IDEALS IN COMPUTABLE RINGS

RODNEY G. DOWNEY, STEFFEN LEMPP, AND JOSEPH R. MILETI

ABSTRACT. We show that the existence of a nontrivial proper ideal in a commutative ring with identity which is not a field is equivalent to WKL_0 over RCA_0. We also prove that there are computable commutative rings with identity where the nilradical is Σ^0_1-complete, and the Jacobson radical is Π^0_2-complete, respectively.

1. INTRODUCTION

It was only about a hundred years ago that algebra slowly turned away from an algorithmic approach toward a more abstract, axiomatic approach. (See, for instance, Metakides and Nerode [10] and Stolenberg-Hansen and Tucker [20].) The use of computers in understanding algebraic objects has highlighted the need to understand the effective, or algorithmic, content of mathematics. Classical studies in this area include the famous studies of the effective content of field theory: Frölich and Shepherdson [5], Malt'cev [7], Rabin [13], and Metakides and Nerode [8, 9]. As witnessed by these studies and the work in, for instance, combinatorial group theory, we also get an additional motivation for trying to understand the algorithmic content of algebra. Not only is it the case that we gain insight into the algorithmic nature of the structures, but we also often gain additional algebraic insight into the structures themselves. For example, Rabin showed that each computable field[1] has a computable algebraic closure, but in Metakides and Nerode [8] it is shown that the usual method of constructing such a closure is possible if and only if there is a "splitting algorithm." The point is that Rabin's construction of the algebraic closure must be distinct from the usual one.

1991 *Mathematics Subject Classification.* 03B30, 03C57, 03D45, 03F35.

Key words and phrases. computable ring, reverse mathematics, ideal, nilradical, Jacobson radical.

The authors would like to thank Don Passman for some helpful discussions. The first author's research was partially supported by The Marsden Fund of New Zealand. The second author's research was partially supported by NSF grant DMS-0140120. The third author's research was partially supported by ...

[1] We make these notions more precise later.

In recent years, this area has become an active field of research, in particular by researchers in computability theory and proof theory. Worker in proof theory have become interested in questions of effectiveness since such issues are strongly related to provability in weak proof-theoretic systems. Again the motivation is both intrinsic and relates to additional algebraic structure. For example, as we discuss in detail below, Friedman, Simpson and Smith FSS83,FSS85 proved that the existence of maximal ideals in commutative rings with identity is equivalent to a certain system ACA_0, whereas the existence of prime ideals is equivalent to a provably weaker system WKL_0. The point again is that there must be another way to construct prime ideals which does not filter through maximal ones. (More on this in Section 2.)

This paper is a contribution to the study of the effective content of the theory of ideals in commutative rings. Thus we follow earlier papers such as, for instance, Baumslag, Canonito, and Miller [1], Richman [14], Seidenberg [15, 16], Shlapentokh [17], Stolenberg-Hansen and Tucker [18, 19]. For general background we refer the reader to [20].

A companion paper by the authors as well as Hirschfeldt, Kach, and Montalbán [2] will study the effective content of the theory of subspaces of a vector space.

Throughout this paper, by a ring we mean a commutative ring with identity. Our goal here is to analyze the complexity of ideals in a ring relative to the complexity of the ring itself, and our main approach is to use computability theory to formulate and answer these questions. Computability theory provides hierarchies and structures by which we can measure the complexity of mathematical objects, and techniques by which to classify them. This framework provides a robust setting in which to gauge not only the information content of mathematical objects up to algorithmic transformations, but also how difficult it is to define certain mathematical objects.

Definition 1.1. *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.*

One particular motivation in the results below is to understand what is lost when one trades elements for ideals. For example, consider the following elementary characterization of when a ring is a field.

Proposition 1.2. *A ring R is a field if and only if it has no nontrivial proper ideals.*

The question is whether this process of shifting from elements to ideals forces us to sacrifice "effectiveness", which can be made precise with the concept of computability. The issue here is the right-to-left direction. Suppose that R is a computable ring which is not a field, and fix $a \in R$ such that a is not a unit. We then have that $I = (a)$ is a proper nontrivial ideal. However, from the point of view of computability theory, the ideal I may not be computable. Given an element $b \in R$, it seems that in order to determine whether $b \in I$, we need to check $r \cdot a$ for every $r \in R$, and if we simply start looking at multiples we may never know when to stop. More precisely, the ideal I is computably enumerable but it is not clear that it is computable. We thus ask the following effective analogues of the above proposition: Given a computable ring R which is not a field, should principal ideals in R be computable? Should *any* nontrivial proper principal ideal be computable? Must there exist a *any* nontrivial proper ideal I of R which is computable? If the answer is negative, how high in the hierarchies of noncomputability must we look in order to observe nontrivial proper ideals? Should principal ideals be more complicated than other proper ideals, or less so?

Another goal is to understand the complexity of certain special ideals of a ring. For example, let R be a ring. The Jacobson radical of R is defined to be the intersection of all maximal ideals of R. Notice that this definition involves quantifying over ideals of the ring, and hence over subsets of the ring. From the computability-theoretic perspective, quantifying over subsets can potentially lead to extremely complicated objects (that is, into the analytical hierarchy). Another description of the Jacobson radical, which says that a is in the Jacobson radical of R if and only if $ab + 1$ is a unit for all $b \in R$, which is to say that

$$a \in \mathrm{Jac}(R) \Leftrightarrow \forall b \exists c((ab + 1)c = 1)$$

involves quantifying over elements of the ring followed by a computable statement (whether $(ab + 1)c = 1$ can be checked computably). One could ask whether this description is optimal in its quantifier complexity. For example, is it possible that there is a one quantifier description (using only existentials, or only universals on top of the operations in the ring) or one that involves an $\exists\forall$-description?

