

The Complexity of Nilradicals and Jacobson Radicals in Computable Rings*

Xun Wang

Abstract. This paper expands upon the work by Downey et al. (2007), who proved that there are computable commutative rings with identity where the nilradical is Σ_1^0 -complete, and the Jacobson radical is Π_2^0 -complete, respectively. We simplify the proof, showing that there is a computable commutative ring with identity where the nilradical is Σ_1^0 -complete and meanwhile the Jacobson radical is Π_2^0 -complete. Moreover, we show that for any c.e. set A there exists a computable commutative ring with identity where the nilradical is Turing equivalent to A , and for any Π_2^0 set B there exists a computable commutative ring with identity where the Jacobson radical is Turing equivalent to B .

1 Introduction

One of the most important questions to be studied in computable ring theory is the complexity of certain ideals. In this article we analyze two special ideals in computable rings. We mainly use computability theory to formulate and answer these complexity questions. Computability theory provides us hierarchies by which we can classify the complexity of certain mathematical objects, and techniques as well as methods by which to gauge them.

In particular, recently there has been a growing interest in the complexity of radicals in computable rings in terms of the arithmetical hierarchy. For example, Downey et al. ([4]) classified the complexity of the nilradical and Jacobson radical in commutative computable rings with identity, proving that the former is Σ_1^0 -complete, while the latter is Π_2^0 -complete. Conidis ([2]) classified the complexity of the prime radical and Levitzki radical in computable noncommutative rings with identity, proving that the former is Π_1^1 -complete, while the latter is Π_2^0 -complete. In this paper, we expand upon the work by Downey et al. ([4]) and study the nilradical and Jacobson radical.

This paper focuses on *commutative rings with identity*. Throughout the rest of this paper, by a *ring* we mean a commutative ring with identity. We collect here the important facts of commutative algebra that we will need. For general references on commutative algebra and ring theory, see [1, 5, 8].

Received 2021-09-29 Revision Received 2021-12-31

Xun Wang Department of Philosophy, Peking University
wangxun123@pku.edu.cn

*The author thanks Wei Wang for insightful initial discussions on the proofs. The author also thanks the anonymous reviewer for careful checking and insightful advice.

Definition 1. A *computable ring* is a computable subset $R \subseteq \mathbb{N}$ equipped with two computable binary operations $+$ and $\cdot$ on R , together with two elements $0, 1 \in R$ such that $(R, 0, 1, +, \cdot)$ is a ring.

Throughout this paper, we use R to denote both the domain of the ring, as well as the tuple $(R, 0, 1, +, \cdot)$.

Definition 2. An *ideal* I of a ring R is a subset of R , which is an additive subgroup and is such that $RI \subseteq I$ (i.e., $x \in R$ and $y \in I$ imply $xy \in I$).

We say an ideal I in R is *maximal*, if $I \neq R$ and there is no ideal I' such that $I \subset I' \subset R$. We say an ideal I in R is *prime*, if $I \neq R$ and for any $a, b \in R$, $ab \in I$ implies $a \in I$ or $b \in I$.

Definition 3. An element $x \in R$ is *nilpotent* if $x^n = 0$ for some $n > 0$.

A nilpotent element is a zero-divisor (unless $R = 0$), but not conversely in general.

Definition 4. The *nilradical* of R is the set of all nilpotent elements in R .

For convenience, let $\text{Nil}(R)$ denote the nilradical of R .

Definition 5. The *Jacobson radical* of R is the intersection of all the maximal ideals of R .

For convenience, let $\text{Jac}(R)$ denote the Jacobson radical of R .

It is easy to verify the following propositions:

Proposition 1. $\text{Nil}(R)$ is an ideal of R .

Proposition 2. $\text{Jac}(R)$ is an ideal of R .

Now we introduce two special rings, the quotient ring and fraction field. Given a ring R and an ideal I of R , for any $r \in R$, we call the set, $r + I = \{r + i : i \in I\}$, a *coset* of I in R . And let $R/I = \{r + I : r \in R\}$.

Definition 6. Let R be a ring and I be an ideal of R . We define the addition and multiplication on R/I as follows:

- (1) $(a + I) + (b + I) = (a + b) + I$
- (2) $(a + I) \cdot (b + I) = (a \cdot b) + I$

Note that R/I with the addition and multiplication is a ring. We call R/I the *quotient ring*.

Definition 7. Let R be any nonzero ring in which the product of any two nonzero elements is nonzero. For $a, b \in R$ with $b \neq 0$, the fraction $\frac{a}{b}$ denotes the equivalence class of pairs (a, b) , where (a, b) is equivalent to (c, d) iff $ad = bc$. The *fraction field*

of R is defined as the set of all such fractions $\frac{a}{b}$. And we define the addition and multiplication on the fraction field as follows:

$$(1) \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

$$(2) \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Note that the fraction field of R with the addition and multiplication is a ring.¹

Definition 8. A *unit* in R is an element $x \in R$ which “divides 1”, i.e., an element x such that $xy = 1$ for some $y \in R$.

The concept of unit will be used in the following characterization of the Jacobson radical.

Definition 9. A *ring homomorphism* is a mapping f of a ring A into a ring B such that for all $x, y \in A$,

$$(1) f(x + y) = f(x) + f(y)$$

$$(2) f(xy) = f(x)f(y)$$

Moreover, if f is a bijective homomorphism, then f is called an *isomorphism* between A and B , and rings A and B are called *isomorphic*.

We say a set *arithmetical* if to define the set we are only allowed to quantify over number variables, but not set variables. The analytic hierarchy lies above the arithmetical hierarchy. We say a set *analytic* if to define the set we are allowed to quantify over both number variables as well as set variables. Analytic sets are more complicated than arithmetical sets. From the computability-theoretic perspective, quantifying over sets can potentially lead to terribly complex objects.

