Notre Dame Journal of Formal Logic
Volume 59, Number 2, 2018

The Complexity of Primes in Computable Unique Factorization Domains

Damir D. Dzhafarov and Joseph R. Mileti

Abstract In many simple integral domains, such as $\mathbb{Z}$ or $\mathbb{Z}[i]$, there is a straightforward procedure to determine if an element is prime by simply reducing to a direct check of finitely many potential divisors. Despite the fact that such a naive approach does not immediately translate to integral domains like $\mathbb{Z}[x]$ or the ring of integers in an algebraic number field, there still exist computational procedures that work to determine the prime elements in these cases. In contrast, we will show how to computably extend $\mathbb{Z}$ in such a way that we can control the ordinary integer primes in any Π^0_2 way, all while maintaining unique factorization. As a corollary, we establish the existence of a computable unique factorization domain (UFD) such that the set of primes is Π^0_2-complete in every computable presentation.

1 Introduction

The power and versatility of modern algebra arise from the abstract and axiomatic approach it takes. However, with the rise of computer algebra systems, it is important to find algorithms in order to perform computations within these algebraic structures. Of course, in these settings, one also cares about the efficiency of these procedures. For example, although the primes in $\mathbb{Z}$ are trivially computable, there is a great deal of interest in how quickly we can determine whether an element is prime (see Crandall and Pomerance [6] for a general overview of techniques). In contrast, it is known that there are computable integral domains where it is impossible even in principle to determine the primes computationally. In this article, we extend these examples to build a computable unique factorization domain (UFD) where the primes are maximally complicated in a very strong sense. We begin with the following definition

Received November 19, 2014; accepted August 20, 2015
First published online February 27, 2018
2010 Mathematics Subject Classification: Primary 03C57, 03D45; Secondary 13F15, 13L05
Keywords: computable unique factorization domains, computability theory, primes
 10.1215/00294527-2017-0024

(see Soare [18] for background on the formal definitions of computable sets and functions).

Definition 1.1 A *computable ring* is a ring whose underlying set is a computable set $A \subseteq \mathbb{N}$, with the property that $+$ and $\cdot$ are computable functions from $A \times A$ to A.

For example, it is easy to view $\mathbb{Z}$ as a computable ring by using the even natural numbers to code the positive elements in ascending order and the odd natural numbers to code the negative elements in descending order. Of course, we can view $\mathbb{Z}$ as a computable ring in a different way by switching the roles of the evens and odds. Thus, a given ring can have multiple distinct computable *presentations*. Many other natural rings can also be viewed as computable rings. Since we can code relatively prime pairs of natural numbers by using a single natural number, we can view $\mathbb{Q}$ as a computable ring. Similarly, since we can code finite sequences of integers as natural numbers, we can view $\mathbb{Z}[x]$ as a computable ring as well. Generalizing this, given an arbitrary computable ring A, we can realize the polynomial ring $A[x]$ as a computable ring in a natural way. In contrast, uncountable rings can never be viewed as computable rings, and there are some countable rings that cannot be as well.

For a general overview of results about computable rings and fields, see Stoltenberg-Hansen and Tucker [19]. Computable fields have received a great deal of attention (see Frölich and Shepherdson [11], Metakides and Nerode [14], and Rabin [17]), and Miller [15] provides an excellent overview of work in this area. For computable rings, several papers (see Conidis [4], Downey, Lempp, and Mileti [8], and Friedman, Simpson, and Smith [10]) have studied the complexity of ideals and radicals from the perspective of computability theory and reverse mathematics. For information about practical algorithms to perform important computations in algebraic number theory (such as in number fields and function fields), see Cohen [2], [3], Klüners [12], and Müller-Quade and Steinwandt [16]. For some recent work on the complexity of finding a Euclidean function for a computable Euclidean domain, see Downey and Kach [7].

The following algebraic definitions are standard.

Definition 1.2 Let A be an integral domain, that is, a commutative ring with $1 \neq 0$ and with no zero divisors (so $ab = 0$ implies either $a = 0$ or $b = 0$). Recall the following definitions.

(1) An element $u \in A$ is a *unit* if there exists $w \in A$ with $uw = 1$. We denote the set of units by $U(A)$. Note that $U(A)$ is a multiplicative group.
(2) Given $a, b \in A$, we say that a and b are *associates* if there exists $u \in U(A)$ with $au = b$. We denote the set of associates of a by $\text{Associates}_A(a)$.
(3) An element $p \in A$ is *irreducible* if it is nonzero, not a unit, and has the property that whenever $p = ab$, either a is a unit or b is a unit. An equivalent definition is that $p \in A$ is irreducible if it is nonzero, not a unit, and its divisors are precisely the units and the associates of p.
(4) An element $p \in A$ is *prime* if it is nonzero, not a unit, and has the property that whenever $p \mid ab$, either $p \mid a$ or $p \mid b$. We denote the set of primes of A by $\text{Primes}(A)$.
(5) We call A a *unique factorization domain*, or *UFD*, if it has the following two properties.
    - For each $a \in A$ such that a is nonzero and not a unit, there exist irreducible elements $r_1, r_2, \ldots, r_n \in A$ with $a = r_1 r_2 \cdots r_n$.

- If $r_1, r_2, \ldots, r_n, q_1, q_2, \ldots, q_m \in A$ are all irreducible and
$$r_1 r_2 \cdots r_n = q_1 q_2 \cdots q_m,$$
then $n = m$ and there exists a permutation σ of $\{1, 2, \ldots, n\}$ such that r_i and $q_{\sigma(i)}$ are associates for all i.

It is a simple fact that if A is an integral domain, then every prime element of A is irreducible. The converse fails in general, but is true in every UFD. In fact, we have the following standard result.

Theorem 1.3 *Let A be an integral domain. The following are equivalent:*

(1) *A is a UFD, and*
(2) *every element of A that is nonzero and not a unit is a product of irreducibles, and every irreducible element of A is prime.*

Of course, for most computable integral domains that arise in practice, the set of primes forms a computable set in any natural computable presentation. For the ring $\mathbb{Z}$, the set of primes trivially forms a computable set. Kronecker showed that the set of primes in (any reasonable computable presentation of) the UFD $\mathbb{Z}[x]$ is computable. Using Gauss's lemma and the fact that every element of $\mathbb{Q}[x]$ is an associate of an element of $\mathbb{Z}[x]$, it follows that the set of primes in $\mathbb{Q}[x]$ is computable as well. Consider a number field K with $[K : \mathbb{Q}] = n$, and let $\mathcal{O}_K$ be the set of algebraic integers in K. (For an overview of results about $\mathcal{O}_K$ and algorithms to perform computations in them, see [2, Chapter 4].) In general, $\mathcal{O}_K$ is always a Dedekind domain, but it may not be a UFD. We may fix an integral basis of K over $\mathbb{Q}$, that is, fix $b_1, b_2, \ldots, b_n \in \mathcal{O}_K$ that form a basis for K over $\mathbb{Q}$ such that

$$\mathcal{O}_K = \{m_1 b_1 + m_2 b_2 + \cdots + m_n b_n : m_i \in \mathbb{Z}\}.$$

Now given the finitely many values $b_i \cdot b_j$, we can compute the multiplication function on K and hence on $\mathcal{O}_K$ as well. Since we can simply hard-code in these values, it follows that any integral basis provides a computable presentation of the field K (by working with underlying set $\mathbb{Q}^n$) and the ring $\mathcal{O}_K$ (by working with underlying set $\mathbb{Z}^n$). We have the following fact.