Another perspective is to approach these problems from the viewpoint of reverse mathematics. Whereas in the computability-theoretic approach, we use classical mathematical tools and are interested in the complexity of various mathematical objects, in the reverse mathematics approach, we carefully gauge the axioms that are necessary and sufficient to prove theorems of mathematics, such as Proposition 1.2. The weak base system of axioms is denoted by RCA_0 and roughly captures proofs that could be called "effective" or "computable". Thus, an analogue of the effective version of Proposition 1.2 above would to ask whether it is provable in RCA_0. It turns out that there are only a handful of systems more powerful than RCA_0, each of which assert the existence of more complicated types of sets, such that most classical mathematics theorems are equivalent, over RCA_0, to one of these systems. Thus, using the program of reverse mathematics, we are able to precisely calibrate the strength of the set existence axioms necessary and sufficient to prove various mathematical theorems, including Proposition 1.2.

2. Computability Theory and Reverse Mathematics

2.1. **Computability Theory.** For general references on computability theory, please consult Odifreddi [11, 12] or Soare [22]. We call a function $f\colon \mathbb{N}^n \to \mathbb{N}$ or set $A \subseteq \mathbb{N}^n$ *computable* if it falls into any of the many equivalent formal notions (such as Turing machine computable or general recursive). We say that a set $A \subseteq \mathbb{N}$ is *computably enumerable*, or *c. e.*, if either $A = \emptyset$ or $A = \operatorname{ran}(f)$ for some computable function f.

We may also relativize notions of computability, and for $A, B \subseteq \mathbb{N}$ we write $A \leq_T B$ if A is computable relative to B (which can be given a formal definition in terms of oracle Turing machines, for example). The equivalence classes of the corresponding equivalence relation are called *Turing degrees* or simply *degrees*. We typically denote degrees by lower case bold letters such as $\mathbf{d}$, and we write $\mathbf{a} \leq \mathbf{b}$ to mean that $A \leq_T B$ for some (any) $A \in \mathbf{a}$ and $B \in \mathbf{b}$. Given a set $A \subseteq \mathbb{N}$, we use $\deg(A)$ to denote the degree of A. We use $\mathbf{0}$ to denote the degree of the computable sets. Given a set $A \subseteq \mathbb{N}$, we let A' be the set corresponding to the halting problem of A (that is, the set which codes all halting computations relative to A, or, equivalently, which effectively codes all existential questions relative to A). Also, given a degree $\mathbf{a}$, we let $\mathbf{a}'$ be $\deg(A')$ for some (any) $A \in \mathbf{a}$.

Computably enumerable sets correspond to an existential question relative to a computable set, and we may form a hierarchy of sets by alternating quantifiers (because we can code two like quantifiers as one). This gives rise to the *arithmetical hierarchy.*

Definition 2.1. *Let $n \in \mathbb{N}$.*

(1) *A set $B \subseteq \mathbb{N}^m$ is Σ^0_n if there exists a computable $A \subseteq \mathbb{N}^{n+m}$ such that for all $x_1, x_2, \dots, x_m \in \mathbb{N}$, we have*

$$(x_1, x_2, \dots, x_m) \in B \Leftrightarrow \\ \exists y_1 \forall y_2 \exists y_3 \cdots Q y_n [(x_1, x_2, \dots, x_m, y_1, y_2, \dots, y_n) \in A]$$

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

(2) *A set $B \subseteq \mathbb{N}^m$ is Π^0_n if there exists a computable $A \subseteq \mathbb{N}^{n+m}$ such that for all $x_1, x_2, \ldots, x_m \in \mathbb{N}$, we have*

$$(x_1, x_2, \ldots, x_m) \in B \Leftrightarrow \forall y_1 \exists y_2 \forall y_3 \cdots Q y_n [(x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_n) \in A]$$

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

Proposition 2.2. *A set $A \subseteq \mathbb{N}$ is c. e. if and only if is it Σ^0_1.*

Before describing some other important classes of degrees which will play a role below, we first give a couple of examples of how degrees and the arithmetical hierarchy can be used to describe the complexity of ideals in rings. Notice that if R is a computable ring, then every finitely generated ideal of R is c. e. and so has degree at most $\mathbf{0}'$. In particular, if R is a computable Noetherian ring, then every ideal of R is c. e. and so has degree at most $\mathbf{0}'$.

Friedman, Simpson, and Smith [3, 4] showed that $\mathbf{0}'$ exactly captures the degree where you need to look in order to ensure that you can find a maximal ideal.

Theorem 2.3 (Friedman, Simpson, Smith [3, 4]).

(1) *Suppose that R is a computable ring. Then there exists a maximal ideal M of R such that* $\deg(M) \leq \mathbf{0}'$.

(2) *There is computable local ring R such that* $\deg(M) = \mathbf{0}'$ *for the unique maximal ideal M of R.*

One combinatorial principle which often plays an important role in understanding the effectiveness of certain mathematical objects is König's Lemma about infinite trees. We collect here the important facts that we'll need.

Definition 2.4. *We use $2^{<\mathbb{N}}$ to denote the set of all finite sequences of 0's and 1's, partially ordered by the initial substring relation $\subseteq$.*

Definition 2.5.

(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) *If T is a tree and $S \subseteq T$ is also a tree, we say that S is a* subtree *of T.*

(3) *A* branch *of a tree T is a function $f \colon \mathbb{N} \to \{0, 1\}$ such that $f \upharpoonright n \in T$ for all $n \in \omega$ (where $f \upharpoonright n$ is the finite sequence of the first n values of f).*

Proposition 2.6 (Weak König's Lemma). *Every infinite subtree of $2^{<\mathbb{N}}$ has an infinite branch.*

One important fact about Weak König's Lemma is that it does not hold effectively. That is, we have the following proposition.

Proposition 2.7. *There exists an infinite computable subtree of* $2^{<\mathbb{N}}$ *with no infinite computable branch.*

To codify the degrees which are able to find solutions to Weak König's Lemma, we introduce the following definition.