By Definition 4, we have that:

$$\text{Nil}(R) = \{a \in R : \exists n(a^n = 0)\},$$

Obviously the nilradical is arithmetical. But the Jacobson radical is analytic since Definition 5 involves quantifying over maximal ideals of the ring, i.e., over subsets of the ring. However, it is a standard result in commutative algebra that:

$$\begin{aligned} \text{Jac}(R) &= \{a \in R : ab + 1 \text{ is a unit for all } b \in R\} \\ &= \{a \in R : \forall b \exists c((ab + 1)c = 1)\} \end{aligned}$$

It follows that the Jacobson radical is also arithmetical, which means that we describe the Jacobson radical in a easier way than Definition 5. However, there is only one existential quantification on top of the operations in the definition of the nilradical. Further we could ask whether this characterization of the Jacobson radical is optimal in its quantifier complexity. For example, is it possible that there is a one quantifier

¹The fraction field is not only a ring, but also a *field*. But here we do not need any results of field theory.

description of the Jacobson radical using only existential quantification like the definition of the nilradical, or using only universal quantification? Or, is it possible that there is an $\exists\forall$ -description of the Jacobson radical?

Downey et al. ([4]) have showed that the simplest characterization of the nilradical is just the standard definition, while the simplest characterization of the Jacobson radical is the $\forall\exists$ -description above, by showing that the former is Σ_1^0 -complete while the latter is Π_2^0 -complete. Arithmetical hierarchies and completeness are formally introduced in the next section. But intuitively, Γ -completeness means that:

- (1) The complexity is Γ .
- (2) Moreover, the complexity is maximal among Γ -sets, i.e., every Γ -set can be reduced to a Γ -complete-set.

This paper is a continuation of [4] in which the authors construct two different rings to show the complexity of the nilradical and Jacobson radical, respectively. Our goal here is to simplify the proof by constructing a ring where the nilradical is Σ_1^0 -complete and meanwhile the Jacobson radical is Π_2^0 -complete. Moreover, we show that for any c.e. set A there exists a computable ring where the nilradical is Turing equivalent to A , and for any Π_2^0 set B there exists a computable ring where the Jacobson radical is Turing equivalent to B .

2 Preliminaries

In this section we give the reader basic background information about computability theory. For a general reference on computability theory, see [9].

We call a function $f : \mathbb{N}^n \rightarrow \mathbb{N}$ *computable* if there is a Turing machine that outputs the value $f(\bar{x}) \in \mathbb{N}$ on input $\bar{x} \in \mathbb{N}^n$. Given a set $A \subseteq \mathbb{N}^n$, let C_A denote its characteristic function. We call a set $A \subseteq \mathbb{N}^n$ *computable* if there is a Turing machine that outputs $C_A(\bar{x}) \in \{0, 1\}$ on input $\bar{x} \in \mathbb{N}^n$. We call a set $A \subseteq \mathbb{N}$ *computably enumerable*, or *c.e.*, if $A = \emptyset$ or $A = \text{ran}(f)$ for some computable function f .

We may also relativize notions of computability. For any sets $A, B \subseteq \mathbb{N}$, we say that A is *computable relative to* B (written $A \leq_T B$), if there is a Turing machine such that when given access to the function C_B , it outputs $C_A(x)$ on input $x \in \mathbb{N}$. For any sets $A, B \subseteq \mathbb{N}$, we say that A is *Turing equivalent* to B (written $A \equiv_T B$), if $A \leq_T B$ and $B \leq_T A$. The *Turing degree* of A , or simply *degree* of A , is the equivalence class $\deg(A) = \{B : B \equiv_T A\}$. Moreover, we write $\deg(A) \leq \deg(B)$ to mean that $A^* \leq_T B^*$ for some (any) $A^* \in \deg(A)$ and some (any) $B^* \in \deg(B)$.

Before introducing arithmetical hierarchies which will play a role below, we first give an example of how degrees can be used to describe the complexity of ideals. Consider this question: given a computable ring R and an element a in R but not in $\text{Nil}(R)$, how hard is it to find (or construct) a prime ideal P of R such that $a \notin P$? It is not sure that we could find a computable one. Naturally, we ask the following questions. Should any such prime ideal P be computable? Must there exist a such

prime ideal P which is computable? If the answer is negative, how high in the hierarchies of noncomputability must we need in order to observe such prime ideals? To answer these questions, we first introduce some related concepts.

Definition 10. We use $2^{<\mathbb{N}}$ to denote the set of all finite sequences of 0 and 1, partially ordered by the substring relation $\subseteq$.

Definition 11. (1) A *tree* is a subset T of $2^{<\mathbb{N}}$ such that for all $\sigma \in T$, if $\tau \in 2^{<\mathbb{N}}$ and $\tau \subseteq \sigma$, then $\tau \in T$.

(2) An *infinite path* or *branch* of a tree T is a function $f : \mathbb{N} \rightarrow \{0, 1\}$ such that for each $n \in \mathbb{N}$ we have that:

$$\langle f(0), f(1), \dots, f(n) \rangle \in T.$$

Proposition 3 (Weak König's Lemma). *Every infinite tree has an infinite path.*

Weak König's Lemma is not “computably” true, in the sense that:

Proposition 4. *There exists a computable tree T with no computable infinite path.*

To characterize the degrees which compute solutions to Weak König's Lemma, we introduce the following concept.

Definition 12. Given $A, B \in \mathbb{N}$, we say A is *PA over B* if every B -computable infinite tree has an A -computable infinite path. We say that a set A is of *PA degree* if A is PA over computable sets.

The following theorem relates PA degree to the complexity of prime ideals in computable rings.

Theorem 5 (Friedman et al., [6, 7]). *There exists a computable ring R such that every prime ideal P of R is of PA degree.*

Theorem 5 shows that you need to look at least PA degree in order to ensure that you can find a prime ideal, partly answering our question about the complexity hierarchy that we need in order to find a prime ideal such that the prime ideal does not contain a particular element.

Next we complete the answer by proving that to find such a prime ideal, we need at most PA degree, showing that PA degree exactly captures the degree that you need in order to find such a prime ideal.

Theorem 6. *Suppose that R is a computable ring and x is an element of R not in the nilradical. Then for every A of PA degree, there exists a prime ideal P of R such that $\deg(P) \leq \deg(A)$ and $x \notin P$.²*

²The proof borrows idea from [3].

