The Journal of Symbolic Logic
Volume 85, Number 4, December 2020

UNIFORM DEFINABILITY OF INTEGERS IN REDUCED INDECOMPOSABLE POLYNOMIAL RINGS

MARCO BARONE, NICOLÁS CARO, AND EUDES NAZIAZENO

Abstract. We prove first-order definability of the prime subring inside polynomial rings, whose coefficient rings are (commutative unital) reduced and indecomposable. This is achieved by means of a uniform formula in the language of rings with signature $(0,1,+,\cdot)$. In the characteristic zero case, the claim implies that the full theory is undecidable, for rings of the referred type. This extends a series of results by Raphael Robinson, holding for certain polynomial integral domains, to a more general class.

§1. Introduction. Over more than 60 years, the problem of defining rational integers inside a ring has been object of extensive investigation (for an overview, we refer the reader to the surveys [15, 18, 20, 25]). Much attention has been drawn onto Diophantine definability, for this would yield a counterpart result about other versions of Hilbert's tenth problem (see [16]). More specifically, Diophantine definability implies the undecidability of polynomial equations over $\mathbb{Z}$.

In a similar vein, first-order (not necessarily Diophantine) definability of integers in a characteristic zero ring is known to imply that the full first-order theory of such a ring is undecidable. For instance, Julia Robinson showed that $\mathbb{Z}$ is first-order definable in $\mathbb{Q}$ [21]. Concerning negative results, it was recently proved [2, Lemma 4.7] that the direct product of two infinite finitely generated rings is not bi-interpretable with $\mathbb{Z}$; the proof of this result can be easily seen to contain, in its essence, the fact that $\mathbb{Z}$ is not definable in $\mathbb{Z}\times\mathbb{Z}$, for instance.

The same questions arise within the class of polynomial rings over integral domains. Raphael Robinson [22, §4d] proved the undecidability of polynomial integral domains. Jan Denef in [5, 6] proves that, given an integral domain R of characteristic zero (resp. characteristic p), the problem of solvability in $R[T]$ of polynomials with coefficients in $\mathbb{Z}[T]$ (resp. $(\mathbb{Z}/p\mathbb{Z})[T]$) is undecidable. Furthermore, Thanases Pheidas and Karim Zahidi in [19] work with the language of the rings augmented by a symbol for the nonconstant polynomials, proving undecidability of the positive existential theory of polynomial rings over integral domains. Recently, Javier Utreras proved interpretability of integers in polynomial rings over GCD domains, in a modified language [26].

However, except for the case of finitely generated $\mathbb{Z}$-algebras [2, Corollary 2.19 and Section 6.3], we have no knowledge of any attempt to extend definability and undecidability results outside the class of integral domains, partly due to the

Received October 23, 2018.
2020 *Mathematics Subject Classification*. 03C40, 13B25, 13F99, 16U99.
Key words and phrases. definability, polynomial rings, language of rings.

0022-4812/20/8504-0003
DOI:10.1017/jsl.2020.50

consistent use of field extensions of the quotient field of these rings throughout the results mentioned. In this paper, we work with polynomial rings $S = R[x]$ and formulate a criterion for the definability of the prime subring of S, that is, the smallest subring of S (denoted here by $\mathcal{Z}_S$). In the characteristic zero case, $\mathcal{Z}_S$ is exactly $\mathbb{Z}$, and in positive characteristic it coincides with some quotient $\mathbb{Z}/n\mathbb{Z}$.

We put aside the assumption that R be an integral domain, and explore a wider range of coefficient rings, which is in fact a natural class to which to extend the results, namely, the class of reduced indecomposable (commutative unital) rings (Proposition 3.5). In general, any Noetherian reduced ring can be written out as a finite product of such rings [4, Proposition 4.5.4], so we may consider these rings as the basic bricks for building up an important class of objects in commutative algebra, corresponding to the notion of connected components of reduced schemes in algebraic geometry.

This work is divided as follows:

In Section 2, we establish standard definitions and notation from Logic and Algebra that are going to be used throughout the paper, and we discuss some basic properties.

In Section 3 we explore first-order definability of sets of powers, by introducing the concept of *logical powers*, that is, a first-order property that coincides with the property of being a positive power of a given element of a ring, under some special conditions on both the element and the ring, mainly focusing on the case of polynomial rings in one variable.

In Section 4, we investigate such special conditions, and study the class of reduced indecomposable rings, proving several of its algebraic properties; we also provide examples of such rings that are not integral domains, both Noetherian and non-Noetherian.

In Section 5 we use the theory developed in Section 3 and Section 4 to construct three special definable sets of polynomials with coefficients in a reduced indecomposable ring, which are crucially used in Section 6 in the proof of the main result (by using explicit definitions for sets of powers of a fixed element).

In Section 6 we present a general criterion to define sets of exponents of powers of suitable elements. We specialize this criterion to reduced indecomposable polynomial rings, in two different versions, corresponding to two different subclasses of such polynomial rings.

The first version provides a uniform formula that ensures the definability of the prime subring, upon the condition that the nonzero integers are invertible. This condition is satisfied by all polynomial rings over a field or over reduced indecomposable rings of positive characteristic; the second one no longer relies on this condition, and it also provides a uniform formula, which works for polynomial rings over reduced indecomposable nonfields of characteristic zero.

We end Section 6 by gathering the two formulas previously obtained into a single uniform formula defining the prime subring of $S = R[x]$, for any reduced indecomposable (commutative unital) ring R.

All our results and proofs are developed in the framework of Zermelo–Fraenkel (ZF) set theory; in particular, they do not depend on AC or any choice principle.[1]

[1]However, some interesting issues concerning choice principles arise in Remark 4.4 and Examples 4.10 and 4.12.

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

§2. Preliminary definitions and notation. In this section we recall some basic notions from ring theory which will be used throughout this work (see [13] for a background). We also discuss some logical issues concerning the axioms for reduced and/or indecomposable rings, and concerning the notion of "integers" in a given ring, as well as its definability. More specifically, we distinguish between zero and positive characteristic.

All rings considered are commutative, unital and nonzero. Except in a few cases where emphasis is required, we denote the additive unit of a ring S by 0 instead of 0_S, and similarly we denote by 1 the multiplicative unit of S (instead of 1_S). Note that a ring is nonzero precisely when $1 \neq 0$.

We will work in the first-order theory in the language of rings, with signature $(+, \cdot, 0, 1)$. Unless the dependency on parameters is explicitly mentioned, by "definable" we mean "definable without parameters".

For the sake of brevity and notational convenience, whenever a subset A of a ring S (or, more generally, a property $\mathcal{P}$) is definable by a formula, say $\psi(\cdot)$, we will write "$t \in A$" (or, more generally, that "$\mathcal{P}$ holds") instead of "$\psi(t)$" in subsequent formulas; likewise, for two-variable formulas expressing binary relations $\psi(\cdot,\cdot)$ which correspond to algebraic properties, we abbreviate by using classical notation (e.g., "$s \mid t$" for divisibility).

Let S be a ring. An element $a \in S$ is said to be *nilpotent* if $a^n = 0$ for some $n \geq 1$, and *idempotent* if $a^2 = a$; in the latter case, the element $1 - a$ is idempotent as well. The ring S is said to be *reduced* if its only nilpotent element is zero, and *indecomposable*[2] if its only idempotent elements are 0 and 1.

An element $a \in S$ is said to be *regular* if, whenever $ab = ac$, with $b, c \in S$, it follows that $b = c$; otherwise, it is said to be a *zerodivisor*. Notice that invertible elements are always regular. The multiplicative group of invertible elements of S (also called *units* of S) is denoted by S^*. An *irreducible* element of S is a nonzero, noninvertible element that cannot be written as a product of two nonunits. Finally, an element p of S is *prime* if it is nonzero and noninvertible, and whenever p divides a product, it divides some of the factors.

For a ring R, we denote the polynomial ring in one indeterminate x with coefficients in R by $R[x]$, and we refer to the elements of R, that is, polynomials of degree zero, as the *constant polynomials*, or the *constants* of this larger ring (such "constants" should not be confused with the symbols of constants of the language of rings). Given $f \in R[x]$, we denote its coefficient of degree i by $f_i \in R$. Finally, we will always make clear when we need to distinguish between the element $f \in R[x]$ and its associated polynomial function $f : R \to R$.

2.1. Remarks on local rings. We say that a ring S is *local* if $a + 1$ is a unit for every nonunit a of S; for example, any polynomial ring $R[x]$ is nonlocal (take $a = x$).

If S is a local ring, then the set of nonunits of S is closed under sums, and consequently it forms an ideal in S: indeed, if $b, c \notin S^*$, then for any $z \in S$ the element $a = bz - 1$ satisfies $a + 1 = bz \notin S^*$, so necessarily $a \in S^*$. Since $-cz \notin S^*$,

[2]Also referred to, in the literature, as *directly irreducible*. Indecomposable rings are equivalently (and more customarily) defined as those not isomorphic to the direct product of two nonzero rings.

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

it follows that $a \neq -cz$, which amounts to saying that $(b+c)z \neq 1$. As z is arbitrary, this proves that $b+c$ is a nonunit.