Definition 2.8 (Simpson). *Let* $\mathbf{a}$ *and* $\mathbf{b}$ *be Turing degrees. We write* $\mathbf{a} \gg \mathbf{b}$ *to mean that every infinite* $\mathbf{b}$*-computable subtree of* $2^{<\mathbb{N}}$ *has an infinite* $\mathbf{a}$*-computable branch.*

By Proposition 2.7, it follows that $\mathbf{0} \not\gg \mathbf{0}$. Building on Kreisel's Basis Theorem, which states that $\mathbf{0}' \gg \mathbf{0}$, Jockusch and Soare [6] proved the following result which implies that there are degrees strictly below $\mathbf{0}'$ that suffice to find branches through infinite computable trees.

Theorem 2.9 (Low Basis Theorem - Jockusch, Soare [6]). *There exists* $\mathbf{a} \gg \mathbf{0}$ *such that* $\mathbf{a}' = \mathbf{0}'$.

Roughly speaking, the fundamental characteristic of prime ideals, which is that whenever $a \cdot b \in P$ we have either $a \in P$ or $b \in P$, is similar to having a choice in the branching of a tree. Building on this analogy, we have the following theorem about prime ideals.

Theorem 2.10 (Friedman, Simpson, Smith [3, 4]).

(1) *Suppose that* R *is a computable ring and that* $\mathbf{d} \gg \mathbf{0}$. *Then there exists a prime ideal* P *of* R *such that* $\deg(P) \leq \mathbf{d}$.

(2) *There is computable ring* R *such that* $\deg(P) \gg \mathbf{0}$ *for all prime ideals* P *of* R.

Instead of working with trees directly in the arguments below, it will be simpler to work with c. e. sets and the following equivalent characterization of degrees $\mathbf{a} \gg \mathbf{0}$.

Proposition 2.11. *Suppose that* $\mathbf{a}$ *is a degree. The following are equivalent.*

(1) $\mathbf{a} \gg \mathbf{0}$.

(2) *Whenever* $A, B \subseteq \mathbb{N}$ *are disjoint c. e. sets, there exists an* $\mathbf{a}$*-computable set* C *such that* $A \subseteq C$ *and* $B \cap C = \emptyset$ *(we call* C *a* separator *for* A *and* B*).*

In fact, there are c. e. sets which have the property that if a degree $\mathbf{a}$ is able to computable a separator for them, then $\mathbf{a}$ can compute a separator for all such pairs of c. e. sets.

Proposition 2.12. *There exists disjoint c. e. sets* $A, B \subseteq \mathbb{N}$ *such that whenever* C *is a set with* $A \subseteq C$ *and* $B \cap C = \emptyset$*, we have* $\deg(C) \gg \mathbf{0}$.

2.2. **Reverse Mathematics.** We refer the reader to Simpson [21] as the standard reference for reverse mathematics. In this context, we work with a weak base system RCA_0 (which stands for Recursive Comprehension Axiom) which consists of the discretely ordered semiring axioms for $\mathbb{N}$, together with Δ^0_1-comprehension and Σ^0_1-induction. Proofs which only involve "effective" constructions and verifications can often be carried out in RCA_0. For example, the standard proofs of the following proposition easily go through in RCA_0.

Proposition 2.13. *The following are provable in* RCA_0.

(1) *If a ring R is a field, then it has no nontrivial proper ideals.*
(2) *If I is an ideal of R such that R/I is a field, then I is maximal.*

If we add the formal statement that for every set X, the set X' exists, then we get the system ACA_0 (which stands for Arithmetical Comprehension Axiom). Since X' is not computable for computable sets X, it follows that ACA_0 is strictly stronger than the system RCA_0. Also, by the computability-theoretic results above, it follows that the statement of Weak König's Lemma is not provable in RCA_0. The system WKL_0 consists of RCA_0 together with the statement of Weak König's Lemma. Making use of the Low Basis Theorem, one can show that WKL_0 lies strictly between RCA_0 and ACA_0. By a careful analysis of the arguments in Proposition 2.3 and Proposition 2.10, one arrives at the following theorems.

Theorem 2.14 (Friedman, Simpson, Smith [3, 4]).

(1) *Over* RCA_0*, the statement "Every ring has a maximal ideal" is equivalent to* ACA_0.
(2) *Over* RCA_0*, the statement "Every ring has a prime ideal" is equivalent to* WKL_0.

2.3. **Building Computable Rings.** Typical rings such as $\mathbb{Z}$ and $\mathbb{Q}[x]$ come equipped with natural representations as computable rings. Using such representations of standard rings, we can construct interesting examples of computable rings by taking subrings and quotient rings in two different ways.

We first consider subrings. Suppose that A is an infinite computable ring. If S is a computable subset of A which is a subring, then we certainly can view S as a computable ring in its own right. However, suppose more generally that S is an infinite c. e. subset of A which is a subring. Even in this more general setting, we may realize the subring S as a computable ring R in the following way. Since S is an infinite c. e. subset of A, there exists a computable bijective function $h\colon \mathbb{N} \to S$. Let R be the computable ring obtained by letting the universe be $\mathbb{N}$, letting $0_R = h^{-1}(0_A)$ and $1_R = h^{-1}(1_A)$, letting $a +_R b = h^{-1}(h(a) +_A h(b))$, and letting $a \cdot_R b = h^{-1}(h(a) \cdot_A h(b))$. Notice that $h\colon R \to S$ is a computable isomorphism.

We next consider quotients. Suppose that A is a computable ring and J is computable subset of A which is an ideal. We may realize the quotient ring A/J as a computable ring in the following way. Let R be the set of minimal elements (with respect to the ordering on $\mathbb{N}$) of cosets of J in A, and notice that R is computable. Define a computable function $h\colon A \to R$ by letting $h(a)$ be the unique element of R such that $a - h(a) \in J$. Make R into a computable ring by letting $0_R = h(0_A)$ and $1_R = h(1_A)$, letting $a +_R b = h(a +_A b)$ and letting $a \cdot_R b = h(a \cdot_A b)$. Notice that this makes R into a computable ring and as such h is a computable surjective homomorphism with kernel J.

