2}\right)$$

in this case too. However, in the case $i = i_1$, we have that

$$v\left(a_i\varphi^i\left(b_{i_1+i_2-i}\right)\right) = v\left(a_{i_1}\varphi^i\left(b_{i_2}\right)\right) = v\left(a_{i_1}\right) + v\left(b_{i_2}\right).$$

We conclude that

$$v\left(\sum_{i=0}^{i_1+i_2} a_i\varphi^i\left(b_{i_1+i_2-i}\right)\right) = v\left(a_{i_1}\right) + v\left(b_{i_2}\right)$$

since we know that v is a valuation on $\mathbb{Q}[y]$. Now, since $v(a_i) \geq v\left(a_{i_1}\right)$ and $v(b_i) \geq v\left(b_{i_2}\right)$, we have that

$$v\left(a_i\varphi^i\left(b_{l-i}\right)\right) \geq \min\left\{v(a_i) + v(b_{l-i})\right\} \geq v\left(a_{i_1}\right) + v\left(b_{i_2}\right)$$

for any $0 \leq i \leq l \leq m+n$, and hence

$$v(fg) \geq v(f) + v(g). \tag{4.8}$$

However, the valuation of the coefficient of $x^{i_1+i_2}$ is $v(f) + v(g)$, so we have in fact equality in (4.8).

(iii) Let $f, g \in A$ where $f = \sum_{i=0}^{n} a_i x^i$ and $g = \sum_{j=0}^{m} b_j x^j$ such that $m \leq n$. Let $b_i = 0$ for all $m+1 \leq i \leq n$. Then

$$\begin{aligned} v(f+g) &= v\left(\sum_{i=0}^{n} a_i x^i + \sum_{j=0}^{n} b_j x^j\right) = v\left(\sum_{i=0}^{n}(a_i+b_i)x^i\right) = \min_i v(a_i+b_i) \\ &\geq \min_i\left(\min\left\{v(a_i), v(b_i)\right\}\right) = \min\left\{\min_i v(a_i), \min_i v(b_i)\right\} = \min\left\{v(f), v(g)\right\}. \end{aligned}$$

It remains to show that $\delta_v(fg) = \delta_v(f) + \delta_v(g)$. Recall that $\delta_v(f) + \delta_v(g) = i_1 + i_2$. For $l > i_1 + i_2$, the coefficient of x^l in the product fg is $\sum_{i=0}^{l} a_i\varphi^i\left(b_{l-i}\right)$. If $i \leq i_1$, then $l - i > i_1 + i_2 - i \geq i_2$ and hence

$$v\left(\varphi^i\left(b_{l-i}\right)\right) > v\left(b_{i_2}\right) = v(g),$$

and if $i > i_1$, then

$$v(a_i) > v\left(a_{i_1}\right) = v(f).$$

Hence

$$v\left(\sum_{i=0}^{l} a_i\varphi^i\left(b_{l-i}\right)\right) \geq \min\left\{v(a_i)+v(b_{l-i})\right\} > v(f)+v(g).$$

We conclude that $\delta_v(fg) = \delta_v(f) + \delta_v(g)$. ■

Let V be the set of all valuations induced by the cyclotomic polynomial Φ_p with p prime and $p > 2$. Then

(i) V is a infinite set because there are infinitely many prime numbers $p > 2$;

(ii) $v(r(y)) = v(r(y^2))$ for all $v \in V$ by Lemma 4.11;

(iii) Given $r \in \mathbb{Q}(y)$, we have that $v(r) = 0$ for all but a finite number of valuations $v \in V$. This is because r has finite degree in y and hence there are also a finitely many cyclotomic polynomials in its factorisation;

(iv) Given $v \in V$, there exists a nonzero $r_v \in \mathbb{Q}(y)$ such that $v(r_v) > 0$ and $w(r_v) \geq 0$ for all $w \in V$. This is because $v = v_p$ for some prime number $p > 2$, so just let $r_v = \Phi_p(y)$.

Example 4.14. Let r be as in Example 4.10. Since $r = \frac{\Phi_3(y)^4(3y^3-4y+2)}{3\Phi_3(y)}$, we have that $v_3(r) = 3$ while $v_p(r) = 0$ for all other prime numbers $p \geq 5$.