Proposition 1.4 *Let K be a number field with $[K : \mathbb{Q}] = n$. If we fix an integral basis of K over $\mathbb{Q}$, and represent elements of $\mathcal{O}_K$ by using elements of $\mathbb{Z}^n$, then the set of prime elements of $\mathcal{O}_K$ is computable.*

Proof Given $\alpha \in K$, the map $\varphi_\alpha : K \to K$ defined by $\varphi_\alpha(x) = \alpha \cdot x$ is a $\mathbb{Q}$-linear map, and moreover we can uniformly compute a matrix M_α with rational entries representing this map because we need only express $\alpha \cdot b_i$ in terms of our basis. Furthermore, note that if $\alpha \in \mathcal{O}_K$, then φ_α maps $\mathcal{O}_K$ into $\mathcal{O}_K$, and hence M_α has integer entries. From this, we can conclude that the norm map $N : \mathcal{O}_K \to \mathbb{Z}$ defined by $N(\alpha) = \det(\varphi_\alpha) = \det(M_\alpha)$ is a computable function. Since an element $\alpha \in \mathcal{O}_K$ is a unit if and only if $N(\alpha) = \pm 1$, it follows that $U(\mathcal{O}_K)$ is a computable set.

Moreover, given $\alpha, \beta \in K$ with $\alpha \neq 0$ represented as elements of $\mathbb{Q}^n$, we can uniformly compute $\frac{\beta}{\alpha}$ as represented by an element of $\mathbb{Q}^n$ by simply searching through the effectively countable set $\mathbb{Q}^n$ until we find $\gamma \in K$ with $\gamma \cdot \alpha = \beta$. Now if $\alpha, \beta \in \mathcal{O}_K$, we can effectively determine if $\alpha \mid \beta$ in $\mathcal{O}_K$ by checking if this representation of $\frac{\beta}{\alpha}$ is in $\mathbb{Z}^n$. Therefore, the divisibility relation on $\mathcal{O}_K$ is computable.

Since we can compute the norm of an element, and since $|\mathcal{O}_K/\langle\alpha\rangle| = |N(\alpha)|$, we can compute the function $f\colon \mathcal{O}_K\backslash\{0\} \to \mathbb{N}$ defined by $f(\alpha) = |\mathcal{O}_K/\langle\alpha\rangle|$. Now to determine if α is prime, we compute $f(\alpha)$ and then search until we find $f(\alpha)$ many distinct representatives of the quotient (this is possible because the divisibility relation is computable). With these representatives, we can form the finite multiplicative table of the quotient (again using the fact that the divisibility relation is computable). To determine if α is prime, we then check if the quotient has any zero divisors, which is now just a finite check. □

Despite all of this, there are computable integral domains such that the set of primes is not computable. In fact, there is a computable field F such that the set of primes in $F[x]$ is not computable (see, e.g., [15, Lemma 3.4] or [19, Section 3.2]). There exist methods to measure the complexity of sets that are not computable, and we investigate the placement of such sets in the arithmetical hierarchy arising from quantifying over computable relations.

Definition 1.5 Let $Z \subseteq \mathbb{N}$.

- We say that Z is a Σ^0_1 set if there exists a computable $R \subseteq \mathbb{N}^2$ such that
$$i \in Z \iff (\exists x)R(x, i).$$
- We say that Z is a Π^0_1 set if there exists a computable $R \subseteq \mathbb{N}^2$ such that
$$i \in Z \iff (\forall x)R(x, i).$$
- We say that Z is a Π^0_2 set if there exists a computable $R \subseteq \mathbb{N}^3$ such that
$$i \in Z \iff (\forall x)(\exists y)R(x, y, i).$$

Since it is possible to computably code finite sequences of natural numbers with a single natural number, the above definitions do not change if we allow finite consecutive blocks of the same (existential or universal) quantifiers. Although every computable set is Σ^0_1, there exists a Σ^0_1 set that is not computable, such as the set of natural numbers coding programs that halt. Similarly, the collection of Σ^0_1 sets is a proper subset of the collection of all Π^0_2 sets, and the collection of Π^0_1 sets is a proper subset of the collection of all Π^0_2 sets. (See [18, Chapter 4] for more information about the arithmetical hierarchy.)

Suppose that A is a computable integral domain. We then have that $U(A)$ is a Σ^0_1 set because
$$u \in U(A) \iff (\exists w)[uw = 1],$$
and the relation $uw = 1$ is computable. The set of irreducibles of A is a Π^0_2 set because p is irreducible in A if and only if
$$p \neq 0 \wedge (\forall c)[pc \neq 1] \wedge (\forall a)(\forall b)\big[p = ab \to a \in U(A) \vee b \in U(A)\big],$$
and we already know that $U(A)$ is a Σ^0_1 set. A similar analysis shows that the set of primes of A is a Π^0_2 set. Our main result is the following, which says that this result is best possible in a very strong sense.

Theorem 1.6 *Let Q be a Π^0_2 set, and let $p_0, p_1, p_2, \ldots$ list the usual primes from $\mathbb{N}$ in increasing order. There exists a computable UFD A such that*

- *$\mathbb{Z}$ is a subring of A,*
- *p_i is prime in A if and only if $i \in Q$.*

This theorem differs from the result that there is a computable field F such that the set of prime elements in $F[x]$ is not computable. One reason is that we are working directly with the usual primes rather than coding into polynomials (such as $x^2 - p_i$), or creating our own primes to do the coding. As a result, our approach has a more number-theoretic flavor. Furthermore, if F is a computable field, then $U(F[x])$ is a computable set in any reasonable computable presentation of $F[x]$, so the set of irreducibles (and hence primes) of $F[x]$ will always be a Π^0_1 set by our above analysis, and hence could not be Π^0_2-complete. Moreover, we obtain the following strong corollary that may not hold if we code complexity into other primes.

Corollary 1.7 *There exists a computable UFD A such that the set of primes of A is Π^0_2-complete in every computable presentation of A, uniformly in an index for the presentation.*

Proof Fix a Π^0_2-complete set Q (see [18, Theorem IV.3.2]), and construct A by using this Q as in Theorem 1.6. Now given any computable presentation of A, we can find the multiplicative identity element of A by searching until we find $a \in A$ such that $a^2 = a$ and $a + a \neq a$ (note that the multiplicative identity is the only such element because A is an integral domain). With this element in hand, we can find the representation of each p_i in A by adding the multiplicative identity to itself the required number of times. Therefore, the set of primes of A is Π^0_2-complete in every computable presentation of A. □

Since we are working with the normal integer primes rather than creating some new ones, we need to be much more careful because of the algebraic dependence relationships that exist between them. By adjusting the status of one prime, that is, by introducing a new factorization of it, it is certainly conceivable that we could interfere with others. For example, suppose that A is a integral domain, that $q \in \text{Primes}(A)$, and that we want to break the primeness/irreducibility of q, that is, we want to introduce a nontrivial factorization of q. One idea is to introduce a square root of q, that is, to introduce a new element x with $x^2 = q$. The natural way to do this is to consider $A[x]/\langle x^2 - q\rangle$, but this is problematic for a few reasons. With this approach, we might destroy the primeness/irreducibility of other elements in A, as it is well known that if $p, q \in \mathbb{N}$ are distinct odd primes, then p is not prime in $\mathbb{Z}[\sqrt{q}] \cong \mathbb{Z}[x]/\langle x^2 - q\rangle$ if and only if q is a square modulo p. For example, in $\mathbb{Z}[\sqrt{7}]$, we have that 3 is not prime because $3 \mid (1 - \sqrt{7})(1 + \sqrt{7})$ but $3 \nmid 1 - \sqrt{7}$ and $3 \nmid 1 + \sqrt{7}$. Moreover, in $\mathbb{Z}[\sqrt{q}]$, irreducibles might fail to be prime, and hence we may have lost the property of being a UFD. Finally, with this approach it is also impossible to later destroy this factorization as we cannot make x a unit without making q a unit.