Conversely, if the set $\mathfrak{m}$ of nonunits of a ring S forms an ideal, then S is local, because for any $a \in \mathfrak{m}$ we have $(a+1)-a = 1 \notin \mathfrak{m}$, so necessarily $a+1 \notin \mathfrak{m}$, that is, $a+1 \in S^*$.

Notice that our definition of "local ring" (as well as the equivalent characterization just proven: "nonunits form an ideal") differs from the standard definition used in commutative algebra and algebraic geometry, namely: a ring is local if it has a unique maximal ideal. We would like to stress that only our definition of "local ring" is used throughout the paper to prove the main result (concretely, in the proof of Lemma 5.7): we refrain from using the standard definition of local ring, because such a notion involves maximal ideals, and it is well-known that the existence of such ideals, in any nonzero commutative unital ring, is equivalent to the axiom of choice [10]. In particular, our main results hold unconditionally on ZF, that is, they do not rely on any choice principle.

2.2. On the theory of reduced/indecomposable rings. The existence of an idempotent element other than 0 and 1 in a ring is clearly a first-order predicate, so that the theory of indecomposable rings is finitely axiomatizable.

As a matter of fact, the same happens with reducedness, even though nilpotency cannot be expressed as a one-variable first-order formula[3]. Indeed, observe that if a is a nonzero nilpotent element of a ring and $n \geq 2$ is its nilpotency index (i.e., the least positive integer such that $a^n = 0$), then a^{n-1} is a nonzero nilpotent element with nilpotency index 2. Therefore a ring is reduced if and only if it contains no nonzero element whose square is zero, and this is obviously a first-order predicate.

Clearly, all the remaining ring-theoretic properties described at the beginning of the section, as well as *our notion* of local ring, are first-order definable in the language of rings.

2.3. The prime subring and its definability. Let S be a ring. The *prime subring* of S, denoted by $\mathcal{Z}_S$, is defined to be the smallest subring of S. It is not hard to show that $\mathcal{Z}_S \subseteq S$ is additively generated by 1_S, and it is also the image of the (unique) ring homomorphism $j : \mathbb{Z} \to S$. The *characteristic* of S, denoted by $\mathsf{char}(S)$, is defined to be the unique natural number n such that $\ker j = n\mathbb{Z}$. Thus, $\mathcal{Z}_S$ is isomorphic to $\mathbb{Z}$ if the characteristic of S is zero, and it is isomorphic to the ring $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n if $\mathsf{char}(S) = n > 0$.

This notion of "prime subring" clearly has nothing to do, and should not be confused, with the notion of "prime element" mentioned at the beginning of the section. When no ambiguity arises, we denote the prime subring $\mathcal{Z}_S$ of a ring S simply by $\mathcal{Z}$, and we may sometimes refer informally to the elements of $\mathcal{Z}$ as the "integers". For $m \in \mathbb{Z}$ we will denote $m \cdot 1_S \in S$, with a slight abuse of notation, simply by m, writing "$m \in S$". Likewise, we will informally refer to the elements of $\mathcal{Z}^+ = j(\mathbb{Z}^+)$ as the "positive integers". Notice that $\mathcal{Z}^+ = \mathcal{Z}$ when $\mathsf{char}(S) > 0$.

The main goal of this work is to prove the definability of $\mathcal{Z} \subseteq S$ for S belonging to a wide class of rings, namely, that of reduced indecomposable polynomial rings. As mentioned in the Introduction, the case of characteristic zero (when $\mathcal{Z} = \mathbb{Z}$)

[3]See [11, Exercise 8.5.1] for an example of a ring whose nilradical is not definable.

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

implies undecidability of the full theory of the corresponding ring. Regarding positive characteristic, if $\mathsf{char}(S) = n > 0$, then $\mathcal{Z} = \mathbb{Z}/n\mathbb{Z}$ is trivially definable, via the formula

$$\gamma_n(t)\colon \bigvee_{i=1}^{n} (t = \underbrace{1 + \cdots + 1}_{i \text{ times}}),$$

which depends on n in a cumbersome way. Since we are able to construct a *uniform* formula that covers all reduced indecomposable polynomial rings, regardless of the characteristic, we have in particular that, for $\mathsf{char}(S) = n > 0$, our formula does not depend on n. Obviously, in positive characteristic, our definability result does not imply undecidability of the full theory.

§3. A first-order approach to the definability of sets of powers. Let S be a ring. For an element $p \in S$, let $\mathsf{POW}(p)$ denote the set of positive powers of p. As will be clearer in Section 6, the first clue for definability of $\mathcal{Z}$ comes from the idea of "logically" identifying positive integers with the exponents of a fixed element, reducing the task to defining sets of powers of a fixed element of the ring. This has led to the search for a first-order definable notion that approximates that of "power".

3.1. Logical powers: definition and basic properties. In this subsection we introduce an intuitive notion of positive power of an element $p \in S$ as a multiple of p whose only divisors, up to units, are also multiples of p, together with an additional property which, in the case of polynomial rings and under special conditions, also guarantees monicity (as a monomial in p); this condition is encapsulated by Formula (3.1) below. An analogous approach is considered in [22, p. 145], where it is shown that the same property is satisfied precisely by the nonnegative powers of p, whenever p is a prime element and S is an integral domain (see item d of Proposition 3.4 for a slight generalization). We will explore our notion in a more general context and, for a certain type of ring S and suitable conditions on p (Theorem 5.5 and Remark 5.6), we use it to prove that the set $\mathsf{POW}(p)$ is first-order definable using p as a parameter.

Definition 3.1. Let S be a ring. Given $p \in S$, we define the set $\mathsf{LPOW}(p)$ of *logical powers* of p as the set of elements $f \in S$ satisfying:

- p divides f;
- $p - 1$ divides $f - 1$;
- every divisor of f is a unit or a multiple of p.

Observe that $\mathsf{LPOW}(p)$ is defined by the one-variable formula $\psi(\cdot, p)$, where ψ is given by

$$\psi(f,s)\colon s \mid f \wedge s - 1 \mid f - 1 \wedge \forall g[g \mid f \to (g \mid 1 \vee s \mid g)]. \tag{3.1}$$

In what follows, we explore the similarities between $\mathsf{LPOW}(p)$ (a first-order definable set) and $\mathsf{POW}(p)$ (a set that we want to be first-order definable), in order to justify the expression "logical powers". Unfortunately, in the general case the definition of $\mathsf{LPOW}(p)$ fails badly in conveying the concept of "genuine powers":

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

EXAMPLE 3.2. If $g,h \in S$ are noninvertible and h is regular, then $gh \notin \mathsf{LPOW}(gh)$. In fact, we have that h divides gh, but h is neither a unit nor a multiple of gh (if $h = qgh$, then canceling h would imply that g is a unit).

Another instance in which the two definitions clash is the following: on the one hand, $0 \in \mathsf{POW}(p)$ if and only if p is nilpotent; on the other hand, the following result characterizes whether the zero element is a logical power in nonlocal rings, a wide class of rings that includes all polynomial rings (see Section 2.1):

PROPOSITION 3.3. *Let S be a nonlocal ring. For any $p \in S$, the following are equivalent*:

a. $0 \in \mathsf{LPOW}(p)$.
b. *Both p and $p-1$ are units.*
c. $\mathsf{LPOW}(p) = S$.

PROOF.
(a $\Rightarrow$ b): We have that $p-1$ divides $0-1=-1$, so $p-1$ is a unit. As S is not local, there exists $s \in S$ such that s and $s+1$ are nonunits. Since s and $s+1$ trivially divide 0 and $0 \in \mathsf{LPOW}(p)$, they must be multiples of p. Therefore p divides $(s+1)-s=1$.
(b $\Rightarrow$ c): If both p and $p-1$ are units, then any element $t \in S$ obviously belongs to $\mathsf{LPOW}(p)$, for t, as all its divisors, is a multiple of p, whilst $p-1$ divides $t-1$.
(c $\Rightarrow$ a): Obvious. ⊣

Notice that the hypothesis in Proposition 3.3 is only used in the proof of a $\Rightarrow$ b to prove that p is a unit, whereas b $\Rightarrow$ c $\Rightarrow$ a $\Rightarrow$ "$p-1$ is a unit" holds for any ring.

3.2. Consequences of $\mathsf{LPOW}(x) = \mathsf{POW}(x)$ in $R[x]$. The findings from the previous subsection suggest that our attempt at identifying the sets $\mathsf{POW}(p)$ by $\mathsf{LPOW}(p)$ could be more successful if we avoid nilpotent and reducible elements. As a matter of fact, under certain hypotheses the two sets coincide, producing a first-order definition of the powers of some types of elements. Before proceeding in this direction, we list some general properties concerning logical powers that will be used in the sequel. At this point, one notation is worth introducing: given two elements f,p of a ring, we say that f is *infinitely divisible by p* if f is a multiple of arbitrarily large powers of p (equivalently, a multiple of all positive powers of p).