3. Finding Nontrivial Proper Ideals

Returning to our original question of whether we can effectively detect ideals in computable rings which are not fields, we have the following simple upper bound.

Proposition 3.1. *Suppose that R is a computable ring which is not a field, and that $\mathbf{d} \gg \mathbf{0}$. Then there exists a nontrivial proper ideal I of R such that* $\deg(I) \leq \mathbf{d}$.

Proof. We may assume that 0_R and 1_R are the numbers 0 and 1. Fix $a \in R$ with $a \neq 0$ such that a is not a unit. Let $T \subseteq 2^{<\mathbb{N}}$ be the set of all σ such that

- $\sigma(0) = 1$ if $|\sigma| > 0$.
- $\sigma(1) = 0$ if $|\sigma| > 1$.
- $\sigma(a) = 1$ if $|\sigma| > a$.
- For any $b, c \in R$, if $\sigma(b) = \sigma(c) = 1$ and $b +_R c < |\sigma|$, then $\sigma(b +_R c) = 1$.
- For any $b \in R$, if $\sigma(b) = 1$, $r < |\sigma|$, and $r \cdot_R b < |\sigma|$, then $\sigma(r \cdot_R b) = 1$.

Notice that T is a computable subtree of $2^{<\mathbb{N}}$. Furthermore, T is infinite since the characteristic function of the ideal (a) i sin finite branch of T. Hence, T has an infinite $\mathbf{d}$-computable branch, coding an ideal I of R. It follows that there exists a nontrivial proper ideal I of R such that $\deg(I) \leq \mathbf{d}$. □

Our main result here is that there is a computable ring R (in fact, an integral domain), which is not a field, for which the crude upper bound on the complexity of nontrivial proper ideals is achieved. The rough idea of the construction is as follows. Fix the c. e. sets A and B

from Proposition 2.12 and computable functions $\alpha, \beta \colon \mathbb{N} \to \mathbb{N}$ such that $A = \operatorname{ran}(\alpha)$ and $B = \operatorname{ran}(\beta)$. Build a computable ring R with distinguished elements x_n for each $n \in \mathbb{N}$, and attempt to satisfy the following requirements:

(1) For all $r \in R$ with $r \neq 0$, we have $r \mid x_{\alpha(n)}$ for all $n \in \mathbb{N}$.
(2) For all $r \in R$ with $r \neq 0$, we have $r \mid (x_{\beta(n)} - 1)$ for all $n \in \mathbb{N}$.

If we are successful, then any nontrivial proper ideal must contain $x_{\alpha(n)}$ for each $n \in \mathbb{N}$ and must not contain $x_{\beta(n)}$ for every $n \in \mathbb{N}$ (because otherwise it would contain 1). Thus, from a nontrivial proper ideal we could compute a separator for A and B.

The simplest setting to put this idea into practice is to work in the field of fractions F of $\mathbb{Z}[\overline{x}] = \mathbb{Z}[x_1, x_2, \dots]$. It suffices to give a c. e. subring of F by the construction outlined in Section 2.3. Thus, the idea is to let S be the subring of F generated by

$$\mathbb{Z}[\overline{x}] \cup \{\frac{x_{\alpha(i)}}{p} : i \in \mathbb{N}, p \in \mathbb{Z}[\overline{x}] - \{0\}\} \cup \\ \{\frac{x_{\beta(j)} - 1}{q} : j \in \mathbb{N}, q \in \mathbb{Z}[\overline{x}] - \{0\}\}$$

Since the above set of generators is c. e., S will also be c. e. However, a simple argument shows that $S = F$, so S is a field.

Therefore, a balancing act is needed here, which is to introduce enough divisibilities in the above strategy to encode what we need into the ideals, while ensuring that we don't introduce too many to collapse S into a field. The modification needed is to relax the above requirements to the following requirements:

(1) For all $r \in R$ with $r \neq 0$, we have $r \mid x_{\alpha(n)}$ for all but finitely many $n \in \mathbb{N}$.
(2) For all $r \in R$ with $r \neq 0$, we have $r \mid (x_{\beta(n)} - 1)$ for all but finitely many $n \in \mathbb{N}$.

Finite sets don't affect what is encoded into ideals, and by relaxing the divisibility conditions we can ensure that the ring constructed is not a field.

Theorem 3.2. *There is a computable integral domain R which is not a field such that $\deg(I) \gg \mathbf{0}$ for all nontrivial proper ideals I of R.*

Proof. Fix the c. e. sets A and B from Proposition 2.12 and computable functions $\alpha, \beta \colon \mathbb{N} \to \mathbb{N}$ such that $A = \operatorname{ran}(\alpha)$ and $B = \operatorname{ran}(\beta)$. Let F be the fraction field of $\mathbb{Z}[\overline{x}] = \mathbb{Z}[x_1, x_2, \dots]$. We build a computable ring R by giving a c. e. subset S of F and using the construction in Section 2.3. For each $n \in \mathbb{N}$, let $\mathbb{Z}[\overline{x}]_n$ be the subring of $\mathbb{Z}[\overline{x}]$ consisting of those elements f with $i < n$ for all x_i occurring in f. Let

$$A = \{\frac{x_{\alpha(i)}}{p} : i \in \mathbb{N}, p \in \mathbb{Z}[\overline{x}]_{\alpha(i)} - \{0\}\}$$

and let

$$B = \{\frac{x_{\beta(j)} - 1}{q} : j \in \mathbb{N}, q \in \mathbb{Z}[\overline{x}]_{\beta(j)} - \{0\}\}$$