Another potential issue arises if we do want to destroy a given factorization by making an element a unit, but we are either not in a UFD or we are working with irreducibles. For instance, Conrad [5] gives the following example. In $\mathbb{Z}[\sqrt{-14}]$ one has

$$3 \cdot 3 \cdot 3 \cdot 3 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14}),$$

where all of the above factors are irreducible. It follows that

$$5 + 2\sqrt{-14} \mid 3^4$$

even though $5 + 2\sqrt{-14}$ and 3 are not associates in $\mathbb{Z}[\sqrt{-14}]$ (as the units are ± 1). Thus, in this ring, if we later make 3 a unit, then we must make $5 + 2\sqrt{-14}$ a unit as well.

With all of these potential issues in mind, we now outline the idea behind the construction. Start with $A_0 = \mathbb{Z}$. We want to turn the normal primes p_i *on* and *off* based on a Π^0_2 set Q. Fix a computable $R \subseteq \mathbb{N}^3$ such that

$$i \in Q \iff (\forall w)(\exists z) R(w, z, i).$$

So, intuitively, if i acts infinitely often (i.e., if for each w in turn, we find a witnessing z), then we want p_i to be prime in the end. If i acts finitely often, we want p_i not to be prime. To work for i, we assume finite action, and introduce a factorization $p_i = x_i y_i$ for new elements x_i and y_i. If i acts at a later stage, we want to destroy this factorization. To do this, we make y_i a unit. We will show that this keeps x_i prime, and since p_i will now be an associate of x_i, we will reinstate the fact that p_i is prime. We then introduce another factorization $p_i = x_i' y_i'$ for new x_i' and y_i', and continue, destroying it if i acts again. We do this forever, building a chain of integral domains $\mathbb{Z} = A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots$. Let $A_\infty = \bigcup_{n=0}^{\infty} A_n$.

We build this ring in a computable fashion as follows. We think of the natural numbers as being split into infinitely many infinite columns through a computable pairing function. We start by putting the integers in the first column and call that A_0. Now each extension will add infinitely many elements to the ring, and to do this at a given stage we will simply add these elements into the next column and computably define addition and multiplication at this point both within this column and between this column and previous ones. Eventually, we will fill up all of the columns in turn, and define all of the operations, resulting in a computable ring.

With this construction, we will need to keep track of several things. For example, when we make an element a unit, we will localize our ring, and since we have already constructed part of the ring so far, we will need to ensure that we can computably determine the new elements to add to form this localization. As a result, we will need to ensure that we can computably keep track of the multiples of the x_i and y_i that we introduce. Algebraically, we need to ensure that the rings along the way are all Noetherian UFDs and that unrelated primes are unaffected by these operations. Finally, we need to check that this limiting ring has the required properties since a union of UFDs need not be a UFD in general.

2 Turning a Prime into a Unit

Let A be an integral domain, and let $q \in A$ be prime. Suppose that we want to embed A in another integral domain B such that q is a unit in B. Naturally, one considers the corresponding localization, that is, we take the multiplicative set $S = \{1, q, q^2, \dots\}$ and let $B = S^{-1}A$ (see Eisenbud [9, Chapter 2] or Matsumura [13, Section 4] for general algebraic properties of localization). Thinking of A as sitting inside its field of fractions F by identifying a with $\frac{a}{1}$, we have

$$\begin{aligned} B &= \left\{ \frac{a}{q^k} : a \in A \text{ and } k \geq 0 \right\} \\ &= A \cup \left\{ \frac{a}{q^k} : a \in A \text{ and } k \geq 1 \right\}. \end{aligned}$$

Now if A is a computable integral domain and we want to think about extending to B in a computable fashion, then we need to know which of the elements in the set on the right are really new, along with when they are distinct from each other. For example, we have that $\frac{q^2}{q} = \frac{q}{1}$ is already an element of A, so we do not want to introduce it.

Observe that every element of $B \setminus A$ can be written in the form $\frac{a}{q^k}$, where $k \geq 1$ and $q \nmid a$. To see this, suppose that we are given a general $\frac{a}{q^m} \in B$ with $a \in A$ and $m \geq 1$. If $q \mid a$, we can factor out a q from a and cancel terms to obtain a different representation of the same element with a smaller power of q in the denominator. We can now induct (or take a minimal power in the denominator) to argue that this element is represented in the above set. Thus, we have

$$B = A \cup \left\{ \frac{a}{q^k} : a \in A, q \nmid a, \text{ and } k \geq 1 \right\}.$$

Moreover, it is straightforward to show that the above representations are unique (i.e., that $\frac{a}{q^k} \notin A$ when $q \nmid a$ and $k \geq 1$, and also that two elements of the right set are equal exactly when the numerator and power of q are equal). As a result, if A is computable, and the set $\{a \in A : q \mid a\}$ is computable, then from A, q, and an index for this set we can uniformly computably build B as an extension of A. Since we are going to repeatedly apply this construction along with a factorization construction, we will need to ensure that the set of multiples of other primes remain computable as well.

Using a straightforward algebraic argument, we have the following.

Proposition 2.1 *We have*

$$U(B) = U(A) \cup \left\{ uq^k : k \geq 1 \text{ and } u \in U(A) \right\} \cup \left\{ \frac{u}{q^k} : k \geq 1 \text{ and } u \in U(A) \right\}.$$

Theorem 2.2 *Let A be a computable Noetherian UFD, and let $q \in A$ be prime. Suppose that $\{a \in A : q \mid a \text{ in } A\}$ is a computable set. Let $S = \{1, q, q^2, \dots\}$, and let $B = S^{-1}A$ as above.*

(1) *We can build B as a computable extension of A uniformly from A and an index for the set $\{a \in A : q \mid a \text{ in } A\}$ of multiples of q.*
(2) *Let $p \in \text{Primes}(A) \setminus \text{Associates}_A(q)$. The multiples of p in B are precisely the elements of the following set:*

$$\{a \in A : p \mid a \text{ in } A\} \cup \left\{ \frac{a}{q^k} : a \in A, k \geq 1, q \nmid a \text{ in } A, \text{ and } p \mid a \text{ in } A \right\}.$$

In particular, there are no new elements of A that are multiples of p in B. Furthermore, if we have a computable index for the set $\{a \in A : p \mid a \text{ in } A\}$, then we can uniformly computably obtain a computable index for the set $\{\sigma \in B : p \mid \sigma \text{ in } B\}$.
(3) *If $p_1, p_2 \in \text{Primes}(A)$ are not associates in A, then they are not associates in B.*
(4) *We have $\text{Primes}(A) \setminus \text{Associates}_A(q) \subseteq \text{Primes}(B)$.*
(5) *We have that B is a Noetherian UFD.*

Proof (1) This is immediate from above.