PROPOSITION 3.4. *Let S be a ring, and let $p \in S$.*

a. *Any element f of $\mathsf{LPOW}(p)$ is either infinitely divisible by p, or an element of the form up^n, for some $n \geq 1$ and some unit u satisfying $p-1 \mid u-1$. In particular, if $u=1$, then $f \in \mathsf{POW}(p)$.*
b. *If $f \in \mathsf{LPOW}(p)$ and u is a unit such that $p-1$ divides $u-1$, then $uf \in \mathsf{LPOW}(p)$.*
c. *If p is either invertible or irreducible, then $p \in \mathsf{LPOW}(p)$.*
d. *If p is regular and prime, then $\mathsf{POW}(p) \subseteq \mathsf{LPOW}(p)$.*

PROOF.
a. If f is not infinitely divisible by p, let $n \geq 1$ be the greatest exponent such that $p^n \mid f$, so that $f = up^n$ for some u not divisible by p. Since u divides f and $f \in \mathsf{LPOW}(p)$, u must be a unit. Finally, we have $f-1 = up^n - 1 = u \cdot (p^n - 1) + u - 1$, and since both $f-1$ and p^n-1 are multiples of $p-1$, so is $u-1$.

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

b. Obviously p divides uf. Since $p-1$ divides both $f-1$ and $u-1$, it follows that $p-1$ divides $u\cdot(f-1)+u-1=uf-1$. Finally, if g divides uf, then g divides $u^{-1}\cdot(uf)=f$. Since $f\in \mathsf{LPOW}(p)$, we conclude that g is a unit or a multiple of p.
c. It suffices to observe that every divisor of p would be either invertible or an associate of p (hence a multiple of p), for the other properties are trivially satisfied.
d. Let $n\geq 1$. Obviously $p \mid p^n$ and $p-1 \mid p^n-1$, and if g is a divisor of p^n, say $p^n=gh$, then p^{n+1} cannot divide h (otherwise we would have, by canceling, that p divides 1, which contradicts the primality of p). Thus, the largest k with p^k dividing h must satisfy $k\leq n$. After canceling we get $p^{n-k}=g\hat{h}$, with $\hat{h}$ not a multiple of p. If $k=n$, then g is invertible; otherwise, p divides $g\hat{h}$, so necessarily p divides g because p is prime. ⊣

In what follows we will examine the case $S=R[x]$, in order to draw some consequences from the equality $\mathsf{LPOW}(x)=\mathsf{POW}(x)$:

PROPOSITION 3.5. *Let R be a ring and consider $R[x]$, the polynomial ring in one variable over R. If $x\in \mathsf{LPOW}(x)$, then x is irreducible. If in addition one of the inclusions $\mathsf{LPOW}(x)\subseteq \mathsf{POW}(x)$ or $\mathsf{POW}(x)\subseteq \mathsf{LPOW}(x)$ holds, then R is reduced.*

PROOF. We always have that x is nonzero and noninvertible. Since x is regular, every divisor of it will also be regular, and so if $x\in \mathsf{LPOW}(x)$, then by using the contrapositive of Example 3.2 we can conclude that x is irreducible.

Let $a\in R$ with $a^n=0$ for some $n\geq 1$. We want to prove that if, in addition, $\mathsf{LPOW}(x)\subseteq \mathsf{POW}(x)$ or $\mathsf{POW}(x)\subseteq \mathsf{LPOW}(x)$, then $a=0$, obtaining in this way that R is reduced. Set $u=1-a\cdot(x-1)$. Note that u divides $1-a^n\cdot(x-1)^n=1$, that is, u is invertible, and also that $x-1$ clearly divides $u-1$. Consequently, by item b of Proposition 3.4 we have $ux\in \mathsf{LPOW}(x)$.

If $\mathsf{LPOW}(x)\subseteq \mathsf{POW}(x)$, then $ux=x^m$ for some $m\geq 1$, which forces to have $m=1$ and $u=1$, and so $a=0$. Moreover, observe that $x-a$ is not invertible and divides $x^n-a^n=x^n$, and therefore, if $\mathsf{POW}(x)\subseteq \mathsf{LPOW}(x)$ (in this case the condition $x\in \mathsf{LPOW}(x)$ is superfluous), then $x-a$ must be a multiple of x, so again $a=0$. ⊣

Thus, for a ring R, in order to have $\mathsf{LPOW}(x)=\mathsf{POW}(x)$, it is necessary that R be reduced and the polynomial x be irreducible in $R[x]$. Later we will see (Theorem 5.3) that these conditions are also sufficient, and in the course of the reasoning we will show (see Proposition 4.3) that irreducibility of the polynomial x in $R[x]$ is equivalent to indecomposability of R.

§4. Reduced and indecomposable rings and some of their algebraic properties. In this section we study some algebraic properties of reduced and/or indecomposable rings. We prove, among other things, that just as integral domains, reduced indecomposable rings have characteristic zero or prime, and we exhibit examples of such rings that are not integral domains. Finally, we prove that constant polynomial functions over infinite reduced indecomposable rings can only come from constant polynomials.

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

4.1. Expressing reducedness and indecomposability of rings in terms of the corresponding polynomial rings.

LEMMA 4.1. *Let R be a ring. Let $f, g \in R[x]$ be nonzero polynomials, and denote their degrees by d and m, respectively.*

a. *Let $h \in R[x]$, and let $k = \deg(h)$. If $f = gh$, with $d < m+k$, then for all integer i with $1 \leq i \leq m+k-d$, the ith power of the leading coefficient of g annihilates the i coefficients of h of highest degrees, that is, $h_k, \ldots, h_{k-i+1}$.*
b. *Given $h \in R[x]$ and $r \geq 0$, if x^r divides gh, then x^r divides $g_0^r h$. Moreover, $x^r = gh$ implies $g_0^r = g_0^{r+1} h_r$.*
c. *If g divides f and $m > d$, then f is annihilated by a power of g_m. More specifically, if $f = gh$ and $k = \deg(h)$, then $g_m^{k+1} f = 0$. Consequently, if R is reduced and f is regular, then $g \mid f$ implies $m \leq d$. In particular, whenever the coefficient ring is reduced, divisors of regular constant elements are themselves constants.*
d. *Suppose R is reduced and indecomposable and g divides f. If the leading coefficient of f is a unit, then that of g must be a unit too.*

PROOF.

a. Write $f = gh = (g_m x^m + \cdots + g_0)(h_k x^k + \cdots + h_0)$, with $g_m, h_k \neq 0$. It is enough to show that g_m^i annihilates h_{k-i+1} for all $i = 1, \ldots, m+k-d$, because the same argument, applied to all indices j with $1 \leq j \leq i-1$, would also prove that $g_m^i h_{k-j+1} = g_m^{i-j} \cdot (g_m^j h_{k-j+1}) = 0$, as desired.

   For $i = 1$, the claim follows from $g_m h_k = f_{m+k} = 0$ (recall that $d < m+k$). Suppose the claim holds for all indices up to i, and suppose $i+1 \leq m+k-d$. In this case we have $d < m+k-i$, and therefore $0 = f_{m+k-i} = g_m h_{k-i} + (g_{m-1} h_{k-i+1} + \cdots + g_{m-i} h_k)$. By induction hypothesis, each of the terms within the parentheses is annihilated by a power of g_m of exponent smaller than or equal to i, and therefore the whole expression between parentheses is annihilated by g_m^i. Thus, multiplying by g_m^i, one gets $g_m^{i+1} h_{k-i} = 0$, and this completes the induction.
b. The result is obvious for $r = 0$. For $r > 0$, as gh is a multiple of x^r, we have that all its coefficients in degrees $0, \ldots, r-1$ vanish, so we may apply a specular reasoning to that used in the previous item and get $0 = (gh)_0 = g_0 h_0$ and, if $r > 1, 0 = (gh)_1 = g_0 h_1 + g_1 h_0$, from which $g_0^2 h_1 = 0$ and thus g_0^2 annihilates h_0 and h_1. By proceeding analogously until $r-1$ we obtain that g_0^r annihilates $h_0, \ldots, h_{r-1}$ and therefore all coefficients of $g_0^r h$ vanish until degree $r-1$, which yields the first claim. In the special case where $x^r = gh$ we also have $1 = (gh)_r = g_0 h_r + (g_1 h_{r-1} + \cdots + g_r h_0)$; after multiplying by g_0^r, the second term of the right side vanishes, giving $g_0^r = g_0^{r+1} h_r$.
c. If $d < m$, then we can apply item a to $f = gh$ and $i = k+1 \leq m+k-d$ and get that g_m^{k+1} annihilates $h_k, \ldots, h_0$ and, consequently, annihilates h. Hence $g_m^{k+1} f = (g_m^{k+1} h) g = 0$. For the second assertion, observe that if we had $m > d$, then f would be annihilated by a power of a nonzero constant (the leading coefficient of g), which is also nonzero in a reduced ring. Therefore f would be a zerodivisor, contradicting the hypothesis. The last statement follows immediately.
d. Let $f = gh$, with $h \in R[x]$. In the case $d = m+k$ we have $f_d = g_m h_k$ and therefore, if f_d is invertible, then g_m invertible as well. In the case $d < m+k$, letting $i = m+k-d$, we may write the leading coefficient of f as

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

$u = f_d = f_{m+k-i} = g_m h_{k-i} + L$, where $L = g_{m-1}h_{k-i+1} + \cdots + g_{m-i}h_k$. The item a above may be applied to the index i (because $1 \leq i \leq m+k-d$), implying that $h_k, \ldots, h_{k-i+1}$ are annihilated by g_m^i, and therefore $g_m^i L = 0$.