Notice that A and B are c. e. subsets of F. Let S be the subring of F generated by $\mathbb{Z}[\overline{x}] \cup A \cup B$. Since

$$g_1 \cdot \frac{x_{\alpha(i)}}{p_1} + g_2 \cdot \frac{x_{\alpha(i)}}{p_2} = (g_1p_2 + g_2p_1) \cdot \frac{x_{\alpha(i)}}{p_1p_2}$$

and

$$h_1 \cdot \frac{x_{\beta(j)} - 1}{p_1} + h_2 \cdot \frac{x_{\beta(j)} - 1}{p_2} = (h_1p_2 + h_2p_1) \cdot \frac{x_{\beta(j)} - 1}{p_1p_2}$$

it follows that

$$S = \{f + \sum_{i \in I} g_i \cdot \frac{x_{\alpha(i)}}{p_i} + \sum_{j \in J} h_j \cdot \frac{x_{\beta(j)} - 1}{q_j} : I, J \subseteq \mathbb{N} \text{ are finite,}$$
$$f, g_i, h_j \in \mathbb{Z}[\overline{x}], p_i \in \mathbb{Z}[\overline{x}]_{\alpha(i)} - \{0\}, q_j \in \mathbb{Z}[\overline{x}]_{\beta(j)} - \{0\}\}$$

We first claim that S is not a field. Fix $k \notin A \cup B$. We show that $\frac{1}{x_k} \notin S$. Suppose instead that $\frac{1}{x_k} \in S$ and write

$$\frac{1}{x_k} = f + \sum_{i \in I} g_i \cdot \frac{x_{\alpha(i)}}{p_i} + \sum_{j \in J} h_j \cdot \frac{x_{\beta(j)} - 1}{q_j}$$

where I and J are finite and $|I \cup J|$ is minimal. Notice that since $\frac{1}{x_k} \notin \mathbb{Z}[\overline{x}]$, we have $|I \cup J| \geq 1$. Let $m = \max(\{\alpha(i) : i \in I\} \cup \{\beta(j) : j \in J\})$ and notice that $p_i \in \mathbb{Z}[\overline{x}]_m$ for all $i \in I$ and $q_j \in \mathbb{Z}[\overline{x}]_m$ for all $j \in J$.

Let $p = \prod_{i \in I} p_i$ and let $q = \prod_{j \in J} q_j$. For each $i \in I$, let $\hat{p}_i = \frac{p}{p_i} \in \mathbb{Z}[\overline{x}]$, and for each $j \in J$, let $\hat{q}_j = \frac{q}{q_j} \in \mathbb{Z}[\overline{x}]$. Multiplying through by pqx_k, notice that in $\mathbb{Z}[\overline{x}]$ we have

$$pq = x_k(fpq + \sum_{i \in I} g_i x_{\alpha(i)} \hat{p}_i q + \sum_{j \in J} h_j (x_{\beta(j)} - 1) p \hat{q}_j)$$

Case 1: Suppose that $m = \alpha(i_0)$ for some $i_0 \in I$. Let $\varphi \colon \mathbb{Z}[\overline{x}] \to \mathbb{Z}[\overline{x}]$ be the homomorphism induced by sending x_m to 0 and fixing all other x_n. Notice that $\varphi(p_i) = p_i$ for all $i \in I$ and $\varphi(q_j) = q_j$ for all $j \in J$ because $p_i, q_j \in \mathbb{Z}[\overline{x}]_m$. Thus, by applying φ, we have

$$pq = x_k(\varphi(f)pq + \sum_{i \in I - \{i_0\}} \varphi(g_i) x_{\alpha(i)} \hat{p}_i q + \sum_{j \in J} \varphi(h_j)(x_{\beta(j)} - 1) p \hat{q}_j)$$

and hence

$$\frac{1}{x_k} = \varphi(f) + \sum_{i \in I - \{i_0\}} \varphi(g_i) \cdot \frac{x_{\alpha(i)}}{p_i} + \sum_{j \in J} \varphi(h_j) \cdot \frac{x_{\beta(j)} - 1}{q_j}$$

This is a contradiction because $|(I - \{i_0\}) \cup J| < |I \cup J|$.

Case 2: Suppose that $m = \beta(j_0)$ for some $j_0 \in J$. Let $\varphi\colon \mathbb{Z}[\overline{x}] \to \mathbb{Z}[\overline{x}]$ be the homomorphism induced by sending x_m to 1 and fixing all other x_n. Notice that $\varphi(p_i) = p_i$ for all $i \in I$ and $\varphi(q_j) = q_j$ for all $j \in J$ because $p_i, q_j \in \mathbb{Z}[\overline{x}]_m$. Thus, by applying φ, we have

$$pq = x_k(\varphi(f)pq + \sum_{i \in I} \varphi(g_i)x_{\alpha(i)}\hat{p}_i q + \sum_{j \in J - \{j_0\}} \varphi(h_j)(x_{\beta(j)} - 1)p\hat{q}_j)$$

and hence

$$\frac{1}{x_k} = \varphi(f) + \sum_{i \in I} \varphi(g_i) \cdot \frac{x_{\alpha(i)}}{p_i} + \sum_{j \in J - \{j_0\}} \varphi(h_j) \cdot \frac{x_{\beta(j)} - 1}{q_j}$$

This is a contradiction because $|I \cup (J - \{j_0\})| < |I \cup J|$.

Let R be the computable ring with universe $\mathbb{N}$ and $h\colon R \to S$ be the computable isomorphism described in Section 2.3. Suppose that I is a nontrivial proper ideal of R and fix $a \in I$ with $a \neq 0$. Notice that $h(I)$ is a nontrivial proper ideal of S. Fix $f, g \in \mathbb{Z}[\overline{x}]$ with $\frac{f}{g} = h(a)$. Since $h(I)$ is an ideal of S and $g \in S$, it follows that $f \in h(I)$. Fix $\ell \in \mathbb{N}$ such that $f \in \mathbb{Z}[\overline{x}]_\ell$. Let

$$D = \{k \in \mathbb{N} : h^{-1}(x_k) \in I\}$$

and notice that $D \leq_T I$. We now show that $\alpha(n) \in D$ for all $n \in \mathbb{N}$ with $\alpha(n) \geq \ell$ and that $\beta(n) \notin D$ for all $n \in \mathbb{N}$ with $\beta(n) \geq \ell$. Fix $n \in \mathbb{N}$ with $\alpha(n) \geq \ell$. We then have that $\frac{x_{\alpha(n)}}{f} \in S$, hence $x_{\alpha(n)} \in h(I)$ because $h(I)$ is an ideal of S, and so $\alpha(n) \in D$. We also have that $\frac{x_{\beta(n)}-1}{f} \in S$, hence $x_{\beta(n)} - 1 \in h(I)$, so $x_{\beta(n)} \notin h(I)$ because $h(I)$ is a proper ideal of S, and so $\beta(n) \notin D$. □

As a corollary, we get the existence of a computable ring in which every nontrivial proper finitely generated ideal is as complicated as the crude upper bound of $\mathbf{0}'$.