Proof. Let $\{a_i : i \in \mathbb{N}\}$ be an enumeration of R . We define a sequence of finite sets $X_\sigma \subset R$, $\sigma \in 2^{<\mathbb{N}}$. Let $X_\emptyset = \{0_R\}$. Suppose that X_σ has been defined. Let

$$|\sigma| = 4 \cdot \langle i, j, m \rangle + k$$

where $0 \leq k \leq 3$, $|\sigma|$ is the length of σ , $\langle i, j \rangle = \frac{1}{2}(i^2 + 2ij + j^2 + 3i + j)$ and $\langle i, j, m \rangle = \langle \langle i, j \rangle, m \rangle$.³

- $k = 0$. If $a_i \cdot a_j \in X_\sigma$, set $X_{\sigma 0} = X_\sigma \cup \{a_i\}$ and $X_{\sigma 1} = X_\sigma \cup \{a_j\}$. Otherwise, set $X_{\sigma 0} = X_\sigma$ and $X_{\sigma 1} = \emptyset$.
- $k = 1$. Set $X_{\sigma 0} = \emptyset$. If $a_i, a_j \in X_\sigma$, set $X_{\sigma 1} = X_\sigma \cup \{a_i + a_j\}$. Otherwise, set $X_{\sigma 1} = X_\sigma$.
- $k = 2$. Set $X_{\sigma 0} = \emptyset$. If $a_i \in X_\sigma$, set $X_{\sigma 1} = X_\sigma \cup \{a_i \cdot a_j\}$. Otherwise, set $X_{\sigma 1} = X_\sigma$.
- $k = 3$. Set $X_{\sigma 0} = \emptyset$. If $x^m \in X_\sigma$, set $X_{\sigma 1} = \emptyset$. Otherwise, set $X_{\sigma 1} = X_\sigma$.

Let $S = \{\sigma : X_\sigma \neq \emptyset\} \subseteq 2^{<\mathbb{N}}$. We have that S is a computable tree.

Now we show that for each $m, n \in \mathbb{N}$, there exists $\sigma \in S$ of length n such that $x^m \notin \langle X_\sigma \rangle$ where $\langle X_\sigma \rangle$ is the ideal of R generated by X_σ . For $n = 0$, the claim holds since $x^m \neq 0$ for all $m \in \mathbb{N}$. For $n \equiv 1, 2, 3 \pmod{4}$ and, obviously, if the claim holds for n then it also holds for $n + 1$. Suppose that $n \equiv 0 \pmod{4}$ and the claim holds for n . Next we show that it also holds for $n + 1$. Let $\sigma \in S$ be of length $n = 4 \cdot \langle i, j, m \rangle$ such that $x^m \notin \langle X_\sigma \rangle$ for all $m \in \mathbb{N}$. If $a_i \cdot a_j \notin X_\sigma$, then the claim holds since $X_{\sigma 0} = X_\sigma$. If $a_i \cdot a_j \in X_\sigma$, we show that $\langle X_{\sigma 0} \rangle = \langle X_\sigma \cup \{a_i\} \rangle$ and $\langle X_{\sigma 1} \rangle = \langle X_\sigma \cup \{a_j\} \rangle$ do not both generate elements $x^{m_0}, x^{m_1} \in R$. Assume for the sake of a contradiction that:

$$x^{m_0} = c + ra_i, \quad x^{m_1} = d + sa_j,$$

where $r, s \in R$ and c, d are finite linear combinations of elements of X_σ with coefficients from R . Then,

$$x^{m_0+m_1} = cd + csa_j + dra_i + rsa_ia_j,$$

and so $x^{m_0+m_1} \in \langle X_\sigma \rangle$.⁴ So we have a contradiction. Thus, $x^m \notin \langle X_{\sigma 0} \rangle$ for all $m \in \mathbb{N}$, or $x^m \notin \langle X_{\sigma 1} \rangle$ for all $m \in \mathbb{N}$. Therefore the claim holds for $n + 1$.

We have that S is infinite. Let $A \subseteq N$ be of PA degree. Then there exists an A -computable infinite path σ' in S . Let $P = X_{\sigma'}$. Then $P \leq_T A$. By the construction of S , we have that P is a prime ideal of R and $x \notin P$. $\square$

³Just note that $\langle i, j, m \rangle$ is a bijection between $\mathbb{N}^3$ and $\mathbb{N}$. It does not matter what is $\langle i, j, m \rangle$.

⁴This relies on that R is a commutative ring. Note again that this paper only talks about commutative rings with identity.

Now we turn to *arithmetical hierarchy*, which will be used to classify the complexity hierarchy of the nilradical and Jacobson radical. We form the hierarchy of sets by alternating quantifiers.

Definition 13. Let natural numbers $m, n \geq 1$.

(1) A set $A \subseteq \mathbb{N}^m$ is Σ_n^0 (written $A \in \Sigma_n^0$) if there exists a computable relation $R \subseteq \mathbb{N}^{m+n}$ such that for each $x_1, \dots, x_m \in \mathbb{N}$, we have that:

$$(x_1, \dots, x_m) \in A \Leftrightarrow \exists y_1 \forall y_2 \exists y_3 \cdots Q y_n [(x_1, \dots, x_m, y_1, \dots, y_n) \in R],$$

where Q is $\exists$ if n is odd, and $\forall$ if n is even.

(2) A set $A \subseteq \mathbb{N}^m$ is Π_n^0 (written $A \in \Pi_n^0$) if there exists a computable relation $R \subseteq \mathbb{N}^{m+n}$ such that for each $x_1, \dots, x_m \in \mathbb{N}$, we have that:

$$(x_1, \dots, x_m) \in A \Leftrightarrow \forall y_1 \exists y_2 \forall y_3 \cdots Q y_n [(x_1, \dots, x_m, y_1, \dots, y_n) \in R],$$

where Q is $\forall$ if n is odd, and $\exists$ if n is even.

Proposition 7. $A \subseteq \mathbb{N}$ is computably enumerable (c.e.) iff $A \in \Sigma_1^0$.

Definition 14. A is *many-one reducible* (m -reducible) to B (written $A \leq_m B$) if there is a computable function f such that $f(A) \subseteq B$ and $f(\overline{A}) \subseteq \overline{B}$, i.e., $x \in A$ iff $f(x) \in B$.

Although m -reducibility is the first and most natural reducibility, it is too restrictive. The reducibility $\leq_T$ we referred early is a more general concept, and we have that if $A \leq_m B$, then $A \leq_T B$.

Definition 15. (1) A set A is Σ_n^0 -complete, if $A \in \Sigma_n^0$ and $B \leq_m A$ for each set $B \in \Sigma_n^0$.

(2) A set A is Π_n^0 -complete, if $A \in \Pi_n^0$ and $B \leq_m A$ for each set $B \in \Pi_n^0$.