If u is a unit, so is $u^i = (g_m h_{k-i} + L)^i = g_m^i h_{k-i}^i + LM$, for some $M \in R$. Multiplying by $v = u^{-i}$, we have $1 = v g_m^i h_{k-i}^i + vLM$. By setting $e = v g_m^i h_{k-i}^i$ and $e' = vLM$ we have written $e + e' = 1$, and since $g_m^i L = 0$, it follows that $ee' = 0$. Therefore e and e' are idempotent, and since R is indecomposable, one of them must be 1. We also have $g_m^i \neq 0$ because R is reduced, and since $g_m^i e' = (vM) \cdot (g_m^i L) = 0$, we conclude that e' is a zerodivisor and, consequently, $e' \neq 1$. This forces $1 = e = v g_m^i h_{k-i}^i$, and thus g_m is a unit. ⊣

PROPOSITION 4.2. *For a ring R, the following conditions are equivalent*:

a. $R[x]$ *is reduced.*
b. R *is reduced.*
c. $R[x]^* = R^*$.

PROOF. The implication a ⇒ b is obvious. For b ⇒ c, note that units are precisely the divisors of 1, which is a regular constant element, and apply the last assertion of Lemma 4.1c. Finally, if $R[x]^* = R^*$ and $f \in R[x]$ satisfies $f^m = 0$, with $m \geq 2$, then $(1 + xf^{m-1})(1 - xf^{m-1}) = 1$ implies $1 + xf^{m-1} \in R[x]^* \subseteq R$, so necessarily $f^{m-1} = 0$. Iterating this reasoning we conclude that $f = 0$, proving that $R[x]$ is reduced. ⊣

The next result relates indecomposability of a ring R to a property about its polynomial ring $R[x]$:

PROPOSITION 4.3. *A ring R is indecomposable if and only if the polynomial $x \in R[x]$ is irreducible.*

PROOF. Obviously x is nonzero and noninvertible. Suppose that R is indecomposable, and assume $x = gh$, with $g, h \in R[x]$; we want to show that either g or h is a unit. Set $e = g_0 h_1$ and $e' = g_1 h_0$. We have $e + e' = g_0 h_1 + g_1 h_0 = (gh)_1 = (x)_1 = 1$. Furthermore, by the last part of Lemma 4.1b with $r = 1$ we have $g_0^2 h_1 = g_0$, so $e^2 = (g_0 h_1)^2 = (g_0^2 h_1) h_1 = g_0 h_1 = e$, and therefore e, being idempotent, must be 0 or 1 (in a similar way one can show that e' is idempotent). If $e = 1$, then $g_0 \in R^*$; since $g_0 h_0 = (gh)_0 = (x)_0 = 0$, it follows that $h_0 = 0$, so x divides h, and dividing out the equality $x = gh$ by the regular element x, we get that g is a unit. If $e = 0$, then $e' = 1$, and proceeding analogously we conclude that $h \in R[x]^*$.

For the converse, since the only invertible idempotent f in a ring is $f = f^2 f^{-1} = f f^{-1} = 1$, if $e \in R$ is a nontrivial idempotent (i.e., other than 0 or 1), then $1 - e$ is also a nontrivial idempotent, and therefore both e and $1 - e$ are nonunits. Thus, the polynomials $g = ex + (1 - e)$ and $h = (1 - e)x + e$ have noninvertible constant term, so they cannot be units in $R[x]$. Since $x = gh$, we conclude that x is reducible. ⊣

REMARK 4.4. Notice that the argument above proves that, if x has any nontrivial factorization, then it has one as a product of two linear polynomials. Furthermore, by putting together Propositions 4.2 and 4.3, we obtain a characterization of reduced indecomposable rings in terms of a property of the polynomials 1 and x in $R[x]$: that they both be not a product of two positive degree polynomials. For those acquainted

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

with algebraic geometry, we recall the special meaning that indecomposability has in terms of the topology of the corresponding Zariski affine scheme: a ring R is indecomposable if and only if its prime spectrum $\mathsf{Spec}(R)$ is connected[4].

From the very definition of polynomials and their multiplication, it follows that 0 is the only polynomial infinitely divisible by x. This will be used in the proof of the following result, which shares the same spirit of Proposition 4.2, but concerning indecomposability:

PROPOSITION 4.5. *For any ring R, a polynomial $e \in R[x]$ is idempotent if and only if e is constant and idempotent in R. In particular, R is indecomposable if and only if $R[x]$ is indecomposable.*

PROOF. Let $e \in R[x]$ be idempotent. Writing $e = e_0 + gx$, with $g \in R[x]$, the equality $e = e^2$ becomes $e_0 + gx = e_0^2 + 2e_0gx + g^2x^2$, yielding $e_0 = e_0^2$, and in particular $(1 - 2e_0)gx = (gx)^2$. Since $(1 - 2e_0)^2 = 1$, it follows that $(1 - 2e_0)gx = [(1 - 2e_0)gx]^2$. Thus $(1 - 2e_0)gx = [(1 - 2e_0)g]^n x^n$ for all $n \geq 1$, that is, $(1 - 2e_0)gx$ is infinitely divisible by x, and so necessarily $(1 - 2e_0)gx = 0$. Since $(1 - 2e_0)x$ is regular, it follows that $g = 0$, so $e = e_0$ is idempotent in R. ⊣

From Propositions 4.2 and 4.5 we obtain the following characterization of reducedness/indecomposability for polynomial rings in an arbitrary set of indeterminates:

PROPOSITION 4.6. *Let R be a ring and let $\boldsymbol{X} = \{x_i\}_{i \in I}$ be a set of indeterminates over R. If $S = R[\boldsymbol{X}]$, then S is reduced (resp. indecomposable) if and only if R is reduced (resp. indecomposable).*

PROOF. Obviously, if S reduced (resp. indecomposable), then the subring R of S is also reduced (resp. indecomposable). Conversely, assume that R is reduced (resp. indecomposable). Given $f \in S$, there exists a finite subset $\boldsymbol{X'}$ of $\boldsymbol{X}$ such that $f \in S_0$, where $S_0 = R[\boldsymbol{X'}]$. Proposition 4.2 (resp. Proposition 4.5), together with induction, shows that S_0 is reduced (resp. indecomposable) as well, and therefore f nilpotent (resp. idempotent) implies $f = 0$ (resp. $f = 0$ or 1), which shows that S is reduced (resp. indecomposable). ⊣

Notice that, although our class of rings of the form $S = R[x]$ was initially described in terms of properties of R, we now have instead an intrinsic characterization of the same class, regardless of the presentation of $S \cong R'[\boldsymbol{X}]$ (i.e., independent of the subring R' and the set $\boldsymbol{X}$ of indeterminates over R'). Consequently, provided that a given ring is polynomial (in any set of variables), all other conditions for membership in our class are first-order axiomatizable in the language of rings (Section 2.2), without extra symbols for the coefficient ring or the indeterminates. The main result of this paper, that is, definability of the prime subring (Theorem 6.11), is therefore true for "polynomial reduced indecomposable rings".

It is trivial that, given an element of a ring that is zero or a unit, it has a positive power dividing the previous corresponding power (actually, this happens with *every*

[4]For a proof of this equivalence, see [7, Exercise 2.25]. The proof relies heavily upon the Boolean prime ideal theorem (BPI); see [12, Forms 14 AL and 14 AN].

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

positive power of it). For reduced indecomposable rings, the converse holds. This basic result will be used repeatedly, and we prove it below:

PROPOSITION 4.7. *For any reduced indecomposable ring R and any $c \in R$, we have*:

a. *If c^{m+1} divides c^m for some $m \geq 0$, then $c \in \{0\} \cup R^*$.*
b. *If $c \notin \{0\} \cup R^*$, then all nonnegative powers of c are pairwise distinct.*
c. *If R is finite, then R is a field.*

PROOF.

a. If $c^m = c^{m+1}d$, then $(cd)^m = c^m d^m = (c^{m+1}d)d^m = (cd)^{m+1}$, hence $(cd)^m = (cd)^{m+1} = \cdots = (cd)^{2m}$. Therefore $(cd)^m$ is idempotent, hence it equals 1 or 0 (because R is indecomposable). If $(cd)^m = 1$, then $c \in R^*$. Otherwise, since R is reduced, it follows that $cd = 0$, which implies $c^m = c^{m+1}d = c^m \cdot (cd) = 0$, and therefore $c = 0$ (again by reducedness of R).
b. If two nonnegative powers of an element t coincide, say $t^m = t^n$, with $0 \leq m < n$, then $t^m = t^{m+1}t^{n-m-1}$, so $t \in \{0\} \cup R^*$ by item a.
c. If R is finite, then item b implies that R coincides with $\{0\} \cup R^*$ and is therefore a field. ⊣

The following result shows that, like integral domains, reduced indecomposable rings can only have zero or prime characteristic:

PROPOSITION 4.8. *If R is a reduced indecomposable ring of positive characteristic, then R has prime characteristic. In particular, every nonzero integer in R is invertible.*

PROOF. The prime subring $\mathcal{Z}$ of R is reduced and indecomposable, since R is. If $\mathsf{char}(R) > 0$, then $\mathcal{Z}$ is finite, so $\mathcal{Z}$ is a field by Proposition 4.7c, and we know that in this case $|\mathcal{Z}| = \mathsf{char}(R)$ is a prime number. ⊣

4.2. Examples of reduced and indecomposable rings. Clearly, any integral domain is reduced and indecomposable. In this subsection we provide some examples of reduced/indecomposable rings that are not integral domains.