(2) It is easy to see that the elements in the given sets are indeed multiples of p in B. Suppose then that $\sigma \in B$ is arbitrary with $p \mid \sigma$ in B. Suppose first that $\sigma = a \in A$. We need to show that $p \mid a$ in B. We have two cases.

- Suppose that there exists $b \in A$ with $pb = \sigma = a$. We then trivially have that $p \mid a$ in A.
- Suppose instead that there exists $b \in A$ with $q \nmid b$ and $\ell \geq 1$ such that $p \cdot \frac{b}{q^\ell} = a$. We then have $pb = aq^\ell$. Thus $p \mid aq^\ell$ in A, and since p is prime and $p \nmid q$ (as $p \notin \text{Associates}_A(q)$), it follows that $p \mid a$ in A.

Suppose instead that $\sigma = \frac{a}{q^k}$, where $a \in A$ with $q \nmid a$ and $k \geq 1$. We need to show that $p \mid a$ in A.

- Suppose that there exists $b \in A$ with $pb = \sigma = \frac{a}{q^k}$. We then have $pbq^k = a$, so $p \mid a$ in A.
- Suppose instead that there exists $b \in A$ with $q \nmid b$ and $\ell \geq 1$ such that $p \cdot \frac{b}{q^\ell} = \sigma = \frac{a}{q^k}$. We then have $pbq^k = aq^\ell$. Thus $p \mid aq^\ell$ in A, and since p is prime and $p \nmid q$ (as $p \notin \text{Associates}_A(q)$), it follows that $p \mid a$ in A.

This completes the proof.

(3) We prove the contrapositive. Suppose that p_1 and p_2 are associates in B. Fix $\sigma \in U(B)$ such that $p_1 = \sigma p_2$. We know the units of B from Proposition 2.1, so we handle the cases.

- If $\sigma \in U(A)$, then clearly p_1 and p_2 are associates in A.
- Suppose that $\sigma = uq^k$ with $u \in U(A)$. We then have $p_1 = uq^k p_2$, so $p_2 \mid p_1$ in A. Since p_1 is prime in A, it is irreducible in A, so as p_2 is not a unit we can conclude that p_1 and p_2 are associates in A.
- Suppose that $\sigma = \frac{u}{q^k}$, where $k \geq 1$ and $u \in U(A)$. We then have $p_1 = \frac{u}{q^k} \cdot p_2$, so $p_1 u^{-1} q^k = p_2$. This implies that $p_1 \mid p_2$ in A. As in the previous case, this implies that p_1 and p_2 are associates in A.

(4) Let $p \in \text{Primes}(A) \setminus \text{Associates}_A(q)$. First note that $p \notin U(B)$ from Proposition 2.1 because $p \notin U(A)$ and that p is not an associate of any q^k (because if $p \mid q^k$, then $p \mid q$ as p is prime, and hence p is an associate of q). Suppose that

$$\frac{p}{1} \mid \frac{a}{q^k} \cdot \frac{b}{q^\ell},$$

where we allow the possibility that $k = 0$ and/or $\ell = 0$. Fix $c \in A$ and $m \geq 0$ with

$$\frac{p}{1} \cdot \frac{c}{q^m} = \frac{a}{q^k} \cdot \frac{b}{q^\ell}.$$

We then have $pcq^{k+\ell} = q^m ab$, so $p \mid q^m ab$ in A. Now p is prime and $p \nmid q$ (as $p \notin \text{Associates}_A(q)$), so either $p \mid a$ in A or $p \mid b$ in A. If $p \mid a$ in A, then $\frac{p}{1} \mid \frac{a}{q^k}$ in B, and a similar statement holds if $p \mid b$. Therefore, $p \in \text{Primes}(B)$.

(5) This is immediate from the fact that the localization of a Noetherian ring is a Noetherian ring, and the localization of a UFD is a UFD. □

Note that we can use this machinery to prove the result (essentially appearing in Baur [1] and [19, Example 4.3.9]) that there exists a computable principal ideal domain (PID) A such that $U(A)$ is Σ^0_1-complete in all computable presentations. Fix a Σ^0_1-complete set Q. Start with $A_0 = \mathbb{Z}$, and let $p_0, p_1, p_2, \ldots$ be a listing of the usual primes. As we go along, if we have A_n and we ever see that $e \in Q$, then we perform our unit construction to build A_{n+1} extending A_n so that $p_e \in U(A_{n+1})$ while maintaining the primeness of the p_i not equal to p_e or to any elements we already made units. Let $A = A_\infty = \bigcup_{n=0}^{\infty} A_n$, and note that $i \in Q$ if and only if $p_i \in U(A_\infty)$. Since the final ring A_∞ is a localization of the PID $A_0 = \mathbb{Z}$, it follows that A_∞ is a PID.

3 Introducing a Factorization

In this section, we suppose that we have a computable Noetherian UFD A and an element $q \in \text{Primes}(A)$. We introduce a new factorization of q by going to the ring $B = A[x, y]/\langle xy - q\rangle$. The hope is that we only destroy the primeness/irreducibility of q (and its associates), and we leave enough flexibility so that we can later make y a unit without making x a unit (so that then q and x will be associates).

Proposition 3.1 *The ring B is an integral domain.*

Proof It is straightforward to check that $xy - q$ is irreducible in $A[x, y]$. Since $A[x, y]$ is a UFD (because A is a UFD), we conclude that $xy - q$ is prime in $A[x, y]$, so the quotient $B = A[x, y]/\langle xy - q\rangle$ is an integral domain. □

Proposition 3.2 *Every element of B can be represented uniquely in the form*

$$a_m x^m + \cdots + a_1 x + c + b_1 y + \cdots + b_n y^n,$$

where each $a_i \in A$, $b_i \in A$, and $c \in A$.

Proof Given an arbitrary polynomial $h(x, y) \in A[x, y]$, we can divide by $xy - q$ (using the fact that the leading term is a unit) to obtain a remainder where no monomial is divisible by xy. In other words, in the quotient, reduce any monomial with xy in it to q, and repeat until there are no xy's. This proves existence. For uniqueness, the difference of any polynomials of this form is another polynomial of this form, and hence has no monomial containing both an x and a y. Any nonzero multiple of $xy - q$ must have a monomial divisible by xy by looking at a leading term under some monomial ordering (and again using the fact that A is an integral domain). □

Note that in B we have $xy = q$. Thinking of $y = \frac{q}{x}$, we can alternatively think about B in the following way.

Proposition 3.3 *Consider the following subring of the field of fractions of $A[x]$:*

$$A\left[x, \frac{q}{x}\right] = \left\{a_m x^m + \cdots + a_1 x + a_0 + a_{-1} \cdot \frac{q}{x} + \cdots + a_{-n} \cdot \frac{q^n}{x^n} : a_i \in A\right\}.$$

We have $B \cong A[x, \frac{q}{x}]$.

Proof The proof is straightforward. □

We will use the different ways of representing elements of the extension $B \cong A[x, \frac{q}{x}]$ interchangeably depending on which is most convenient. With this isomorphism in mind, we define the following two functions.

Definition 3.4 Define $\deg_x : B\backslash\{0\} \to \mathbb{Z}$ as follows. Let $\sigma \in B$, and consider the unique representation of σ given in Proposition 3.2.