Example 4.15. Let $v = v_5 \in V$. Then $r_v := \Phi_5(y) = y^4 + y^3 + y^2 + y + 1$ has valuation $v(r_v) = 1 > 0$ while $w(r_v) = 0$ for all other valuations $w \in V$.

Proposition 4.16. Let V be the set of all valuations induced by some cyclotomic polynomial and for each $v \in V$, define $A_v := \{a \in A : v(a) \geq 0\}$. Then A_v is a subring of A.

Proof. Since $v(1) = 0$ by Proposition 4.12, we have that $1 \in A_v$. Let $a, b \in A_v$. Then $v(a) \geq 0$ and $v(b) \geq 0$ and hence $v(a+b) = \min\{v(a), v(b)\} \geq 0$. Thus $a + b \in A_v$. Furthermore,

$$v(-a) = v(-1 \cdot a) = v(-1) + v(a) \geq 0,$$

where we used that $v_p(-1) = 0$ by Proposition 4.12, so we have that $-a \in A_v$. Moreover, $v(ab) = v(a) + v(b) \geq 0$ and hence $ab \in A_v$. We conclude that A_v is a subring of A. ■

Define

$$B := \bigcap_{v \in V} A_v,$$

that is, B consists of those elements on which all the valuations are non-negative. Since each A_v are subrings of A, it is clear that B is a subring of A as well.

Theorem 4.17. Let $A = \mathbb{Q}(y)[x, \varphi]$ where $\varphi : \mathbb{Q}(y) \to \mathbb{Q}(y)$ takes $r(y)$ to $r\left(y^2\right)$ for every $r \in \mathbb{Q}(y)$, and let V be the set of all valuations induced by some cyclotomic polynomial. For each $v \in V$, define $A_v = \{a \in A : v(a) \geq 0\}$. Then $B = \bigcap_{v \in V} A_v$ is right primitive but not left primitive.

Proof. Since no cyclotomic polynomials divides y, we have $v(y) = 0$. Also, $v(x) = v(1x) = v(1) = 0$ by Propositions 4.13 and 4.12 for all valuations v. It follows that B contains x and y, so by Theorem 4.9, B is right primitive.

Let I be any nonzero left ideal of B. Since B is left primitive if and only if B has a simple faithful left B-module, B not being primitive is equivalent to either I not being maximal or B/I not being faithful by Lemma 1.4 (iii). Since A is a principal ideal domain by Proposition 1.35, there exists $0 \neq g \in I$ such that $AI = Ag$. We can assume without loss of generality that the leading coefficient of g is 1. We will divide our analyses of the left primitivity of B into two cases; the case where the x-degree of g is strictly positive, and the case where the x-degree of g is 0.

Case 1: g has x-degree $d > 0$.

Choose $w \in V$ such that $w(g) = 0$. Because the leading coefficient of g is 1, we have that $\delta_w(g) = d$. Any nonzero element in AI can be written as ag for some $a \in A$, and

$$\delta_w(ag) = \delta_w(a) + \delta_w(g) \geq \delta_w(g) = d > 0, \tag{4.9}$$

by Proposition 4.13. By hypothesis, we can choose $r_w \in \mathbb{Q}(y)$ such that $w(r_w) > 0$. Then $r_w \notin I$ because otherwise, there exists $a \in A$ such that $r_w = ag$ and $w(r_m) = w(a)w(g) = w(a) \cdot 0 = 0$ for some $a \in A$, a contradiction. Hence, if I were maximal, we could write $br_w + e = 1$, for some $b \in B$ and some $e \in I$, by Lemma 1.4 (iv). But then we would have $e = 1 - br_w$, which has relativized v-degree $\delta_w(1 - br_w) = 0$ because $w(1) = 0$. This contradicts (4.9), so we conclude that I is not maximal.

Case 2: g has x-degree $d = 0$.