EXAMPLE 4.9. Let B be a ring, $p,q \in B$, and let $\mathfrak{b}$ be the ideal in B generated by pq. We are going to impose sufficient conditions on p and q in such a manner that the ring $R = B/\mathfrak{b}$ be reduced, indecomposable, and not an integral domain.

Suppose firstly that $p \nmid q$ and $q \nmid p$. This implies $pq \nmid p$ and $pq \nmid q$, hence $\mathfrak{b}$ is not prime, and so R is not an integral domain.

Furthermore, if p and q are prime, then R is reduced: for if $a \in B$ and $n \geq 1$ satisfy $pq \mid a^n$, then by primality of p and q we have $p \mid a$ and $q \mid a$, say $a = sp = tq$. As q is prime and $q \nmid p$, we necessarily have $q \mid s$, which shows that $pq \mid a$.

If in addition the ideal $Bp + Bq$ in B is proper, then R is also indecomposable. In fact, if $a \in B$ satisfies $pq \mid (a-1)a$, then p must divide a or $a-1$, and the same for q. If p and q do not divide the same factor, then $1 = a - (a-1) \in Bp + Bq$, which contradicts our assumption. Therefore p and q both divide the same factor, being it either a or $a-1$, which implies $pq \mid a^2$ or $pq \mid (a-1)^2$. As we already proved reducedness of $B/(pq)$, either $pq \mid a$ or $pq \mid a-1$, as desired.

As concrete examples of rings satisfying the conditions above, we can take $B = \mathbb{Z}[t], p = 2, q = t$, or $B = \mathbb{Q}[s,t], p = s, q = t$. In the latter case, we obtain an example

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

of reduced indecomposable characteristic zero ring R which is not a field, but such that every nonzero integer is invertible.

As a final remark, we could replace the hypotheses "$p \nmid q$ and $q \nmid p$" by "q is regular and $q \nmid p$", obtaining the same results.

EXAMPLE 4.10. For a nonempty set X and a ring B, let $S = B^X$ be the set of B-valued functions on X. Endowed with componentwise addition and product, S is a ring. On the one hand, if B is reduced, then so is any subring of S; on the other hand, if B is indecomposable, then the idempotent elements of a given subring of S are precisely those functions that take only the values 0 and 1.

If B is a reduced indecomposable topological ring such that its singletons are closed sets (i.e., endowed with a T_1 topology), and X is a connected topological space, then $R = \mathcal{C}(X,B)$, the subring of S of B-valued continuous functions on X, is indecomposable: for if $f \in R$ is idempotent, then $X = f^{-1}(\{0\}) \cup f^{-1}(\{1\})$ is the disjoint union of two closed sets, so by connectedness of X we must have that f is constant.

Consequently, the existence in R of two continuous functions with disjoint supports provides examples of reduced indecomposable rings that are not integral domains. The last condition is guaranteed in many cases: for instance, if $B = \mathbb{R}$, this holds whenever X separates some pair of disjoint closed sets, which is the case if X is a metric space or a completely regular space or, under certain standard assumptions, whenever X is a normal space[5].

EXAMPLE 4.11. Consider the subring R of $\mathbb{Z} \times \mathbb{Z}$ consisting of those pairs (m,n) with $m \equiv n \pmod 2$. Since $\mathbb{Z} \times \mathbb{Z}$ is reduced, so is R. Moreover, the idempotents in $\mathbb{Z} \times \mathbb{Z}$ are precisely $(0,0),(1,1),(1,0)$ and $(0,1)$; since $(1,0),(0,1) \notin R$, it follows that R is indecomposable.

Notice that the main result of this paper (Theorem 6.11) implies that $\mathbb{Z}$ is definable in the subring $R[x]$ of the ring $(\mathbb{Z} \times \mathbb{Z})[x] \cong \mathbb{Z}[x] \times \mathbb{Z}[x]$, where R is as described in Example 4.11. In this line of thought, the reader may wonder whether $\mathbb{Z}$ is definable in $(\mathbb{Z} \times \mathbb{Z})[x]$. Nevertheless, one can extract from the proof of [2, Lemma 4.7] that this is not the case (actually, that $\mathbb{Z}$ is not even definable in $A \times B$, whenever A and B are characteristic zero rings[6]). In other words, the condition on the subring R in Example 4.11 is essential for the definability of $\mathbb{Z}$ in $R[x]$.

Example 4.11 is just a special case of the following more general class of examples:

EXAMPLE 4.12. Let B be a reduced indecomposable ring which is not a field (e.g., an integral domain such as $\mathbb{Z}$ or $\mathbb{F}_p[t], p$ prime), and let $\mathfrak{b}$ be a nonzero proper ideal in B. Given a set I with more than one element, let $R \subseteq B^I$ be the set of I-tuples whose entries are pairwise congruent modulo $\mathfrak{b}$. Since B^I is reduced, so is R. The set of idempotents in B^I is precisely $\{0,1\}^I$ and, since $\mathfrak{b}$ is a proper ideal, it follows that $\{0,1\}^I \cap R = \{0_R, 1_R\}$, which shows that R is indecomposable.

[5]Urysohn's lemma cannot be proved in ZF [8, Corollary 2.2]: the usual proof of this result relies on DC. However, as shown in [3, p. 55], it suffices to use DMC, the axiom of dependent multiple choice [12, Form 106 A].

[6]See [1] for another proof in the case $A = B = \mathbb{Z}$.

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

Finally, for each $i \in I$, denote by e_i the ith canonical I-tuple in B^I taking value 1 at position i and 0 elsewhere. If c is a nonzero element in $\mathfrak{b}$, then R contains two nonzero elements of the form ce_i and ce_j, with $i, j \in I$ and $i \neq j$, whose product is 0, and this shows that R is not an integral domain.

Unless I is finite[7], the ring R in Example 4.12 is not, in general, Noetherian: indeed, if I contains a denumerable subset $\{i_n : n \in \mathbb{N}\}$ (i.e., if I is Dedekind-infinite), c is a nonzero element of $\mathfrak{b}$ and $\mathfrak{c}_n \subseteq R$ is the ideal generated by $ce_{i_0}, \ldots, ce_{i_n}$, then the ascending chain of ideals $(\mathfrak{c}_n)_{n\in\mathbb{N}}$ is not stationary[8].

The reader may notice that the technique shown in Example 4.12 also provides examples in positive characteristic (which is necessarily prime, by Proposition 4.8). More specifically, for each p prime, the following ring is reduced and indecomposable, has characteristic p, and it is not an integral domain:

$$R = \{(f,g) \in \mathbb{F}_p[t] \times \mathbb{F}_p[t] : t \mid f - g\}.$$

Example 4.13. Let R be a local ring (see Section 2.1). If $a \in R$ is idempotent, then $(a-1)a = 0$; since one of $a-1$ or a is a unit, it follows that $a = 0$ or $a - 1 = 0$, which proves that R is indecomposable. This provides more examples of reduced indecomposable rings which are not integral domains, obtained as suitable localizations of further rings at prime ideals[9], such as the germs of rational functions at points lying in more than one irreducible component of a (reduced) algebraic set (e.g., $R = \left(\mathbb{C}[x,y]/(xy)\right)_{(\overline{x},\overline{y})}$).

4.3. Polynomials *versus* polynomial functions. In this subsection we address the relationship between polynomials in one variable and their corresponding polynomial functions. More specifically, we want to provide a sufficient condition on the coefficient ring that ensures that polynomial constant functions can only come from constant polynomials.

If R is a finite ring, then the nonzero polynomial $\prod_{r\in R}(x - r)$ is zero as a function on R, so we may restrict our discussion to infinite rings. If D is an integral domain, then any nonzero polynomial $f \in D[x]$ can only have finitely many roots; in particular, if D is infinite, then f does not vanish identically on R (as a polynomial function). For infinite reduced indecomposable rings, the set of roots of a nonzero polynomial may be infinite (take for instance the reduced indecomposable ring of characteristic zero $R = \mathbb{Z}[t]/(2t)$ in Example 4.9, and consider the polynomial $\overline{t} \cdot (x^2 + x) \in R[x]$, vanishing at all integers), yet it can never be all of R, as the following result shows[10].

---

[7] If $\mathfrak{b} = Rc$ is principal and $I = \{1, \ldots, n\}$, then R is the image of the ring $B[x_1, \ldots, x_n]$ under the ring homomorphism $f \mapsto \big(f(ce_1), \ldots, f(ce_n)\big)$. Thus, B being Noetherian implies that R is Noetherian as well.

[8] If I is merely infinite, then we can only prove that R has a nonfinitely generated ideal, namely, that one generated by all the I-tuples ce_i. See [9, Section 3] for a comparison, in ZF, of the various notions of Noetherianity.