- If there is a term containing a power of x with a nonzero coefficient, then $\deg_x(\sigma)$ is the largest such power of x.
- If there is no such power of x, but there is a nonzero constant term, then $\deg_x(\sigma) = 0$.
- If there is no such power of x and no constant term, let m be the least power of y with a nonzero coefficient, and define $\deg_x(\sigma) = -m$.

We define $\deg_y : B\backslash\{0\} \to \mathbb{Z}$ similarly.

For example, we have $\deg_x(y^2 + y^5) = -2$ and $\deg_y(y^2 + y^5) = 5$.

Proposition 3.5 *Let $\sigma, \tau \in B\backslash\{0\}$. We then have*

$$\deg_x(\sigma\tau) = \deg_x(\sigma) + \deg_x(\tau),$$
$$\deg_y(\sigma\tau) = \deg_y(\sigma) + \deg_y(\tau).$$

Proof It is straightforward to prove this in the case when σ and τ are monomials, that is, of the form ax^k, by^ℓ, or $c \neq 0$. Notice that here we use the fact that A is an integral domain to conclude that the product is a nonzero monomial. For general σ and τ, we need only examine the leading x-terms or y-terms. □

Proposition 3.6 *We have*

$$\deg_x(\sigma) + \deg_y(\sigma) \geq 0$$

for all $\sigma \in B\backslash\{0\}$, with equality if and only if σ is a constant times a monomial.

Proof Let $\sigma \in B\backslash\{0\}$. If the leading x-term is x^m, then $\deg_x(\sigma) = m$ and $\deg_y(\sigma) \geq -m$, with equality if and only if x^m is the leading y-term as well. A similar argument works if the leading y-term is y^n. Otherwise, we only have a constant, in which case both $\deg_x(\sigma) = 0$ and $\deg_y(\sigma) = 0$. □

Proposition 3.7 *Let $\sigma, \tau \in B$. We then have that $\sigma\tau \in A$ in exactly the following cases:*

- *$\sigma = 0$ or $\tau = 0$;*
- *$\sigma \in A$ and $\tau \in A$;*
- *there exist $a, b \in A$ and $n \in \mathbb{N}^+$ with $\sigma = ax^n$ and $\tau = by^n$, or there exist $a, b \in A$ and $n \in \mathbb{N}^+$ with $\sigma = by^n$ and $\tau = ax^n$.*

Proof In each of these cases it is easy to see that $\sigma\tau \in A$. Suppose conversely that $\sigma\tau \in A$. We may assume that $\sigma \neq 0$ and $\tau \neq 0$ or else we are done. We then have

$$\deg_x(\sigma) + \deg_x(\tau) = \deg_x(\sigma\tau) = 0$$

so $\deg_x(\tau) = -\deg_x(\sigma)$. Similarly, we have $\deg_y(\tau) = -\deg_y(\sigma)$. Adding these gives

$$\deg_x(\tau) + \deg_y(\tau) = -\deg_x(\sigma) - \deg_y(\sigma) = -\big(\deg_x(\sigma) + \deg_y(\sigma)\big).$$

Using Proposition 3.6, the only possibility is that

$$\deg_x(\tau) + \deg_y(\tau) = 0 = \deg_x(\sigma) + \deg_y(\sigma),$$

and hence that both σ and τ are constants times monomials. The result now follows. □

Corollary 3.8 *Let $a \in A$ with $q \nmid a$ in A. If $\sigma \in B$ and $\sigma \mid a$ in B, then $\sigma \in A$ and $\sigma \mid a$ in A. In other words, the set of divisors of a in B equals the set of divisors of a in A.*

Proof By Proposition 3.7, the only possible new divisors of a are when $a = bx^n \cdot cy^n$ with $n \geq 1$. However, this implies that $a = bc \cdot q^n$, so $q \mid a$ in A. □

Corollary 3.9 *The units of B are precisely the units of A, that is, $U(B) = U(A)$.*

Proof This is immediate because the set of units is the set of divisors of $1 \in A$. □

Theorem 3.10 *Let A be a computable Noetherian UFD, and let $q \in A$ be prime. Let $B = A[x, y]/\langle xy - q\rangle$ as above.*

(1) *We can build B as a computable extension of A uniformly.*
(2) *If $p_1, p_2 \in \text{Primes}(A)$ are not associates in A, then they are not associates in B.*
(3) *Let $p \in \text{Primes}(A)\setminus \text{Associates}_A(q)$, and let $\sigma \in B$. We have that $p \mid \sigma$ in B if and only every coefficient of σ is divisible by p in A. In particular, there are no new elements of A that are multiples of p in B. Furthermore, if we have a computable index for the set $\{a \in A : p \mid a \text{ in } A\}$, then we can uniformly computably obtain a computable index for the set $\{\sigma \in B : p \mid \sigma \text{ in } B\}$.*
(4) *We have* $\text{Primes}(A)\setminus \text{Associates}_A(q) \subseteq \text{Primes}(B)$.
(5) *We have that $x \mid \sigma$ in B if and only if the constant term and the coefficients of each y^j in σ are all divisible by q in A. Therefore, if we have a computable index for the set $\{a \in A : q \mid a \text{ in } A\}$, then we can uniformly computably obtain a computable index for the set $\{\sigma \in B : x \mid \sigma \text{ in } B\}$.*
(6) *We have that $y \mid \sigma$ in B if and only if the constant term and the coefficients of each x^i in σ are all divisible by q in A. Therefore, if we have a computable index for the set $\{a \in A : q \mid a \text{ in } A\}$, then we can uniformly computably obtain a computable index for the set $\{\sigma \in B : y \mid \sigma \text{ in } B\}$.*
(7) *We have that x and y are primes in B that are not associates of each other in B.*
(8) *We have that x and y are not associates in B with any element of A, and hence not with any element of* $\text{Primes}(A)$.
(9) *We have that B is a Noetherian UFD.*

Proof (1) This follows immediately from Proposition 3.2.
(2) This follows immediately from Corollary 3.9.
(3) This follows from the fact that

$$\begin{aligned} &p \cdot (a_m x^m + \cdots + a_1 x + c + b_1 y + \cdots + b_n y^n) \\ &\quad = pa_m x^m + \cdots + pa_1 x + pc + pb_1 y + \cdots + pb_n y^n. \end{aligned}$$

(4) Let $p \in \text{Primes}(A)\setminus \text{Associates}_A(q)$. Note that p is nonzero and is not a unit of B by Corollary 3.9. Let $\sigma, \tau \in B$, and suppose that $p \mid \sigma\tau$. Assume that $p \nmid \sigma$ and $p \nmid \tau$. We clearly have that both σ and τ are nonzero. Using Theorem 3.10(3), we know that p divides every coefficient of $\sigma\tau$ in A, but there are coefficients of σ and τ that are not divisible by p in A. Write

$$\sigma = a_m x^m + \cdots + a_1 x + a_0 + a_{-1} \cdot \frac{q}{x} + \cdots + a_{-n} \cdot \frac{q^n}{x^n}$$

and

$$\tau = b_m x^m + \cdots + b_1 x + b_0 + b_{-1} \cdot \frac{q}{x} + \cdots + b_{-n} \cdot \frac{q^n}{x^n}.$$

Let k and ℓ be the largest possible such that $p \nmid a_k$ in A and $p \nmid b_\ell$ in A. Look at the coefficient of $x^{k+\ell}$ in $\sigma\tau$. This coefficient will be a sum of terms, one of which is $a_k b_\ell q^j$ for some j, while other terms will be divisible by p in A. Since p divides the resulting coefficient, it follows that $p \mid a_k b_\ell q^j$ in A. However, this is a contradiction because p is prime in A but divides none of a_k, b_ℓ, or q (the last because p is not an associate of q in A).