In this paper, we are most interested in c.e. sets and Π_2^0 sets. Here we introduce a Π_2^0 -complete set.

Let $\{\varphi_e\}_{e \in \mathbb{N}}$ be a standard listing of the partial computable functions. Then for every $e \in \mathbb{N}$, the e th c.e. set is defined to be:

$$W_e = \text{dom } \varphi_e = \{x : \exists y (\varphi_e(x) = y)\}.$$

Proposition 8 (Soare, [9]). The set $\text{Inf} = \{k \in \mathbb{N} : W_k \text{ is infinite}\}$ is Π_2^0 -complete.

Then, to show that a given set A is Π_2^0 -complete, it suffices to find a computable function f such that for all $k \in \mathbb{N}$, $k \in \text{Inf}$ iff $f(k) \in A$. Likewise, to show that A is Σ_1^0 -complete, it suffices to find a computable function f and a Σ_1^0 -complete set B such that $k \in B$ iff $f(k) \in A$.

3 The Nilradical and Jacobson Radical

Proposition 9 (Downey et al., [4]). *If R is a computable ring, then $\text{Nil}(R)$ is Σ_1^0 .*

Proof. We have that:

$$\text{Nil}(R) = \{a \in R : \exists n(a^n = 0)\},$$

$\{(a, n) : a^n = 0\}$ is computable, so $\text{Nil}(R)$ is Σ_1^0 . □

Proposition 10 (Downey et al., [4]). *If R is a computable ring, then $\text{Jac}(R)$ is Π_2^0 .*

Proof. We have that:

$$\text{Jac}(R) = \{a \in R : \forall b \exists c((ab + 1)c = 1)\},$$

$\{(a, b, c) : (ab + 1)c = 1\}$ is computable, so $\text{Jac}(R)$ is Π_2^0 . □

In [4], the complexity of the two radicals in computable rings was studied. In particular, the following computability-theoretic results were established:

Theorem 11 (Downey et al., [4]). *There exists a computable ring R such that $\text{Nil}(R)$ is Σ_1^0 -complete.*

Theorem 12 (Downey et al., [4]). *There exists a computable ring R' such that $\text{Jac}(R')$ is Π_2^0 -complete.*

Theorem 11 shows that $\exists$ -description is optimal for the nilradical in its quantifier complexity, and Theorem 12 shows that $\forall\exists$ -description is optimal for the Jacobson radical. However, in [4], the ring R constructed for Theorem 11 and the ring R' for Theorem 12 are totally different. We next simplify the proofs of these two theorems by constructing one computable ring where the nilradical is Σ_1^0 -complete and meanwhile the Jacobson radical is Π_2^0 -complete. Before proving the result, we first introduce two methods of building computable rings by taking subrings and quotient rings, which are very helpful for our proofs.⁵

We first consider subrings. Suppose that A is an infinite computable ring and S is an infinite c.e. subring of A . We may view S as a computable ring R in the following way. Note that S is a c.e. subset of A , then there exists a computable bijection $f : \mathbb{N} \rightarrow S$. Let R be the tuple $(\mathbb{N}, 0, 1, +, \cdot)$ where $0_R = f^{-1}(0_A)$ and $1_R = f^{-1}(1_A)$, $a +_R b = f^{-1}(f(a) +_A f(b))$ and $a \cdot_R b = f^{-1}(f(a) \cdot_A f(b))$. Note that R is a computable ring and f is a computable isomorphism between R and S , in a sense we could view S as a computable ring.

We now consider quotient rings. Suppose that A is a computable ring and I is a computable ideal of A . We may realize the quotient ring A/I as a computable

⁵The methods are given by [4].

ring R in the following way. Let R be the set of minimal elements (with respect to the ordering on $\mathbb{N}$) of cosets of I in A . Then R is computable. Define a function $h : A \rightarrow R$ by letting $h(a)$ be the unique element of R such that $a - h(a) \in I$. We have that h is computable. Let the tuple $(R, 0, 1, +, \cdot)$ be such that $0_R = h(0_A)$ and $1_R = h(1_A)$, $a +_R b = h(a +_A b)$ and $a \cdot_R b = h(a \cdot_A b)$. Note that R is a computable ring and h is a computable surjective homomorphism with kernel I , in a sense we could view A/I as a computable ring.

Combining the two methods, here we give a new method of building computable ring:

Lemma 1. *Suppose that S is an infinite c.e. ring and J is a computable set such that $S \cap J$ is an ideal of S . Then there exist a computable ring R and a computable surjective homomorphism $h : S \rightarrow R$ with kernel $S \cap J$, in a sense we could view $S/(S \cap J)$ as a computable ring.*

Proof. S is an infinite c.e. ring, so we may realize S as a computable ring as described before. There exists a computable bijection $f : \mathbb{N} \rightarrow S$. Let $S' = (\mathbb{N}, 0, 1, +, \cdot)$ where $0_{S'} = f^{-1}(0_S)$ and $1_{S'} = f^{-1}(1_S)$, $a +_{S'} b = f^{-1}(f(a) +_S f(b))$ and $a \cdot_{S'} b = f^{-1}(f(a) \cdot_S f(b))$. We have that S' is a computable ring and $f : S' \rightarrow S$ is a computable isomorphism. Let $I = f^{-1}(S \cap J)$. We have that $S \cap J$ is an ideal of S . It is easy to see that I is an ideal of S' . I is computable, since

$$a \in I \Leftrightarrow f(a) \in S \cap J \Leftrightarrow f(a) \in J.$$

Let R be the set of minimal elements (with respect to the ordering on $\mathbb{N}$) of cosets of I in S' . Note that R is computable. Define a computable function $h : S' \rightarrow R$ by letting $h(s)$ be the unique element of R such that $f^{-1}(s) - h(s) \in I$. Let the ring $(R, 0, 1, +, \cdot)$ be such that $0_R = h(0_{S'})$ and $1_R = h(1_{S'})$, $a +_R b = h(f(a) +_S f(b))$ and $a \cdot_R b = h(f(a) \cdot_S f(b))$. We have that R is a computable ring and h is a computable surjective homomorphism with kernel $S \cap J$. $\square$

Proposition 13. *Suppose that S/I is a quotient ring and R is a ring. Suppose that $h : S \rightarrow R$ is a surjective homomorphism with kernel I .⁶ Then: $a + I \in \text{Nil}(S/I)$ iff $h(a) \in \text{Nil}(R)$.*