In this case $g \in \mathbb{Q}(y)$, and we may assume without loss of generality that $g = 1$. For any valuation $v \in V$, any nonzero $r \in \mathbb{Q}(y)$ and any $b \in B$, we have that

$$v\left(r^{-1}br\right) = v\left(\frac{1}{r}\right) + v(b) + v(r) = v(1) - v(r) + v(b) + v(r) = 0 + v(b) = v(b).$$

Since $v(b) \geq 0$ for all $v \in V$, we have that $v(r^{-1}br) \geq 0$. Hence $r^{-1}br \in B$ and $br \in rB$ for all $b \in B$. Thus $Br \subseteq rB$ and we can show $Br \supseteq rB$ in the same manner. We conclude that $rB = Br$ for all $r \in \mathbb{Q}(y)$. Since $g = 1$, we have that $AI = Ag = A$ and therefore there exists $a_i \in A$ and $e_i \in I$ such that $1 = \sum a_i e_i$. Each element $a_i \in A$ is a skew polynomial in x with coefficients in $\mathbb{Q}(y)$. Let r be the common denominator of all appearing coefficients. Then $r \in \mathbb{Q}[y]$ and $ra_i \in \mathbb{Q}[y]$. Multiplying $1 = \sum a_i e_i$ by r from the left yields $r = \sum (ra_i)e_i \in I$. Note that by the definition of the v_p-orders by the cyclotomic polynomial, each polynomial in $\mathbb{Q}[y]$ has non-negative valuation and hence $\mathbb{Q}[y]$ is a subring of B. Therefore $r = \sum (ra_i)e_i$ has an element $r \in \mathbb{Q}[y] \subseteq B$ on the left side and an element $(ra_i)e_i \in \mathbb{Q}[y]I \subseteq I$ on the right side. This means that the two-sided ideal $rB = Br$ which is an ideal in B, is contained in the left ideal I and in particular $rB = Br \subseteq \operatorname{ann}_B(B/I)$. Since r, as a common multiple of nonzero elements, is nonzero, Br is nonzero. Therefore B/I is not faithful. We conclude that B is not left primitive. ■

Bibliography

[1] Bergman, G. M. *A ring primitive on the right but not on the left* Proc. Amer. Math. Soc. 15 pp. 473–475, 1964.

[2] Brešar, Matej, *Introduction to Noncommutative Algebra*, Springer Cham Heidelberg New York Dordrecht London, 1st edition, 2014.

[3] Eisenbud, David, *Commutative Algebra with a view Toward Algebraic Geometry*, Springer-Verlag New York, 1st edition, 1995.

[4] Goodearl, K. R. and R. B. Warfield, jr, *An Introduction to Noncommutative Noetherian Rings*, Cambridge University Press, Cambridge, United Kingdom, 2nd edition, 2004.

[5] Irving, R. S. *Prime Ideals of Ore extensions over Commutative Rings.* Journal of Algebra 56, pp. 315-342, 1979.

[6] Irving, R. S. *On the Primitivity of Certain Ore extensions* Math. Ann. 242, no. 2, pp. 177–192, 1979.

[7] Kassel, Christian, *Quantum Groups*, Springer, New York, 1st edition, 1995.

[8] Lam, Tsit-Yuen, *A First Course in Noncommutative Rings*, Springer, New York, 2nd edition, 2001.

[9] Lidl, Rudolf & Günter Pilz, *Applied Abstract Algebra*, Springer, New York, 2nd edition, 1998.

[10] McConnell, John C. and James Christopher Robson, *Noncommutative Noetherian Rings*, American Mathematical Society, USA, 1st edition, 2001.

[11] Musson, I. M. *Some examples of modules over noetherian rings.* Glasgow Mathematical Journal, Volume 23, Issue 1, pp. 9-13, January 1982.

[12] Ribenboim, Paulo, *The Theory of Classical Valuations*, Springer New York, 1st edition, 1999.

[13] Rotman, Joseph J., *Galois Theory*, Springer New York, 2nd edition, 1998.

[14] Sharp, R. Y., *Steps in Commutative Algebra*, Cambridge University Press, UK, 2nd edition, 2000.

[15] Shult, Ernest and David Surowski *Algebra*, Springer, 1st edition, 2015.