(5) Let $\sigma \in B$, and write

$$\sigma = a_m x^m + \cdots + a_1 x + c + b_1 y + \cdots + b_n y^n.$$

Suppose first that $q \mid c$ and $q \mid b_j$ in A for each j. Fix $e \in A$ with $c = qe$, and fix $d_j \in A$ such that $b_j = q d_j$ for all j. We then have

$$x \cdot (a_m x^{m-1} + \cdots + a_1 + ey + d_1 y^2 + \cdots + d_n y^{n+1}) = \sigma.$$

Conversely, suppose that $x \mid \sigma$, so that

$$\sigma = x \cdot (a_m x^m + \cdots + a_1 x + c + b_1 y + \cdots + b_n y^n)$$

for some $a_i, c, b_j \in A$. Then we have

$$\sigma = a_m x^{m+1} + \cdots + a_1 x + cx + qb_1 + qb_2 y + \cdots + qb_n y^{n-1}.$$

(6) This is similar to Theorem 3.10(5).

(7) Note that x is nonzero and is not a unit of B by Corollary 3.9. Let $\sigma, \tau \in B$, and suppose that $x \mid \sigma\tau$. Assume that $x \nmid \sigma$ and $x \nmid \tau$. We clearly have that both σ and τ are nonzero. Using Theorem 3.10(5), we know that q divides the constant term and the coefficients of each y^j in $\sigma\tau$ in A. Write

$$\sigma = a_m x^m + \cdots + a_1 x + a_0 + b_1 y + \cdots + b_n y^n$$

and

$$\tau = c_m x^m + \cdots + c_1 x + c_0 + d_1 y + \cdots + d_n y^n.$$

By Theorem 3.10(5), we may let k and ℓ be largest possible such that $q \nmid a_k$ in A and $q \nmid c_\ell$ in A. Look at the coefficient of $x^{k+\ell}$ in $\sigma\tau$. This coefficient will be a sum of terms, one of which is $a_k c_\ell$, while other terms will be divisible by q in A. Since q divides the resulting coefficient, it follows that $q \mid a_k c_\ell$ in A. However, this is a contradiction because q is prime in A but divides neither of a_k or c_ℓ in A.

The proof that y is prime in B is similar. The fact that x and y are not associates in B follows from Corollary 3.9.

(8) This is immediate from Corollary 3.9.

(9) We are assuming that A is a Noetherian UFD. Since A is Noetherian, we know that $A[x, y]$ is Noetherian by Hilbert's basis theorem. Since B is a quotient of $A[x, y]$, it follows that B is also Noetherian. We also know from Theorem 3.10(7) that x is prime in $B \cong A[x, \frac{q}{x}]$. To argue that B is a UFD, we use Nagata's criterion (see [13, Theorem 20.2] or [9, Lemma 19.20]) which says the following.

Theorem 3.11 (Nagata's criterion) *Let B be a Noetherian integral domain. Let Γ be a set of prime elements of B, and let S be the multiplicative set generated by Γ. If $S^{-1}B$ is a UFD, then B is a UFD.*

Now x is prime in $B \cong A[x, \frac{q}{x}]$ by Theorem 3.10(7). The localization of $A[x, \frac{q}{x}]$ at x equals $A[x, \frac{q}{x}, \frac{1}{x}] = A[x, \frac{1}{x}]$, which is the localization of $A[x]$ at x. Since A is a UFD, we know that $A[x]$ is a UFD . Since any localization of a UFD is a UFD, it follows that $A[x, \frac{1}{x}]$ is a UFD. Since B is a Noetherian integral domain, x is prime in B, and B localized at x is a UFD, we may use Nagata's criterion to conclude that B is a UFD. □

4 Construction and Verification

We now prove Theorem 1.6. Let Q be an arbitrary Π^0_2 set. Fix a computable $R \subseteq \mathbb{N}^3$ such that

$$i \in Q \iff (\forall w)(\exists z) R(w, z, i).$$

Fix a bijective computable pairing function $\langle \cdot, \cdot \rangle : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ with the property that $\langle i, s \rangle < \langle i, t \rangle$ whenever $s < t$.

We work in stages, and begin by initializing with $A_0 = \mathbb{Z}$. We now start at stage 0. At a given stage, we will have introduced finitely many $x_i^{(k)}$ and $y_i^{(k)}$ for each i, and we will have marked a finite initial segment of $\mathbb{N}$ corresponding to those $w \in \mathbb{N}$ for which we have found a witnessing z and done an action. Furthermore, if i has been initialized and the first unmarked w is k, then we will have introduced $x_i^{(\ell)}$ and $y_i^{(\ell)}$ for each $\ell \leq k$, but we will not yet have introduced $x_i^{(k+1)}$ and $y_i^{(k+1)}$.

Suppose that we are now at a stage $\langle i, s \rangle$ and we have constructed through ring A_n at this stage.

- If $s = 0$, we do an initialization for p_i by introducing a first factorization. In other words, we introduce $x_i^{(0)}$ and $y_i^{(0)}$ and perform the factorization construction on p_i to create the ring A_{n+1} (so we fill in one more column), and then move on to the next stage.
- Suppose that $s \geq 1$, and let k be the first unmarked w corresponding to i. Check to see if there exists $z \leq s$ such that $R(w, z, i)$. If not, we do nothing and move to the next stage. If so, we mark k for i, and we act for i at this stage, meaning that we do the following. As mentioned above, we will have introduced through $x_i^{(k)}$ and $y_i^{(k)}$. First, we perform the localization construction to make $y_i^{(k)}$ a unit in order to create the ring A_{n+1}. Next, we introduce $x_i^{(k+1)}$ and $y_i^{(k+1)}$ and perform the factorization construction with these on p_i to create the ring A_{n+2}. Thus, we fill in two more columns in succession, and then move on to the next stage.

Finally, let $A_\infty = \bigcup_{n=0}^{\infty} A_n$.

Theorem 4.1 *Suppose that we are at the beginning of a given stage and we have constructed through A_n. For each i that has been initialized, let $x_i^{(k_i)}$ and $y_i^{(k_i)}$ be the last elements introduced for i (so k_i is the first unmarked w for i).*

- *Suppose that i has not yet been initialized. We have the following.*
  - *We have that p_i is prime in A_n.*

  - *The set $\{a \in A_n : p_i \mid a \text{ in } A_n\}$ is computable and we can uniformly find a computable index for it.*
  - *For any uninitialized $j \neq i$, we have that p_i is not an associate of p_j in A_n.*
  - *For any initialized $j \neq i$, we have that p_i is not an associate of either $x_j^{(k_j)}$ or $y_j^{(k_j)}$ in A_n.*
- *Suppose that i has been initialized. We have the following.*
  - *We have that $x_i^{(k_i)}$ and $y_i^{(k_i)}$ are prime in A_n, and are not associates in A_n.*
  - *The sets $\{a \in A_n : x_i^{(k_i)} \mid a \text{ in } A_n\}$ and $\{a \in A_n : y_i^{(k_i)} \mid a \text{ in } A_n\}$ are computable and we can uniformly find computable indices for them.*
  - *For any uninitialized $j \neq i$, we have that $x_i^{(k_i)}$ and $y_i^{(k_i)}$ are not associates of p_j in A_n.*
  - *For any initialized $j \neq i$, we have that $x_i^{(k_i)}$ is not an associate of either $x_j^{(k_j)}$ or $y_j^{(k_j)}$ in A_n, and $y_i^{(k_i)}$ is not an associate of either $x_j^{(k_j)}$ or $y_j^{(k_j)}$ in A_n.*
- *Suppose that we act for i at this stage. We then have $y_i^{(k_i)} \in U(A_{n+1})$, that $x_i^{(k_i)}$ is prime in A_{n+1}, and that p_i is prime in A_{n+1}.*