Proof. By definition of the nilradical, we have that:

$$\text{Nil}(S/I) = \{a + I \in S/I : \exists n[a^n \in I]\},$$

and

$$\text{Nil}(R) = \{a \in R : \exists n[a^n = 0]\}.$$

Then,

⁶Indeed, even if h is not surjective, the proposition still holds.

$$\begin{aligned}
a + I \in \text{Nil}(S/I) &\Leftrightarrow \exists n[a^n \in I] \\
&\Leftrightarrow \exists n[h(a^n) = 0] \quad (\text{since the kernel of } f \text{ is } I) \\
&\Leftrightarrow \exists n[(h(a))^n = 0] \\
&\Leftrightarrow h(a) \in \text{Nil}(R)
\end{aligned}$$

□

Proposition 14. Suppose that S/I is a quotient ring and R is a ring. Suppose that $h : S \rightarrow R$ is a surjective homomorphism with kernel I . Then: $a + I \in \text{Jac}(S/I)$ iff $h(a) \in \text{Jac}(R)$.

Proof. By a standard result in commutative algebra, we have that:

$$\text{Jac}(S/I) = \{a + I \in S/I : (\forall b \in S)(\exists c \in S)[(ab + 1)c = 1]\},$$

and

$$\text{Jac}(R) = \{a \in R : (\forall b \in R)(\exists c \in R)[(ab + 1)c = 1]\}.$$

Then,

$$\begin{aligned}
a + I \in \text{Jac}(S/I) &\Leftrightarrow (\forall b \in S)(\exists c \in S)[(ab + 1)c = 1] \\
&\Leftrightarrow (\forall b \in S)(\exists c \in S)[(h(a)h(b) + 1)h(c) = 1] \\
&\Leftrightarrow (\forall b' \in R)(\exists c' \in R)[(h(a)b' + 1)c' = 1] \quad (\text{by surjection}) \\
&\Leftrightarrow h(a) \in \text{Jac}(R)
\end{aligned}$$

□

Theorem 15. There exists a computable ring R such that $\text{Nil}(R)$ is Σ_1^0 -complete and $\text{Jac}(R)$ is Π_2^0 -complete.

Proof. Fix a Σ_1^0 -complete c.e. set A . We have that $\text{Inf} = \{k \in \mathbb{N} : W_k \text{ is infinite}\}$ is Π_2^0 -complete. Next we build a computable ring R such that $A \leq_m \text{Nil}(R)$ and $\text{Inf} \leq_m \text{Jac}(R)$ by using the method in Lemma 1.

Let $\alpha : \mathbb{N} \rightarrow A$ be a computable function such that $A = \text{ran}(\alpha)$. Let F be the fraction field of $\mathbb{Z}[\bar{x}, \bar{y}] = \mathbb{Z}[x_1, x_2, \dots, y_1, y_2, \dots]$. For each $n \in \mathbb{N}$, let $\mathbb{Z}[\bar{x}, \bar{y}]_n$ be the subring of $\mathbb{Z}[\bar{x}, \bar{y}]$ consisting of all those elements p such that for each y_i occurring in p we have that $i < n$. Also, let $\mathbb{Z}[\bar{x}, \bar{y}]_\infty = \mathbb{Z}[\bar{x}, \bar{y}]$. Let

$$M = \{1 + \sum_{i=1}^n x_i p_i : n \in \mathbb{N}, p_i \in \mathbb{Z}[\bar{x}, \bar{y}]_{|W_i|} \text{ for all } 1 \leq i \leq n\}.$$

Then M is a subset of $\mathbb{Z}[\bar{x}, \bar{y}]$. And, for all $f, g \in M$, we have that $f \cdot g \in M$. Let

$$S = M^{-1}\mathbb{Z}[\bar{x}, \bar{y}] = \left\{ \frac{g}{m} : g \in \mathbb{Z}[\bar{x}, \bar{y}], m \in M \right\} \subseteq F.$$

We have that S is c.e. Let I be the ideal of S generated by $\{x_{\alpha(n)}^{n+1} \cdot y_0 : n \in \mathbb{N}\}$.

We first show that $k \in A \Leftrightarrow x_k y_0 + I \in \text{Nil}(S/I)$.

- (1) If $k \in A$, say $k = \alpha(n)$, then $x_k^{n+1} y_0^{n+1} \in I$, so $x_k y_0 + I \in \text{Nil}(S/I)$.
- (2) If $k \notin A$, then $x_k y_0 + I \notin \text{Nil}(S/I)$ because $x_k^n y_0^n \notin I$ for each $n \in \mathbb{N}$.

We now show that $k \in \text{Inf} \Leftrightarrow x_k + I \in \text{Jac}(S/I)$.

- (1) Suppose that $k \in \text{Inf}$, i.e., W_k is infinite. Let $\frac{g}{m} \in S$ with $g \in \mathbb{Z}[\bar{x}, \bar{y}]$ and $m \in M$. Since $k \in \text{Inf}$, $\frac{m}{x_k g + m} \in S$. Note that $(x_k \cdot \frac{g}{m} + 1) \frac{m}{x_k g + m} = 1$, so $x_k + I \in \text{Jac}(S/I)$.
- (2) Now suppose that $k \notin \text{Inf}$, i.e., W_k is finite. Fix $l > |W_k|$. We claim that $(x_k + I)(y_l + I) + (1 + I)$ is not a unit in S/I . Assume for the sake of a contradiction that $(x_k + I)(y_l + I) + (1 + I)$ is a unit in S/I . Then there exist $n \in \mathbb{N}$, $p_i \in \mathbb{Z}[\bar{x}, \bar{y}]_{|W_i|}$ and $g \in \mathbb{Z}[\bar{x}, \bar{y}]$ such that:

$$(x_k y_l + 1) \cdot \frac{g}{1 + \sum_{i=1}^n x_i p_i} = 1 + i, \quad i \in I,$$

which gives

$$(x_k y_l + 1) \cdot g = 1 + \sum_{i=1}^n x_i p_i + i \cdot (1 + \sum_{i=1}^n x_i p_i), \quad i \in I.$$

Let $\sigma : \mathbb{Z}[\bar{x}, \bar{y}] \rightarrow \mathbb{Z}[\bar{x}, \bar{y}]$ be the homomorphism induced by fixing x_k and y_l , and sending all other x_i and y_j to 0. Then we have that:

$$(x_k y_l + 1) \cdot \sigma(g) = 1 + x_k \sigma(p_k) + \sigma(i) \cdot (1 + x_k \sigma(p_k)).$$

We have that $\sigma(i) = 0$, since i is divisible by y_0 . Then,

$$(x_k y_l + 1) \cdot \sigma(g) = 1 + x_k \sigma(p_k).$$

We have that $\sigma(g) \neq 0$, since the right-hand side is not 0. Thus the left-hand side has positive y_l -degree. However, the right-hand side has y_l -degree 0 because $y_l \notin p_k$. So we have a contradiction. Thus $(x_k + I)(y_l + I) + (1 + I)$ is not a unit in S/I .