[9] If A is a ring and $\mathfrak{p}$ is a prime ideal in A, then the localization $R = A_{\mathfrak{p}}$ is local. In fact, if $a \in A$ and $s \in A \setminus \mathfrak{p}$ are such that a/s is not a unit in R, then necessarily $a \in \mathfrak{p}$, and thus $a + s \in A \setminus \mathfrak{p}$. Therefore $(a/s) + 1 = (a+s)/s$ is invertible in R.

[10] See [23] for a general condition, and [27] for a second-order topological proof, which relies on different notions of Noetherianity (whose equivalence depends on DC) and connectedness of the prime spectrum (which depends on BPI).

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

THEOREM 4.14. *Let R be a reduced indecomposable ring. Assume that R is infinite, and let $f \in R[x]$. If $f(c) = 0$ for all $c \in R$, then $f = 0$.*

PROOF. The case of integral domains was just discussed, so we may assume that R is not a field. Write $f = f_m x^m + \cdots + f_0 \in R[x]$, with $m \geq 0$. For $c_0, \ldots, c_m \in R$, let $V(c_0, \ldots, c_m)$ be the Vandermonde matrix associated to these elements, that is, the matrix with rows indexed from 0 to m, the ith row being equal to $(1, c_i, c_i^2, \ldots, c_i^{m-1}, c_i^m)$, and for $a \in R$, let $V_a = V(a^0, a^1, \ldots, a^m)$.

We claim that if $a \det(V_a) = 0$, then $a \in \{0\} \cup R^*$: in fact, recall that $\det(V_a) = \prod_{0 \leq i < j \leq m}(a^i - a^j)$. Since $a^i - a^j = a^i \cdot (1 - a^{j-i})$ for each i and j with $0 \leq i < j \leq m$, it follows that $\det(V_a) = a^k[1 - ag(a)]$ for some $k \geq 1$ and some $g \in \mathbb{Z}[x]$. Therefore $a \det(V_a) = 0$ becomes $a^{k+1} = a^{k+2} g(a)$, and the claim follows from item a of Proposition 4.7.

If w denotes the column vector with entries $f_0, \ldots, f_m$, and $V = V(c_0, \ldots, c_m)$, where $c_0, \ldots, c_m$ are arbitrary constants, then Vw is the column vector with entries $f(c_0), \ldots, f(c_m)$, so that $Vw = 0$. Multiplying this equality by the adjugate of V yields $\det(V)w = 0$, and so for each i we have $f_i \det(V) = 0$ for any choice of elements $c_0, \ldots, c_m \in R$; in particular $f_i \det(V_{f_i}) = 0$, and consequently $f_i \in \{0\} \cup R^*$. Thus, to prove that all coefficients of f are zero, it suffices to show that none of them is invertible.

If some f_i were invertible, then $\det(V) = f_i^{-1} \cdot [f_i \det(V)] = 0$ for all $c_0, \ldots, c_m \in R$. Consequently $a \det(V_a) = 0$ for all $a \in R$, so $R = \{0\} \cup R^*$, contradicting the assumption that R is not a field. ⊣

Notice that, in the previous result, none of the two conditions (indecomposability and reducedness) can be removed from the hypothesis. We provide counterexamples in both directions. On the one hand, infinite Boolean rings such as $R = \mathbb{F}_2^{\mathbb{N}}$ are reduced but not indecomposable and the nonzero polynomial $x^2 - x$ vanishes everywhere as a function. On the other hand, $R = \mathbb{F}_2[\{x_i\}_{i \in \mathbb{N}}] / (x_i x_j)_{i,j \in \mathbb{N}}$ is indecomposable but not reduced, and the polynomial $(x^2 - x)^2$ is null as a function.

§5. Logical powers in reduced and indecomposable polynomial rings.

In this section we study the properties of the logical powers (see Definition 3.1) of a polynomial for reduced and/or indecomposable coefficient rings.

5.1. Powers *versus* logical powers.

LEMMA 5.1. *Let R be a reduced ring. If $p \in R[x]$ is nonconstant, then no element of $\mathsf{LPOW}(p)$ can be infinitely divisible by p. If in addition the leading coefficient of p is regular, then $\mathsf{LPOW}(p) \subseteq \mathsf{POW}(p)$.*

PROOF. Let $d = \deg(p)$ and $c \neq 0$ be the leading coefficient of p. Since R is reduced, the leading coefficient of p^r is $c^r \neq 0$, for all $r \geq 1$. Moreover, as $d > 0$, for any given $f \in \mathsf{LPOW}(p)$ we may find $r \geq 1$ such that $\deg(p^r) = rd > \deg(f)$.

Suppose by contradiction that f be infinitely divisible by p, and hence divisible by p^r. Item c of Lemma 4.1 ensures then that f is annihilated by some power of c, say c^s. Setting $\ell = 1 + c^s p$, we find that ℓ divides f (as $\ell f = f$) and that p does not divide ℓ (otherwise p would be a nonconstant invertible polynomial, contradicting Proposition 4.2). Therefore, as $f \in \mathsf{LPOW}(p)$, we must have that ℓ

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

is invertible. However, we have that $\ell = c^s p + 1$ is nonconstant, having coefficient $c^{s+1} \neq 0$ in degree $d > 0$, and so it cannot be invertible (again by Proposition 4.2), a contradiction.

After proving that any $f \in \mathsf{LPOW}(p)$ cannot be infinitely divisible by p, item a of Proposition 3.4 guarantees that f has the form up^n, for some integer $n \geq 1$ and a unit u satisfying $p - 1 \mid u - 1$. As u is constant (Proposition 4.2) and $p - 1$ has positive degree and leading coefficient c, again by Lemma 4.1c we have that $u - 1$ is annihilated by a power of c. Finally, if c is regular, then $u - 1$ must be zero and $f \in \mathsf{POW}(p)$, proving the second assertion. ⊣

Corollary 5.2. *If R is reduced and $p \in R[x]$ is nonconstant, prime, and it has a regular leading coefficient, then* $\mathsf{LPOW}(p) = \mathsf{POW}(p)$. *In particular* $\mathsf{LPOW}(x) = \mathsf{POW}(x)$ *when R is an integral domain.*

Proof. The fact that the leading coefficient of p is regular implies that p is regular, and therefore we can apply Proposition 3.4d to obtain $\mathsf{POW}(p) \subseteq \mathsf{LPOW}(p)$. The reverse inclusion follows from Lemma 5.1. ⊣

The requirement that $\mathsf{LPOW}(x) = \mathsf{POW}(x)$, together with the technique shown in Lemma 6.3, could be at the base of a specific strategy for definability of integers in polynomial rings. However, Corollary 5.2 above only guarantees that $\mathsf{LPOW}(x) = \mathsf{POW}(x)$ for integral domains, where the issue of definability of integers has already been worked out, in a Diophantine way [24, Theorem 5.1]. Fortunately, we now have all the tools to characterize the rings R such that, in the polynomial ring $R[x]$, the equality $\mathsf{LPOW}(x) = \mathsf{POW}(x)$ holds, obtaining in this way the converse of Proposition 3.5:

Theorem 5.3. *Let R be a ring and consider $R[x]$, the polynomial ring in one variable over R.*

a. *If R is reduced, then* $\mathsf{LPOW}(x) \subseteq \mathsf{POW}(x)$.
b. $\mathsf{POW}(x) = \mathsf{LPOW}(x)$ *if, and only if, R is reduced and indecomposable.*

Proof.

a. This follows immediately from Lemma 5.1.
b. If $\mathsf{LPOW}(x) = \mathsf{POW}(x)$, then Propositions 3.5 and 4.3 together imply that R is reduced and indecomposable.

   Conversely, suppose that R is reduced and indecomposable. For every $r \geq 1$ we have that x divides x^r and $x - 1$ divides $x^r - 1$. Suppose that $x^r = gh$, with $g, h \in R[x]$. Following notation as in the beginning of Section 2, we are denoting by g_0 the constant term of g and by h_r the coefficient of x^r in h. Using Lemma 4.1b , we get that x^r divides $g_0^r h$ and $g_0^r = g_0^{r+1} h_r$, hence $g_0 \in \{0\} \cup R^*$ by Proposition 4.7a.

   If $g_0 = 0$, then x divides g. Otherwise, x^r divides $g_0^{-r} \cdot (g_0^r h) = h$, say $h = x^r \hat{h}$, hence $x^r = gh = x^r g\hat{h}$; canceling out x^r we conclude that g is invertible. This shows that $x^r \in \mathsf{LPOW}(x)$ for all $r \geq 1$, that is, $\mathsf{POW}(x) \subseteq \mathsf{LPOW}(x)$, and the reverse inclusion follows from item a. ⊣

Next, we try to distinguish by a logical formula some elements of $R[x]$ whose logical powers coincide with their positive powers. To this end, it is necessary to

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

exclude elements exhibiting logical powers infinitely divisible by them. One way of doing so, which will be presented in the following subsection, relies on producing a first-order equivalent of the concept of "powers of two given elements have the same exponent", and exploits and extends the fact that, under reasonable conditions, for polynomials p and q we have that $p-q$ divides p^m-q^n if and only if $m=n$.

5.2. Some convenient sets whose elements have definable sets of powers. The goal of this subsection is to construct special definable subsets of a ring S, which will end up being useful throughout the paper. When $S=R[x]$, with R reduced and indecomposable, the elements of such sets will turn out to have definable sets of powers. If in addition R is not a field, we are able to show that every constant element in S also has a definable set of powers.