Proof The proof is immediate by using induction on the stages along with Theorems 2.2 and 3.10. □

Definition 4.2 Let $i, k \in \mathbb{N}$, and suppose that we introduce $x_i^{(k)}$ and $y_i^{(k)}$ in our construction. We call $x_i^{(k)}$ and $y_i^{(k)}$ *terminal for i* if we never introduce $x_i^{(k+1)}$ and $y_i^{(k+1)}$ for i.

Proposition 4.3 *We have the following.*

(1) *Suppose that we introduce $x_i^{(k)}$ and $y_i^{(k)}$ in A_m. If $x_i^{(k)}$ and $y_i^{(k)}$ are terminal for i, then they are nonassociate primes in A_n for each $n \geq m$.*
(2) *If $r \in A_m$ is prime in A_m and is not an associate of any p_i, $x_i^{(k)}$, or $y_i^{(k)}$ (whether terminal or nonterminal) in A_m, then r remains prime in A_n for each $n \geq m$.*

Proof Again, this follows by induction using Theorems 2.2 and 3.10. □

Proposition 4.4 *Let $a \in A_\infty$, so $a \in A_m$ for some $m \in \mathbb{N}$. The following are equivalent:*

(1) *$a \in U(A_\infty)$,*
(2) *$a \in U(A_n)$ for all sufficiently large $n \geq m$, and*
(3) *$a \in U(A_n)$ for some $n \geq m$.*

Proof If $a \in U(A_\infty)$, then fixing $b \in A_\infty$ with $ab = 1$, we have that $a \in U(A_n)$ for any n large enough such that $a, b \in A_n$. If $a \in U(A_n)$ for some $n \geq m$, then fixing $b \in A_n$ with $ab = 1$, we have $a, b \in A_\infty$, so $a \in U(A_\infty)$. □

Proposition 4.5 *Let $r \in A_\infty$, so $r \in A_m$ for some $m \in \mathbb{N}$. If there are infinitely many $n \geq m$ such that r is prime in A_n, then r is prime in A_∞.*

Proof Suppose that there are infinitely many $n \geq m$ such that r is prime in A_n. Fix $a, b \in A_\infty$, and suppose that $r \mid ab$ in A_∞. Fix $c \in A_\infty$ with $rc = ab$. Go to a point where each of r, c, a, b exist, and then fix an n beyond that such that r is prime in A_n. We then have $r \mid ab$ in A_n, so as r is prime in A_n, either $r \mid a$ in A_n or $r \mid b$ in A_n. Therefore, either $r \mid a$ in A_∞ or $r \mid b$ in A_∞. Finally, notice that r is nonzero and not a unit in A_∞ because infinitely often it is not a unit in A_n (as infinitely often it is prime in A_n). □

Corollary 4.6 *We have the following.*

(1) *If $x_i^{(k)}$ and $y_i^{(k)}$ are introduced and are terminal for i, then they are nonassociate primes in A_∞.*
(2) *If $x_i^{(k)}$ and $y_i^{(k)}$ are introduced and are nonterminal for i, then $y_i^{(k)} \in U(A_\infty)$, and $x_i^{(k)}$ is an associate of p_i in A_∞.*
(3) *If $r \in A_m$ is prime in A_m and is not an associate of any p_i, $x_i^{(k)}$, or $y_i^{(k)}$ in A_m (whether terminal or nonterminal), then r remains prime in A_∞.*

Proof This is immediate from Theorem 4.1 and Propositions 4.3, 4.4, and 4.5. □

Corollary 4.7 *We have that p_i is prime in A_∞ if and only if $i \in Q$.*

Proof Suppose first that $i \in Q$. We then act for i infinitely often, and hence p_i is prime in infinitely many A_n by Theorem 4.1. Thus, p_i is prime in A_∞ by Proposition 4.5.

Suppose now that $i \notin Q$. We then act for i finitely often, so we may fix k such that $x_i^{(k)}$ and $y_i^{(k)}$ are terminal for i. By Corollary 4.6, each of $x_i^{(k)}$ and $y_i^{(k)}$ are prime in A_∞. Since $p_i = x_i^{(k)} y_i^{(k)}$, it follows that p_i is not irreducible in A_∞, and hence not prime in A_∞. □

Lemma 4.8 *Let $m \in \mathbb{N}$. Let $r \in A_\infty$, and suppose that r is prime in A_m. We then have that either $r \in U(A_\infty)$, r is prime is A_∞, or r is the product of two primes in A_∞.*

Proof We handle the various cases.

- If there exists $i \in Q$ such that r is an associate of p_i in A_m, then r is prime in A_∞ by Corollary 4.7.
- Suppose that there exists $i \notin Q$ such that r is an associate of p_i in A_m. We then act for i finitely often, so we may fix k such that $x_i^{(k)}$ and $y_i^{(k)}$ are terminal for i. By Corollary 4.6, each of $x_i^{(k)}$ and $y_i^{(k)}$ are prime in A_∞. We then have that $p_i = x_i^{(k)} y_i^{(k)}$, so $r = u x_i^{(k)} y_i^{(k)}$ for some unit $u \in U(A_\infty)$. Since $u x_i^{(k)}$ and $y_i^{(k)}$ are prime in A_∞, we see that r is the product of two primes in A_∞.
- If there exists $i, k \in \mathbb{N}$ such that r is an associate of a terminal $x_i^{(k)}$ in A_m, then r is prime in A_∞ by Corollary 4.6.
- If there exists $i, k \in \mathbb{N}$ such that r is an associate of a terminal $y_i^{(k)}$ in A_m, then r is prime in A_∞ by Corollary 4.6.
- If there exists $i \in Q$ and $k \in \mathbb{N}$ such that r is an associate of a nonterminal $x_i^{(k)}$ in A_m, then r is an associate of p_i in A_∞ by Corollary 4.6 and hence r is prime in A_∞ by Corollary 4.7.

- If there exists $i \notin Q$ and $k \in \mathbb{N}$ such that r is an associate of a nonterminal $x_i^{(k)}$ in A_m, then r is an associate of p_i in A_∞ by Corollary 4.6, and hence r is a product of two primes in A_∞ from above.
- If there exists $i, k \in \mathbb{N}$ such that r is an associate of a nonterminal $y_i^{(k)}$ in A_m, then $r \in U(A_\infty)$ by Corollary 4.6.
- If r is not an associate of any p_i, $x_i^{(k)}$, or $y_i^{(k)}$ in A_m, then r is prime in A_∞ by Corollary 4.6. □

Theorem 4.9 *We have that A_∞ is a UFD.*

Proof We prove that every nonzero nonunit element of A_∞ is a product of irreducibles and that every irreducible is prime, which suffices by Theorem 1.3.