Let P be the ideal of $\mathbb{Z}[\bar{x}, \bar{y}]$ generated by

$$\{x_{\alpha(n)}^{n+1} \cdot y_0 : n \in \mathbb{N}\}.$$

Note that a polynomial $f \in \mathbb{Z}[\bar{x}, \bar{y}]$ is in P iff every nonzero monomial summand of f has a factor $x_i^{m+1} y_0$ such that there exists $n \leq m$ with $\alpha(n) = i$. So P is computable. Let

$$J = \left\{ \frac{g}{1 + g'} : g \in P, g' \in \mathbb{Z}[\bar{x}, \bar{y}] \setminus \mathbb{N} \right\} \subseteq F.$$

Note that J is computable. We have that $I = S \cap J$. Then as described in Lemma 1, we could realize S/I as a computable ring R and let $h : S \rightarrow R$ be the computable surjective homomorphism with kernel I .

Define $f_1 : \mathbb{N} \rightarrow R$ by letting $f_1(k) = h(x_k y_0)$ for all $k \in \mathbb{N}$. Since h is computable, f_1 is computable. And we have that:

$$\begin{aligned}
k \in A &\Leftrightarrow x_k y_0 + I \in \text{Nil}(S/I) \quad (\text{from above}) \\
&\Leftrightarrow h(x_k y_0) \in \text{Nil}(R) \quad (\text{by Proposition 13}) \\
&\Leftrightarrow f_1(k) \in \text{Nil}(R)
\end{aligned}$$

It follows that $A \leq_m \text{Nil}(R)$. Thus $\text{Nil}(R)$ is Σ_1^0 -complete.

Define $f_2 : \mathbb{N} \rightarrow R$ by letting $f_2(k) = h(x_k)$ for all $k \in \mathbb{N}$. Since h is computable, f_2 is computable. And we have that:

$$\begin{aligned}
k \in \text{Inf} &\Leftrightarrow x_k + I \in \text{Jac}(S/I) \quad (\text{from above}) \\
&\Leftrightarrow h(x_k) \in \text{Jac}(R) \quad (\text{by Proposition 14}) \\
&\Leftrightarrow f_2(k) \in \text{Jac}(R)
\end{aligned}$$

It follows that $\text{Inf} \leq_m \text{Jac}(R)$. Thus $\text{Jac}(R)$ is Π_2^0 -complete. $\square$

Moreover, from Theorem 11 and Theorem 12 we immediately have the following corollaries:

Corollary 1. *For any Σ_1^0 -complete (c.e.-complete) set A , there exists a computable ring R such that $\text{Nil}(R) \equiv_T A$.*

Corollary 2. *For any Π_2^0 -complete set A , there exists a computable ring R such that $\text{Jac}(R) \equiv_T A$.*

Next we prove more general results about the nilradical and Jacobson radical in computable rings. Let us start with the nilradical.

Theorem 16. *For any c.e. set A , there is a computable ring R such that $\text{Nil}(R) \equiv_T A$.⁷*

Proof. Let α be a computable function with range A . Let I be the ideal of $\mathbb{Z}[\bar{x}]$ generated by

$$\{x_{\alpha(n)}^{n+1} : n \in \mathbb{N}\}.$$

Then $f \in \mathbb{Z}[\bar{x}]$ is in I iff every nonzero monomial summand of f has a factor x_i^m such that there exists $n < m$ with $\alpha(n) = i$. We have that I is a computable ideal. Then we could realize $\mathbb{Z}[\bar{x}]/I$ as a computable ring R and let $h : \mathbb{Z}[\bar{x}] \rightarrow R$ be the computable homomorphism with kernel I as described before. Define $l : \mathbb{N} \rightarrow R$ by letting $l(k) = h(x_k)$ for all $k \in \mathbb{N}$. Since l is a homomorphism with kernel I , we have that $l(k) = h(x_k) \in \text{Nil}(R)$ iff $x_k^n \in I$ for some $n \in \mathbb{N}$. Thus,

- (1) If $k \in A$, say $k = \alpha(n)$, then $x_k^{n+1} \in I$, so $l(k) \in \text{Nil}(R)$.
- (2) If $k \notin A$, then $l(k) \notin \text{Nil}(R)$ since $x_k^n \notin I$ for all $n \in \mathbb{N}$.

Thus, $A \leq_T \text{Nil}(R)$.

And, $\text{Nil}(R) = \{f \in R : \exists n(f^n = 0_R)\} = \{f \in R : \exists n(f^n \in I)\} = \{f \in R : \text{every nonzero monomial summand of } f \text{ has a factor } x_i \text{ such that } i \in A\}$. So $\text{Nil}(R) \leq_T A$. $\square$

⁷The proof borrows idea from [3].

Now we turn to the Jacobson radical.

Theorem 17. *For any Π_2^0 set A , there is a computable ring R such that $\text{Jac}(R) \equiv_T A$.*

Proof. A is Π_2^0 , so there is a computable relation P such that $x \in A \Leftrightarrow \forall y \exists z P(x, y, z)$. By s - m - n Theorem⁸, define an injective computable function f by

$$\varphi_{f(x)}(u) = \begin{cases} 0, & \text{if } (\forall y \leq u)(\exists z)P(x, y, z); \\ \uparrow, & \text{otherwise;} \end{cases}$$

If $x \in A$, then $W_{f(x)} = \mathbb{N}$, so $f(x) \in \text{Inf}$; If $x \notin A$, then $W_{f(x)}$ is finite, so $f(x) \notin \text{Inf}$. Thus, $x \in A$ iff $f(x) \in \text{Inf}$. And note that f is computable.