DEFINITION 5.4. For a ring S, we define the following sets:

- T is the set of elements $p \in S$ such that p is irreducible and $ph \in \mathsf{LPOW}(p)$ whenever $h \in \mathsf{LPOW}(p)$.
- U is the set of elements $p \in T$ such that:
  - For every $q \in T$ and every $f \in \mathsf{LPOW}(p)$, there exists $g \in \mathsf{LPOW}(q)$ such that $p-q \mid f-g$;
  - If $a \in S^*$ satisfies $p-1 \mid a-1$, then $a=1$.
- P is the set of elements $p \in U$ such that $p-1$ is regular.

Observe that the sets T, U and P are first-order definable and $P \subseteq U \subseteq T$. Since irreducible elements are noninvertible by definition, it follows that the sets in Definition 5.4 consist of nonunits.

THEOREM 5.5. *Let S be a ring and let T, U and P as in Definition 5.4. For all $q \in T$ we have $\mathsf{POW}(q) \subseteq \mathsf{LPOW}(q)$. In addition, if $S=R[x]$, with R reduced and indecomposable, then the following hold*:

a. *P is nonempty*; *more specifically, we have $x \in P$.*
b. *$\mathsf{LPOW}(p)=\mathsf{POW}(p)$ for every $p \in U$.*

PROOF. If $q \in T$, then q is irreducible, hence $q \in \mathsf{LPOW}(q)$ by Proposition 3.4c, and if we assume inductively that $m \geq 1$ satisfies $h=q^m \in \mathsf{LPOW}(q)$, then $q^{m+1}=qh \in \mathsf{LPOW}(q)$, by the definition of T. This shows that $\mathsf{POW}(q) \subseteq \mathsf{LPOW}(q)$.

Suppose that $S=R[x]$, with R reduced and indecomposable.

a. First, we prove that $x \in T$. Since R is indecomposable, x is irreducible by Proposition 4.3. Moreover, as R is also reduced, it follows from Theorem 5.3b that $\mathsf{LPOW}(x)=\mathsf{POW}(x)$. Therefore $x \in \mathsf{POW}(x)=\mathsf{LPOW}(x)$, and if $h \in \mathsf{LPOW}(x)=\mathsf{POW}(x)$, then $h=x^k$ for some $k \geq 1$, hence $xh=x^{k+1} \in \mathsf{POW}(x)=\mathsf{LPOW}(x)$. Thus, $x \in T$, as desired.

   Regarding the remaining conditions for membership in U, given $q \in T$ and $f \in \mathsf{LPOW}(x)$, we want to find $g \in \mathsf{LPOW}(q)$ such that $x-q$ divides $f-g$. Since $\mathsf{LPOW}(x)=\mathsf{POW}(x)$, we have $f=x^n$ for some $n \geq 1$. Moreover, we already know that $q \in T$ implies $\mathsf{POW}(q) \subseteq \mathsf{LPOW}(q)$, and so by taking $g=q^n$, we get $g \in \mathsf{LPOW}(q)$, and clearly $x-q$ divides $x^n-q^n=f-g$. Finally, let

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

$a \in S^*$ be such that $x-1$ divides $a-1$. By Proposition 4.2 we have $S^* \subseteq R$, and therefore a is constant. Writing $a-1=(x-1)\ell$, we can evaluate at $x=1$ to conclude $a=1$. Consequently, $x \in U$.

In order to achieve the claim, it just remains to observe that $x-1$ is always a regular polynomial.

b. If $p \in U$, then $p \in T$, and consequently $\mathsf{POW}(p) \subseteq \mathsf{LPOW}(p)$. For the reverse inclusion, let $f \in \mathsf{LPOW}(p)$ and set $q = x \in T$. The first condition in the definition of U guarantees the existence of an element $g \in \mathsf{LPOW}(q) = \mathsf{LPOW}(x) = \mathsf{POW}(x)$ such that $p-x \mid f-g$, say $g=x^n$, with $n \geq 1$.

If f were infinitely divisible by p, then p would be constant by Lemma 5.1. Evaluating at p and using that $x-p$ divides x^n-f, we conclude that $f(p)=p^n$. Since f is infinitely divisible by p, there is an h such that $f=p^{n+1}h$; in particular we have $f(p)=p^{n+1}h(p)$, so p^{n+1} divides p^n. Proposition 4.7a would imply then that $p \in \{0\} \cup R^*$, which is absurd since p is irreducible.

The contradiction above, together with item a of Proposition 3.4, shows that $f=ap^k$ for some $k \geq 1$ and some $a \in R[x]^*$ with $p-1 \mid a-1$; the second condition of the definition of U forces $a=1$ and, consequently, $f=p^k \in \mathsf{POW}(p)$. ⊣

REMARK 5.6. Let S be any ring. If θ is a ring automorphism of S, then θ preserves the logical structure, and therefore the definable sets T, U and P of Definition 5.4 are invariant under θ, that is, $\theta(T)=T, \theta(U)=U$ and $\theta(P)=P$. If $S=R[x], v \in R^*$ and $r \in R$, then the mapping $\theta\colon S \to S$ given by $\theta(f)=f(vx+r)$ is a ring automorphism ($g \mapsto g\left(v^{-1}\cdot(x-r)\right)$ being its inverse). If R is reduced and indecomposable, then $x \in P$ by Theorem 5.5a, and therefore we have $vx+r \in P \subseteq U$ in this case.

The last result of this subsection (Theorem 5.8) ensures definability of sets of powers of any fixed constant, using the corresponding constant as a parameter, for reduced indecomposable coefficient rings that are not fields. Before proceeding, we need the following technical result:

LEMMA 5.7. *Let R be a ring. If R is not a field, then at least one of the following holds*:

- *There exists a unit u with $u-1 \notin \{0\} \cup R^*$.*
- *Every element of R is the sum of two nonunits.*

PROOF. If R is local (see Section 2.1), then, as it is not a field, we may take $z \notin \{0\} \cup R^*$, so that $u=z+1$ must be a unit, satisfying the first property. If R is not local, then nonunits are not closed under sum. Hence, some unit w must be the sum of two nonunits, say x and y, and therefore for any $r \in R$ we have that $r=rw^{-1}w=(rw^{-1}x)+(rw^{-1}y)$ is the sum of two nonunits. ⊣

THEOREM 5.8. *Let $S=R[x]$, with R being a reduced indecomposable ring that is not a field, and let U be as in Definition 5.4. Given $f \in S$ and $a \in R$, we have that $f \in \mathsf{POW}(a)$ if, and only if, for all $p,q \in U$, there exist $y \in \mathsf{POW}(p)$ and $z \in \mathsf{POW}(q)$, such that*:

- $p-a \mid y-f$;
- $q-a \mid z-f$;
- $p-q \mid y-z$.

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

PROOF. If $f = a^n$, with $n \in \mathbb{Z}^+$, then for any $p,q \in U$, by taking $y = p^n$ and $z = q^n$, one clearly has $p-a \mid y-f, q-a \mid z-f$ and $p-q \mid y-z$. Conversely, let $f \in R[x]$ satisfy the properties listed. We will prove that f is constant as a function on R.

Given any two $\rho,\sigma \in R$ and any $\upsilon \in R^*$, define the polynomials $p = x-\rho+a$ and $q = \upsilon x-\sigma+a$ and observe that both p and q lie in U (see Remark 5.6). By the properties listed in the hypothesis, there exist elements $y = p^m = (x-\rho+a)^m$ and $z = q^n = (\upsilon x-\sigma+a)^n$, where m and n are suitable positive integers depending on p and q (and, of course, on a), satisfying

- $x-\rho+a-a \mid (x-\rho+a)^m - f$;
- $\upsilon x-\sigma+a-a \mid (\upsilon x-\sigma+a)^n - f$;
- $(x-\rho+a)-(\upsilon x-\sigma+a) \mid p^m - q^n$,

which yields:

- $f(\rho) = a^m$;
- $f(\upsilon^{-1}\sigma) = a^n$;
- $(1-\upsilon)x+(\sigma-\rho) \mid (x-\rho+a)^m - (\upsilon x-\sigma+a)^n$.

In particular we have $f(0) \in \mathsf{POW}(a)$ (just take $\rho = 0, \sigma = 0$ and $\upsilon = 1$).

Fix a triplet (ρ,σ,υ) and take any $m = m(\rho,\sigma,\upsilon)$ and $n = n(\rho,\sigma,\upsilon)$ satisfying the conditions above. If $m \neq n$, then $(x-\rho+a)^m - (\upsilon x-\sigma+a)^n$ has invertible leading coefficient, being 1 or $-\upsilon^n$, and therefore, by Lemma 4.1d, the last condition can only be satisfied if the leading coefficient of $(1-\upsilon)x+(\sigma-\rho)$ is also invertible. If this does not happen, then we must have $m = n$ and therefore $f(\rho) = a^m = a^n = f(\upsilon^{-1}\sigma)$.

The above reasoning amounts to saying that, given any $\rho,\sigma \in R$ and any $\upsilon \in R^*$, if any of the following conditions holds:

(a) $\upsilon \neq 1$ and $\upsilon - 1 \notin R^*$;
(b) $\upsilon = 1$ and $\rho - \sigma \notin R^*$,

then $f(\rho) = f(\upsilon^{-1}\sigma)$.