Let $a \in A_\infty$ be nonzero and not a unit. Fix n with $a \in A_n$, and note that a is not a unit in A_n. Since A_n is a UFD, we may write $a = r_1 r_2 \cdots r_\ell$ where each r_i is irreducible and hence prime in A_n. By Lemma 4.8, each r_j is either a unit in A_∞, is prime in A_∞, or is the product of two primes in A_∞. It is not possible that all r_j's are units in A_∞, because this would imply that a is a unit in A_∞. Thus, a is a product of primes in A_∞ (since we can absorb the units in one of the primes). Since primes are irreducible, we conclude that a is a product of irreducibles in A_∞.

We now show that every irreducible element of A_∞ is prime. Let $a \in A_\infty$ be irreducible. Fix n with $a \in A_n$. Note that a is nonzero and not a unit in A_n because otherwise it would be zero or a unit in A_∞. Since A_n is a UFD, we may write $a = r_1 r_2 \cdots r_\ell$ where each r_j is irreducible and hence prime in A_n. By Lemma 4.8, each r_j is either a unit in A_∞, is prime in A_∞, or is the product of two primes in A_∞. It is not possible that all r_j's are units in A_∞, because this would imply that a is a unit in A_∞. If some r_j is a product of two primes in A_∞, then a is not irreducible in A_∞, which is a contradiction. Also, if two of the r_j's are prime in A_∞, then A is not irreducible in A_∞, which is a contradiction. Thus, exactly one of the r_i's is prime in A_∞ and the rest are units. It follows that A is a prime times some units in A_∞, so a is prime in A_∞.

This completes the proof of Theorem 1.6. □

References

[1] Baur, W., "Rekursive Algebren mit Kettenbedingungen," *Mathematical Logic Quarterly*, vol. 20 (1974), pp. 37–46. Zbl 0317.02050. MR 0351781. DOI 10.1002/malq.19740200105. 147

[2] Cohen, H., *A Course in Computational Algebraic Number Theory*, vol. 138 of *Graduate Texts in Mathematics*, Springer, Berlin, 1993. Zbl 0786.11071. MR 1228206. DOI 10.1007/978-3-662-02945-9. 140, 141

[3] Cohen, H., *Advanced Topics in Computational Number Theory*, vol. 193 of *Graduate Texts in Mathematics*, Springer, New York, 2000. Zbl 0977.11056. MR 1728313. DOI 10.1007/978-1-4419-8489-0. 140

[4] Conidis, C. J., "On the complexity of radicals in noncommutative rings," *Journal of Algebra*, vol. 322 (2009), pp. 3670–80. Zbl 1182.03073. MR 2568356. DOI 10.1016/j.jalgebra.2009.07.039. 140

[5] Conrad, K., "Factoring in quadratic fields," preprint, http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/quadraticgrad.pdf (accessed 4 October 2017). 143

[6] Crandall, R., and C. Pomerance, *Prime Numbers: A Computational Perspective*, 2nd edition, Springer, New York, 2005. Zbl 1088.11001. MR 2156291. 139

[7] Downey, R. G., and A. M. Kach, "Euclidean functions of computable Euclidean domains," *Notre Dame Journal of Formal Logic*, vol. 52 (2011), pp. 163–72. Zbl 1260.03082. MR 2794649. DOI 10.1215/00294527-1306172. 140

[8] Downey, R. G., S. Lempp, and J. R. Mileti, "Ideals in computable rings," *Journal of Algebra*, vol. 314 (2007), pp. 872–87. Zbl 1127.03037. MR 2344588. DOI 10.1016/j.jalgebra.2007.02.058. 140

[9] Eisenbud, D., *Commutative Algebra: With a View Toward Algebraic Geometry*, vol. 150 of *Graduate Texts in Mathematics*, Springer, New York, 1995. Zbl 0819.13001. MR 1322960. DOI 10.1007/978-1-4612-5350-1. 144, 150

[10] Friedman, H. M., S. G. Simpson, and R. L. Smith, "Countable algebra and set existence axioms," *Annals of Pure and Applied Logic*, vol. 25 (1983), pp. 141–81. Zbl 0575.03038. MR 0725732. DOI 10.1016/0168-0072(83)90012-X. Addendum, *Annals of Pure and Applied Logic*, vol. 28 (1985), pp. 319–20. Zbl 0575.03039. MR 0790391. 140

[11] Fröhlich, A., and J. C. Shepherdson, "Effective procedures in field theory," *Philosophical Transactions of the Royal Society of London, Series A*, vol. 248 (1956), pp. 407–32. Zbl 0070.03502. MR 0074349. DOI 10.1098/rsta.1956.0003. 140

[12] Klüners, J., "Algorithms for function fields," *Experimental Mathematics*, vol. 11 (2002), pp. 171–81. Zbl 1116.11325. MR 1959261. DOI 10.1080/10586458.2002.10504684. 140

[13] Matsumura, H., *Commutative Ring Theory*, vol. 8 of *Cambridge Studies in Advanced Mathematics*, Cambridge University Press, Cambridge, 1986. Zbl 0603.13001. MR 0879273. 144, 150

[14] Metakides, G., and A. Nerode, "Effective content of field theory," *Annals of Mathematical Logic*, vol. 17 (1979), pp. 289–320. Zbl 0469.03028. MR 0556895. DOI 10.1016/0003-4843(79)90011-1. 140

[15] Miller, R., "Computable fields and Galois theory," *Notices of the American Mathematical Society*, vol. 55 (2008), pp. 798–807. Zbl 1194.03030. MR 2436510. 140, 142

[16] Müller-Quade, J., and R. Steinwandt, "Basic algorithms for rational function fields," *Journal of Symbolic Computation*, vol. 27 (1999), pp. 143–70. Zbl 0935.11046. MR 1672124. DOI 10.1006/jsco.1998.0246. 140

[17] Rabin, M. O., "Computable algebra, general theory and theory of computable fields," *Transactions of the American Mathematical Society*, vol. 95 (1960), pp. 341–60. Zbl 0156.01201. MR 0113807. DOI 10.2307/1993295. 140

[18] Soare, R. I., *Recursively Enumerable Sets and Degrees: A Study of Computable Functions and Computably Generated Sets*, *Perspectives in Mathematical Logic*, Springer, Berlin, 1987. Zbl 0667.03030. MR 0882921. DOI 10.1007/978-3-662-02460-7. 140, 142, 143

[19] Stoltenberg-Hansen, V., and J. V. Tucker, "Computable rings and fields," pp. 363–447 in *Handbook of Computability Theory*, vol. 140 of *Studies in Logic and the Foundations of Mathematics*, North-Holland, Amsterdam, 1999. Zbl 0944.03040. MR 1720739. DOI 10.1016/S0049-237X(99)80028-7. 140, 142, 147

Acknowledgments

Dzhafarov's work was partially supported by a National Science Foundation Postdoctoral Fellowship. We thank Sean Sather-Wagstaff for pointing out Nagata'a criterion to us, and we thank Keith Conrad for helpful discussions.

Dzhafarov
Department of Mathematics
University of Connecticut
Storrs, Connecticut 06269
USA
damir@math.uconn.edu
http://www.math.uconn.edu/~damir

Mileti
Department of Mathematics and Statistics
Grinnell College
Grinnell, Iowa 50112
USA
miletijo@grinnell.edu
http://www.math.grinnell.edu/~miletijo