Let F be the fraction field of $\mathbb{Z}[\bar{x}, \bar{y}] = \mathbb{Z}[x_1, x_2, \dots, y_1, y_2, \dots]$. For each $n \in \mathbb{N}$, let $\mathbb{Z}[\bar{x}, \bar{y}]_n$ be the subring of $\mathbb{Z}[\bar{x}, \bar{y}]$ consisting of all those elements p such that for all y_i occurring in p we have that $i \leq n$. Also, let $\mathbb{Z}[\bar{x}, \bar{y}]_\infty = \mathbb{Z}[\bar{x}, \bar{y}]$. Let

$$M = \{1 + \sum_{i=1}^n x_i p_i : n \in \mathbb{N}, p_i \in \mathbb{Z}[\bar{x}, \bar{y}]_{|W_{f(i)}|} \text{ for all } 1 \leq i \leq n\}.$$

Then M is a subset of $\mathbb{Z}[\bar{x}, \bar{y}]$. And, for all $f, g \in M$, we have that $f \cdot g \in M$. Let

$$S = M^{-1}\mathbb{Z}[\bar{x}, \bar{y}] = \left\{ \frac{g}{m} : g \in \mathbb{Z}[\bar{x}, \bar{y}], m \in M \right\} \subseteq F.$$

Note that S is c.e..

We first claim that $k \in A \Leftrightarrow x_k \in \text{Jac}(S)$.

- (1) Suppose that $k \in A$ so that $W_{f(k)}$ is infinite. Let $\frac{g}{m} \in S$ and fix $p_i \in \mathbb{Z}[\bar{x}, \bar{y}]_{|W_{f(i)}|}$ such that $m = 1 + \sum_{i=1}^n x_i p_i$. We have that:

$$x_k \cdot \frac{g}{m} + 1 = \frac{x_k g + m}{m} = \frac{x_k g + 1 + \sum_{i=1}^n x_i p_i}{m},$$

and since $x_k g + 1 + \sum_{i=1}^n x_i p_i \in M$, it follows that:

$$\frac{m}{x_k g + 1 + \sum_{i=1}^n x_i p_i} \in S.$$

So $x_k \cdot \frac{g}{m} + 1$ is a unit in S . Thus, $x_k \in \text{Jac}(S)$.

- (2) Now suppose that $k \notin A$ so that $W_{f(k)}$ is finite. Fix $l > |W_{f(k)}|$. We claim that $x_k y_l + 1$ is not a unit in S . Assume for the sake of a contradiction that $x_k y_l + 1$ is a unit in S . Then there exists $p_i \in \mathbb{Z}[\bar{x}, \bar{y}]_{|W_{f(i)}|}$ such that:

$$\frac{1}{x_k y_l + 1} = \frac{g}{1 + \sum_{i=1}^n x_i p_i},$$

⁸Please refer to [9].

which gives

$$1 + \sum_{i=1}^n x_i p_i = g \cdot (x_k y_l + 1).$$

Let $\sigma : \mathbb{Z}[\bar{x}, \bar{y}] \rightarrow \mathbb{Z}[\bar{x}, \bar{y}]$ be the homomorphism induced by fixing x_k and y_l , and sending all other x_i and y_j to 0. It follows that:

$$1 + x_k \cdot \sigma(p_k) = \sigma(g) \cdot (x_k y_l + 1).$$

Since the left-hand side $\neq 0$, $\sigma(g) \neq 0$, so the right-hand side has positive y_l -degree. But the left-hand side has y_l -degree 0 because $p_k \in \mathbb{Z}[\bar{x}, \bar{y}]_{|W_{f(k)}|}$. So we have a contradiction. Thus $x_k y_l + 1$ is not a unit in S . Therefore $x_k \notin \text{Jac}(S)$.

Let I be the ideal of S generated by $\{x_i : i \in A\}$. We claim that $I = \text{Jac}(S)$.

- (1) Suppose that $\frac{f}{1 + \sum_{i=1}^n x_i p_i} \in I$, where $f \in \mathbb{Z}[\bar{x}, \bar{y}]$ and $p_i \in \mathbb{Z}[\bar{x}, \bar{y}]_{|W_{f(i)}|}$. Then every nonzero monomial summand of f has a factor x_j , $j \in A$. Let $\frac{g}{1 + \sum_{i=1}^{n'} x_i p'_i} \in S$, where $g \in \mathbb{Z}[\bar{x}, \bar{y}]$ and $p'_i \in \mathbb{Z}[\bar{x}, \bar{y}]_{|W_{f(i)}|}$. We have that:

$$\frac{f}{1 + \sum_{i=1}^n x_i p_i} \cdot \frac{g}{1 + \sum_{i=1}^{n'} x_i p'_i} + 1 = \frac{fg + (1 + \sum_{i=1}^n x_i p_i)(1 + \sum_{i=1}^{n'} x_i p'_i)}{(1 + \sum_{i=1}^n x_i p_i)(1 + \sum_{i=1}^{n'} x_i p'_i)}.$$

Note that $fg + (1 + \sum_{i=1}^n x_i p_i)(1 + \sum_{i=1}^{n'} x_i p'_i) \in M$, so

$$\frac{(1 + \sum_{i=1}^n x_i p_i)(1 + \sum_{i=1}^{n'} x_i p'_i)}{fg + (1 + \sum_{i=1}^n x_i p_i)(1 + \sum_{i=1}^{n'} x_i p'_i)} \in S.$$

Thus $\frac{f}{1 + \sum_{i=1}^n x_i p_i} \cdot \frac{g}{1 + \sum_{i=1}^{n'} x_i p'_i} + 1$ is a unit in S . Therefore, $\frac{f}{1 + \sum_{i=1}^n x_i p_i} \in \text{Jac}(S)$.