Corollary 3.3. *There is a computable integral domain R which is not a field such that* $\deg(I) = \mathbf{0}'$ *for all nontrivial proper finitely generated ideals I of R.*

Proof. Let R be the integral domain from above. Suppose that I is a nontrivial proper finitely generated ideal of R. Notice that I is c. e.

Since $\deg(I) \gg \mathbf{0}$, it follows by the Arslanov Completeness Criterion (see, e.g., Soare [22]) that $\deg(I) = \mathbf{0}'$. □

By working carefully in RCA_0, we can translate this result into reverse mathematics. In this context, we define a maximal ideal M in the natural way (i.e., that there is no proper ideal between M and R), rather than using the definition in Simpson that R/M is a field.

Proposition 3.4. *Over* RCA_0, *the following are equivalent to* WKL_0.

(1) *If a ring R has no nontrivial proper ideals, then it is a field.*
(2) *If I is a maximal ideal of R, then R/I is a field*

Proof. Notice first that (1) and (2) are provably equivalent in RCA_0 because the correspondence theorem for ideals in quotients can be proved in RCA_0.

We work in WKL_0 and prove (1). We may assume that 0_R and 1_R are the numbers 0 and 1. Fix $a \in R$ with $a \neq 0$ such that a is not a unit. Let $T \subseteq 2^{<\mathbb{N}}$ be the set of all σ such that

- $\sigma(0) = 1$ if $|\sigma| > 0$.
- $\sigma(1) = 0$ if $|\sigma| > 1$.
- $\sigma(a) = 1$ if $|\sigma| > a$.
- If $\sigma(b) = 1$, $\sigma(c) = 1$, and $b +_R c < |\sigma|$, then $\sigma(b +_R c) = 1$.
- If $\sigma(b) = 1$, $r < |\sigma|$, and $r \cdot_R b < |\sigma|$, then $\sigma(r \cdot_R b) = 1$.

Notice that T is a subtree of $2^{<\mathbb{N}}$ which exists by Δ^0_1-comprehension. If we could argue that T is infinite, then we may use Weak König's Lemma to get a branch, and from this branch obtain a nontrivial proper ideal. Of course, classically T is infinite because there is a nontrivial proper ideal (as in the proof of Proposition 3.1), but we certainly can't use that in our proof here.

Instead, we argue that T is infinite as in the argument in Simpson [21] that WKL_0 proves that every ring has a prime ideal: We define sets X_n for $n \in \mathbb{N}$ by primitive recursion as follows. Let $X_0 = \{0, a\}$. Given X_n, write $n = 2 \cdot \langle i, j, k \rangle + d$ where $\langle \cdot, \cdot, \cdot \rangle$ is a bijective function coding triples and $d \in \{0, 1\}$, and act as follows.

- Suppose that $d = 0$. If $i, j \in X_n$, let $X_{n+1} = X_n \cup \{i +_R j\}$ and otherwise let $X_{n+1} = X_n$.
- Suppose that $d = 1$. If $j \in X_n$, let $X_{n+1} = X_n \cup \{i \cdot_R j\}$ and otherwise let $X_{n+1} = X_n$.

By Σ^0_1-induction, it follows that 1 is not in the ideal generated by X_n for all $n \in \mathbb{N}$.

We now show that T is infinite. Suppose that $m \in \mathbb{N}$. By bounded Σ^0_1-comprehension, we may form the set Y consisting of all $i < m$ such that $\exists n(i \in X_n)$. Now if we let $\sigma \in 2^{<\mathbb{N}}$ be the finite sequence of length m such that $\sigma(i) = 0$ if $i \notin Y$ and $\sigma(i) = 1$ if $i \in Y$, then $\sigma \in T$. Therefore, T has an element of every length, so T is infinite. As remarked above, this completes the proof.

We next show that (1) implies WKL_0 over RCA_0. We use the construction in Theorem 3.2. Suppose that $\alpha\colon \mathbb{N} \to \mathbb{N}$ and $\beta\colon \mathbb{N} \to \mathbb{N}$ are such that $\forall x \forall y(\alpha(x) \neq \beta(y))$. The subring of F that we describe can be given by a Σ^0_1 formula $\varphi(x)$, and RCA_0 can prove $\neg\varphi(\frac{1}{x_k})$ by Σ^0_1-induction. Now RCA_0 proves that if $\varphi(x)$ is a Σ^0_1-formula such that there are infinitely many n with $\varphi(n)$, then there exists an injective function $h\colon \mathbb{N} \to \mathbb{N}$ such that for all $n \in \mathbb{N}$, we have $n \in \operatorname{ran}(h)$ if and only if $\varphi(n)$. Thus, we may build the ring given by the above construction within RCA_0. From here, the rest of the argument can be carried out to show that from a proper nontrivial ideal, one can prove the existence of a separator for $\operatorname{ran}(\alpha)$ and $\operatorname{ran}(\beta)$. □

4. The Nilradical and Jacobson Radical

Proposition 4.1. *If R is a computable ring, then* $\operatorname{Nil}(R)$ *is* Σ^0_1.

Proof. We have

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

Since $\{(a,n) : a^n = 0\}$ is computable, it follows that $\operatorname{Nil}(R)$ is Σ^0_1. □

We next show that this result is optimal. In this case, we use the quotient construction and build a computable ideal of $\mathbb{Z}[\overline{x}]$. The idea here is that if we want to make the element x_k nilpotent, we need only add x_k^n for some n to the ideal we are using to take the quotient. Now we want the ideal to be computable, so if k enters our c. e. set at stage n, we add x_k^n to our ideal.

Theorem 4.2. *There exists a computable ring R such that* $\operatorname{Nil}(R)$ *is* Σ^0_1*-complete.*

Proof. Fix a Σ^0_1-complete c. e. set A and a computable function $\alpha\colon \mathbb{N} \to \mathbb{N}$ such that $A = \operatorname{ran}(\alpha)$. We build a computable ring R such that $A \leq_1 \operatorname{Jac}(R)$ (see Odifreddi [11, 12] or Soare [22] for the definition of $\leq_1$). Let J be the ideal of $\mathbb{Z}[\overline{x}]$ generated by

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

Notice that a polynomial $f \in \mathbb{Z}[\overline{x}]$ is in J if and only if every nonzero monomial summand of f has a factor x_i^m such that there exists $n \leq m$ with $\alpha(n) = i$. In particular, J is a computable ideal. Let R be the computable quotient ring together with the computable homomorphism $h\colon \mathbb{Z}[\overline{x}] \to R$ as described in Section 2.3. Define $\theta\colon \mathbb{N} \to R$ by letting $\theta(k) = h(x_k)$ for all $k \in \mathbb{N}$. Since h is a homomorphism with kernel J, we have that $\theta(k) = h(x_k) \in \mathrm{Nil}(R)$ if and only if $x_k^n \in J$ for some $n \in \mathbb{N}$. Thus,

(1) If $k \in A$, say $k = \alpha(n)$, then $x_k^n \in J$, so $\theta(k) \in \mathrm{Nil}(R)$.
(2) If $k \notin A$, then $\theta(k) \notin \mathrm{Nil}(R)$ because $x_k^n \notin J$ for all $n \in \mathbb{N}$.

It follows that $A \leq_1 \mathrm{Nil}(R)$. □

We turn now to the Jacobson radical.

Proposition 4.3. *If R is a computable ring, then* $\mathrm{Jac}(R)$ *is* Π^0_2.

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

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

Since $\{(a,b,c) : (ab+1)c = 1\}$ is computable, it follows that $\mathrm{Jac}(R)$ is Π^0_2. □

We next show that this result is optimal. In this case, we use the subring construction. The idea is to encode a standard Π^0_2-complete set, such as $\mathrm{Inf} = \{k \in \mathbb{N} : W_k \text{ is infinite}\}$ (where W_k is the k^{th} c. e. set in some standard enumeration) into the Jacobson radical of a ring. We thus want to build a computable ring R with distinguished elements x_n for each $n \in \mathbb{N}$, and attempt to satisfy the following requirements:

(1) For all $k \in \mathrm{Inf}$, we have that $x_k \cdot r + 1$ is a unit for all $r \in R$.
(2) For all $k \notin \mathrm{Inf}$, there exists $r \in R$ such that $x_k \cdot r + 1$ is not a unit.

The idea then is to work in a ring like $\mathbb{Z}[\overline{x}]$, and as we see more and more elements enter W_k, we put $\frac{1}{x_k \cdot p + 1}$ into S for more and more polynomials p. In order to avoid contamination between these requirements, it's helpful to have another stock of variables which gauges how many polynomials p we've put to work for x_k.

Theorem 4.4. *There exists a computable integral domain R such that* $\mathrm{Jac}(R)$ *is Π^0_2-complete.*

Proof. Recall that $\mathrm{Inf} = \{k \in \mathbb{N} : W_k \text{ is infinite}\}$ is Π^0_2-complete. Let F be the fraction field of $\mathbb{Z}[\overline{x}, \overline{y}] = \mathbb{Z}[x_1, x_2, \ldots, y_1, y_2, \ldots]$. We build a computable ring R such that $\mathrm{Inf} \leq_1 \mathrm{Jac}(R)$ by giving a c. e. subset S of F and using the construction in Section 2.3. For each $n \in \mathbb{N}$, let

$\mathbb{Z}[\overline{x},\overline{y}]_n$ be the subring of $\mathbb{Z}[\overline{x},\overline{y}]$ consisting of those elements p with $i < n$ for all y_i occurring in p. Also, let $\mathbb{Z}[\overline{x},\overline{y}]_\infty = \mathbb{Z}[\overline{x},\overline{y}]$. Let

$$M = \{1 + \sum_{i=1}^{n} x_i p_i : p_i \in \mathbb{Z}[\overline{x},\overline{y}]_{|W_i|} : i, n \in \mathbb{N}\}$$

Notice that M is a multiplicative subset of $\mathbb{Z}[\overline{x},\overline{y}]$ (and that $1 \in M$). Let

$$S = M^{-1}\mathbb{Z}[\overline{x},\overline{y}] = \{\frac{f}{m} : f \in \mathbb{Z}[\overline{x},\overline{y}], m \in M\} \subseteq F$$

and notice that S is c. e.

Suppose first that $k \in \mathrm{Inf}$ so that W_k is infinite. Let $\frac{f}{m} \in S$ and fix $p_i \in \mathbb{Z}[\overline{x},\overline{y}]_{|W_i|}$ such that $m = 1 + \sum_{i=1}^{n} x_i p_i$. Notice that

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

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

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

so $x_k \cdot \frac{f}{m} + 1$ is a unit in S. Therefore, $x_k \in \mathrm{Jac}(S)$.