- (2) Now suppose that $\frac{f}{1 + \sum_{i=1}^n x_i p_i} \notin I$, where $f \in \mathbb{Z}[\bar{x}, \bar{y}]$ and $p_i \in \mathbb{Z}[\bar{x}, \bar{y}]_{|W_{f(i)}|}$. Then f has a monomial summand d such that d could not be divisible by any x_i for $i \in A$. Let $B = \{i \in \mathbb{N} : d \text{ is divisible by } x_i\}$. Then $A \cap B = \emptyset$. Let $C = \{j \in \mathbb{N} : d \text{ is divisible by } y_j\}$. Let $l' = \max\{|W_{f(i)}| : i \in B\} + 1$. Then for each $i \in B$, $l' > |W_{f(i)}|$. We claim that $\frac{f}{1 + \sum_{i=1}^n x_i p_i} \cdot y_{l'} + 1$ is not a unit in S . Assume for the sake of a contradiction that $\frac{f}{1 + \sum_{i=1}^n x_i p_i} \cdot y_{l'} + 1$ is a unit. Then there exist $n' \in \mathbb{N}$, $p'_i \in \mathbb{Z}[\bar{x}, \bar{y}]_{|W_{f(i)}|}$ and $g \in \mathbb{Z}[\bar{x}, \bar{y}]$ such that:

$$\frac{1}{\frac{f}{1 + \sum_{i=1}^n x_i p_i} \cdot y_{l'} + 1} = \frac{g}{1 + \sum_{i=1}^{n'} x_i p'_i},$$

which gives

$$(1 + \sum_{i=1}^n x_i p_i)(1 + \sum_{i=1}^{n'} x_i p'_i) = g \cdot (f y_{l'} + 1 + \sum_{i=1}^n x_i p_i).$$

Let $\tau : \mathbb{Z}[\bar{x}, \bar{y}] \rightarrow \mathbb{Z}[\bar{x}, \bar{y}]$ be the homomorphism induced by fixing x_i and y_j for each $i \in B$, each $j \in C$ and $j = l'$, and sending all other $x_{i'}$ and $y_{j'}$ to 0. It follows that:

$$(1 + \sum_{i \in B} x_i \tau(p_i))(1 + \sum_{i \in B} x_i \tau(p'_i)) = \tau(g) \cdot (\tau(f) y_{l'} + 1 + \sum_{i \in B} x_i \tau(p_i)).$$

$\tau(g) \neq 0$ because the left-right hand is not zero. $\tau(f) \neq 0$ because d is a nonzero monomial summand of $\tau(f)$ and $\tau(d) = d$. Since for each $i \in B$, $l' > |W_{f(i)}|$, so $y_{l'}$ does not occur in $\sum_{i \in B} x_i \tau(p_i)$. Thus the right-hand side has positive $y_{l'}$ -degree. But the left-hand side has $y_{l'}$ -degree 0, since $y_{l'}$ does not occur in $\sum_{i \in B} x_i \tau(p_i)$ or $\sum_{i \in B} x_i \tau(p'_i)$. So we have a contradiction. Thus $\frac{f}{1 + \sum_{i=1}^n x_i p_i} \cdot y_{l'} + 1$ is not a unit in S . That is, $\frac{f}{1 + \sum_{i=1}^n x_i p_i} \notin \text{Jac}(S)$.

Next we built the desired computable ring R . S is an infinite c.e. subring of F , so we may realize S as a computable ring as described before. There exists a computable bijection $h : \mathbb{N} \rightarrow S$. Let R be the computable ring $(\mathbb{N}, 0, 1, +, \cdot)$ where $0_R = h^{-1}(0_S)$ and $1_R = h^{-1}(1_S)$, $a +_R b = h^{-1}(h(a) +_S h(b))$ and $a \cdot_R b = h^{-1}(h(a) \cdot_S h(b))$. Note that $h : R \rightarrow S$ is a computable isomorphism. We have that:

$$k \in A \Leftrightarrow x_k \in \text{Jac}(S) \Leftrightarrow h^{-1}(x_k) \in \text{Jac}(R).$$

It follows that $A \leq_T \text{Jac}(R)$. Moreover, we have that:

$$\begin{aligned} a \in \text{Jac}(R) &\Leftrightarrow h(a) \in \text{Jac}(S) \\ &\Leftrightarrow h(a) \in I \\ &\Leftrightarrow \text{every monomial summand of the numerator of } h(a) \text{ has} \\ &\quad \text{a factor } x_i \text{ with } i \in A \end{aligned}$$

It follows that $\text{Jac}(R) \leq_T A$. Therefore, $A \equiv_T \text{Jac}(R)$. □

References

- [1] M. Atiyah and I. Macdonald, 1969, *Introduction to Commutative Algebra*, Oxford: Westview Press.
- [2] C. J. Conidis, 2009, "On the complexity of radicals in noncommutative rings", *Journal of Algebra*, **322**(10): 3670–3680.
- [3] C. J. Conidis, 2010, "Chain conditions in computable rings", *Transactions of the American Mathematical Society*, **362**(12): 6523–6550.
- [4] R. Downey, S. Lempp and J. Mileti, 2007, "Ideals in computable rings", *Journal of Algebra*, **314**(2): 872–887.
- [5] D. Dummit and R. Foote, 1999, *Abstract Algebra*, Danvers: John Wiley & Sons.
- [6] H. Friedman, S. Simpson and R. Smith, 1983, "Countable algebra and set existence axioms", *Annals of Pure and Applied Logic*, **25**(2): 141–181.
- [7] H. Friedman, S. Simpson and R. Smith, 1985, "Addendum to 'countable algebra and set existence axioms'", *Annals of Pure and Applied Logic*, **28**(3): 319–320.
- [8] H. Matsumura, 2004, *Commutative Ring Theory*, Cambridge: Cambridge University Press.
- [9] R. Soare, 1987, *Recursively Enumerable Sets and Degrees*, Berlin: Springer.

可计算环上幂零根与 Jacobson 根的计算复杂度

王勋

摘 要

Downey 等人 (2007) 证明了: 存在一个可计算的有单位元素的交换环, 其幂零根是 Σ_1^0 -完全集; 存在另一个可计算的有单位元素的交换环, 其 Jacobson 根是 Π_2^0 -完全集。本文进一步证明了: 存在一个可计算的有单位元素的交换环, 其幂零根是 Σ_1^0 -完全集且其 Jacobson 根是 Π_2^0 -完全集。此外, 对于任意 c.e. 集 A , 都存在一个可计算的有单位元素的交换环使其幂零根与 A 图灵等价; 对于任意 Π_2^0 集 B , 都存在一个可计算的有单位元素的交换环使其 Jacobson 根与 B 图灵等价。

王勋 北京大学哲学系
wangxun123@pku.edu.cn