Suppose now that $k \notin \mathrm{Inf}$ so that W_k is finite. Fix $\ell > |W_k|$. We claim that $x_k y_\ell + 1$ is not a unit in S. If $x_k y_\ell + 1$ is a unit in S, then there exist $p_i \in \mathbb{Z}[\overline{x},\overline{y}]_{|W_i|}$ such that

$$\frac{1}{x_k y_\ell + 1} = \frac{f}{1 + \sum_{i=1}^{n} x_i p_i}$$

which gives

$$1 + \sum_{i=1}^{n} x_i p_i = f \cdot (x_k y_\ell + 1)$$

Let $\varphi\colon \mathbb{Z}[\overline{x},\overline{y}] \to \mathbb{Z}[\overline{x},\overline{y}]$ be the homomorphism induced by fixing x_k and y_ℓ, and sending all other x_i and y_j to 0. We then have that

$$1 + x_k \cdot \varphi(p_k) = \varphi(f) \cdot (x_k y_\ell + 1)$$

Now $\varphi(f) \neq 0$ (because the left-hand side is nonzero), so the right-hand side has positive y_ℓ-degree. However, the left-hand side has y_ℓ-degree 0 because $p_k \in \mathbb{Z}[\overline{x},\overline{y}]_{|W_k|} \subseteq \mathbb{Z}[\overline{x},\overline{y}]_\ell$, so we have a contradiction. It follows that $x_k y_\ell + 1$ is not a unit in S, hence $x_k \notin \mathrm{Jac}(S)$.

Let R be the computable ring with universe $\mathbb{N}$ and $h\colon R \to S$ be the computable isomorphism described in Section 2.3. Define $\theta\colon \mathbb{N} \to R$ by letting $\theta(k) = h^{-1}(x_k)$ for all $k \in \mathbb{N}$. Since $h\colon R \to S$ is a computable isomorphism, we have that θ is computable and that

$$\begin{aligned} k \in \mathrm{Inf} &\Leftrightarrow x_k \in \mathrm{Jac}(S) && \text{(from above)} \\ &\Leftrightarrow \theta(k) = h^{-1}(x_k) \in \mathrm{Jac}(R) \end{aligned}$$

It follows that Inf $\leq_1$ Jac(R). □

References

[1] Baumslag, G., F. Cannonito, and C. Miller III, *Computable algebra and group embeddings,* J. Algebra, **69** (1981), 186-212.

[2] Downey, Rodney G.; Hirschfeldt, Denis R.; Kach, Asher M.; Lempp, Steffen; Mileti, Joseph R.; and Montalbán, Antonio, *Subspaces of computable vector spaces*, to appear.

[3] Friedman, Harvey M.; Simpson, Stephen G.; and Smith, Rick L., *Countable algebra and set existence axioms,* Ann. Pure Appl. Logic **25** (1983), 141–181.

[4] Friedman, Harvey M.; Simpson, Stephen G.; and Smith, Rick L., *Addendum to: "Countable algebra and set existence axioms"*, Ann. Pure Appl. Logic **28** (1985), 319–320.

[5] Frölich, A. and J. Shepherdson, *Effective procedures in field theory,* Phil. Trans. Royal Soc. London Ser. A., **248** (1956), 407-432.

[6] Jockusch, Carl G., Jr. and Soare, Robert I., Π^0_1 *classes and degrees of theories,* Trans. Amer. Math. Soc. **173** (1972), 33–56.

[7] Mal'cev, A., *Constructive algebra I,* Russian Math. Surveys, **16** (1961), 77-129.

[8] Metakides, G. and A. Nerode, *Effective content of field theory,* Ann. Math. Logic, **17** (1979), 289-320.

[9] Metakides, G. and A. Nerode, *Recursion theory on fields and abstract dependence,* J. Algebra, **65** (1980), 36-59

[10] Metakides, G. and A. Nerode, *The introduction of non-recursive methods into mathematics,* in *The L. E. J. Brouwer Centenary Symposium,* (Ed. A Troelstra and D. van Dalen), North-Holland, Amsterdam, (1982) 319-335.

[11] Odifreddi, Piergiorgio, *Classical recursion theory,* North-Holland, Amsterdam, 1989.

[12] Odifreddi, Piergiorgio, *Classical recursion theory, Vol. II,* North-Holland, Amsterdam, 1999.

[13] Rabin, M. O., *Computable algebra, general theory and theory of computable fields,* Trans. Amer. Math. Soc., **95**, (1960), 341–360.

[14] Richman, F. *Constructive aspects of Noetherian rings,* Proc. Amer. Math. Soc., **44** (1974), 436-441.

[15] Seidenberg, A., *Constructions in algebra,* Trans. Amer. Math. Soc. **197** (1974), 273-313.

[16] Seidenberg, A. *Constructions in a polynomial ring over the ring of integers,* American J. Math., **100** (1978), 685-703.

[17] Shlapentokh, A. *Algebraic and Turing Separability of Rings,* Journal of Algebra, **185** (1996), 229-257

[18] Stolenberg-Hansen, V. and J. Tucker, *Computing roots of unity in fields,* Bull. London Math. Soc., **12** (1980), 463-471.

[19] Stolenberg-Hansen, V. and J. Tucker, *Complete local rings as domains,* J. Symb. Logic, **53** (1988), 603-624.

[20] Stolenberg-Hansen, V. and J. Tucker, *Computable rings and fields,* in *Handbook of Computability Theory* (Ed. E. Griffor) North-Holland, 1999, 336-447.

[21] Simpson, Stephen G., *Subsystems of Second Order Arithmetic*, Springer-Verlag, Berlin, 1999.

[22] Soare, Robert I., *Recursively enumerable sets and degrees*, Springer-Verlag, Berlin, New York, 1987.

Department of Mathematics, Victoria University, P. O. Box 600, Wellington, NEW ZEALAND
E-mail address: Rod.Downey@mcs.vuw.ac.nz

Department of Mathematics, University of Wisconsin, Madison, WI 53706-1388, USA
E-mail address: lempp@math.wisc.edu

Department of Mathematics, University of Chicago, Chicago, IL 60637-1514, USA
E-mail address: mileti@math.uchicago.edu