Take any $r \in R$: we want to prove that $f(r) = f(0)$. By Lemma 5.7, either there exists a unit u with $u-1 \notin \{0\} \cup R^*$ or any element of R is the sum of two nonunits. In the first case, condition (a) is satisfied for $\upsilon = u$; taking $\rho = r$ and $\sigma = 0$ we conclude that $f(r) = f(\rho) = f(\upsilon^{-1}\sigma) = f(0)$. In the second case, there are two nonunits s and t such that $r = s+t$. Set $\upsilon = 1$. Considering $\rho = r$ and $\sigma = s$, we can use (b) to prove that $f(r) = f(1^{-1}\cdot s) = f(s)$. Analogously, considering $\rho = s$ and $\sigma = 0$, we can use (b) again to prove that $f(s) = f(1^{-1}\cdot 0) = f(0)$. Thus, $f(r) = f(s) = f(0)$.

We have proven that, in both cases, $f(r) = f(0)$. As r was arbitrarily taken, it follows that f is constant as a function on R. Since R is reduced and indecomposable but not a field, it follows from Proposition 4.7c that R is infinite, and thus Theorem 4.14 ensures that $f = f(0) \in \mathsf{POW}(a)$. ⊣

REMARK 5.9. Let $S = R[x]$ be as in Theorem 5.8. We have that the sets of powers of elements of U coincide with their corresponding sets of logical powers (Theorem 5.5b), and therefore they are definable, using the corresponding elements as parameters; see Formula (3.1). Since the condition in the statement of Theorem 5.8 involves quantification over the definable set U, we get that the set of positive

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

powers of any constant $a \in R$ is definable in $R[x]$ using a as a parameter. In other words, we proved the following:

COROLLARY 5.10. *Let $S = R[x]$, with R being a reduced indecomposable ring that is not a field. There is a two-variable first-order formula $\Phi(\cdot,\cdot)$ such that, for each $a \in R$, the formula $\Phi(\cdot,a)$ defines the set $\mathsf{POW}(a)$ in S. More explicitly, we can take*

$$\Phi(t,a)\colon \forall p \forall q \big([p \in U \wedge q \in U] \to \exists y \exists z [y \in \mathsf{LPOW}(p) \wedge z \in \mathsf{LPOW}(q) \\ \wedge p - a \mid y - t \wedge q - a \mid z - t \wedge p - q \mid y - z]\big).$$

§6. The main results. We end this paper by proving the definability of the prime subring of $R[x]$, whenever R is a reduced indecomposable ring. Clearly it is sufficient to define just the subset $\mathcal{Z}^+$ of positive integers in S. We will initially express the class of reduced indecomposable coefficient rings as a union of two subclasses, for each of which we produce a uniform formula defining $\mathcal{Z}^+$. Once this is done, we manipulate the two formulas obtained and merge them, in a convenient way, into a unified formula that covers the whole class.

6.1. Defining sets of exponents: the first steps. In this subsection we provide a first-order technique for extracting "approximate" exponents from sets of powers, in the sense that, given a suitable element p in a ring S, the (images in $\mathcal{Z}^+$ of the) exponents of its powers are determined modulo $p-1$. Of course, we are interested in extracting the "actual" images in $\mathcal{Z}^+$ of the exponents (not only their classes modulo $p-1$). This will be done in the two next subsections in two different ways, according to whether every nonzero element of the prime subring is invertible, or the coefficient ring is a nonfield of characteristic zero.

We remind the reader that, if n is a positive integer (e.g., when appearing as an exponent), then the symbol n is also conventionally used in this work to denote the element $n \cdot 1_S$ in S, as discussed in Section 2.3.

DEFINITION 6.1. Let S be a ring, $p \in S$ and $B \subseteq \mathsf{POW}(p)$. We define the sets

$$\log_p B = \{n \in \mathcal{Z}^+ \colon p^n \in B\},$$
$$\log_p B + (p-1)S = \{n + (p-1)s \colon n \in \log_p B, s \in S\}.$$

Notice that $\log_p B + (p-1)S$ is precisely the set of elements $t \in S$, such that $p-1$ divides $t-n$, for some $n \in \log_p B$.

In what follows, given a formula defining a set B of powers of a fixed element p such that $p-1$ is regular, we provide a formula that defines the set $\log_p B + (p-1)S$. Before we state our preliminary result we define, for $p \in S$ and $n \in \mathbb{Z}^+$, the element

$$w_n(p) = p^{n-1} + p^{n-2} + \cdots + p + 1 \in S.$$

Observe that $w_n(p)$ satisfies the equality $(p-1)w_n(p) = p^n - 1$. Moreover, writing $w_n(p)$ as

$$w_n(p) = \begin{cases} 1, & \text{if } n = 1; \\ n + (p-1)\sum_{k=0}^{n-2} (n-1-k)p^k, & \text{otherwise,} \end{cases}$$

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

it follows immediately that $p-1$ divides $w_n(p)-n$. These relations are used crucially to prove the main results of this section. We begin our reasoning by introducing a formula, together with a lemma that makes its meaning clearer.

DEFINITION 6.2. For a two-variable formula β, we define the four-variable formula

$$L_\beta(t,p,y,w)\colon \beta(y,p)\wedge y-1=(p-1)w\wedge p-1\mid w-t.$$

Given a ring S, we denote by B_p the subset of S defined by $\beta(\cdot,p)$.

LEMMA 6.3. *Let S be a ring, and let $p\in S$ with $p-1$ regular. With notation as in Definition 6.2, suppose that $B_p\subseteq \mathsf{POW}(p)$.*

a. *Given $t,y,w\in S$, we have that $L_\beta(t,p,y,w)$ holds if, and only if, there exists $n\in \log_p B_p$ such that*
   - $y=p^n$,
   - $w=w_n(p)$, *and*
   - $p-1$ *divides* $t-n$.

b. *The formula $\exists y\exists w L_\beta(\cdot,p,y,w)$ defines the set $\log_p B_p+(p-1)S$ of elements $t\in S$, such that $p-1$ divides $t-n$ for some $n\in \log_p B_p$ (see Definition 6.1).*

PROOF. We will use the fact that the element $w_n(p)=(p^n-1)/(p-1)$ is congruent to n modulo $p-1$, which, together with the hypotheses, will allow us to recover the value n modulo $p-1$ from the expression p^n-1 in a definable way.

a. Observe that $L_\beta(t,p,y,w)$ holds if and only if there exists a positive integer n satisfying:
   - $y=p^n\in B_p$ (recall that $B_p\subseteq \mathsf{POW}(p)$ by hypothesis),
   - $y-1=(p-1)w$, and
   - $p-1$ divides $w-t$.

   The chain of equalities

   $$(p-1)w_n(p)=p^n-1=y-1=(p-1)w,$$

   together with the regularity of $p-1$, implies that the only possible such value of w is $w_n(p)$. Thus, $L_\beta(t,p,y,w)$ holds if and only if there exists $n\in \log_p B_p$ such that
   - $y=p^n$,
   - $w=w_n(p)$, and
   - $p-1$ divides $w_n(p)-t$.

   Finally, recall that $p-1$ divides $w_n(p)-n$, so $p-1$ divides $w_n(p)-t$ if and only if $p-1$ divides $[w_n(p)-n]-[w_n(p)-t]=t-n$.

b. If $\exists y\exists w L_\beta(t,p,y,w)$ holds, then item a implies that $p-1$ divides $t-n$, for some $n\in \log_p B_p$, and therefore $t=n+(t-n)\in \log_p B_p+(p-1)S$. Conversely, if $t=m+(p-1)s$, with $m\in \log_p B_p$ and $s\in S$, then $L_\beta(t,p,y,w)$ is satisfied by taking $y=p^m$ and $w=w_m(p)$. ⊣

In our setting we have $S=R[x]$, with R reduced and indecomposable, and we are interested in using the elements p of the form $p=x-r+1$, with $r\in R$, which satisfy the property that $p-1$ is regular. For any such choice of p, if $L_\beta(t,p,y,w)$ holds, then

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

by Lemma 6.3a we have $x - r = p - 1 \mid t - n$, for some $n \in \mathcal{Z}^+$ possibly depending on r, which amounts to saying that t, seen as polynomial function, satisfies $t(r) = n \in \mathcal{Z}^+$.

In order to obtain from L_β a formula that corresponds to "$t \in \mathcal{Z}^+$", we must necessarily bind the variables y, z and p. First, we quantify existentially over y and w, obtaining an auxiliary value $n \in \log_p B_p$, and afterwards we vary p in a suitable definable subset containing all the linear polynomials $x - r + 1$, with $r \in R$. The first step, besides leaving n dependent on p, only specifies it modulo $p - 1$. To fix this issue, we will express the class of reduced indecomposable polynomial rings as the union of two subclasses, for each of which a different technique defining $\mathcal{Z}^+$ is introduced. Both techniques involve making further restrictions on t. This will allow us, all in all, to cover our whole class of rings. We point out that the two subclasses considered do indeed overlap, so in particular some of our rings may be treated by any of the two techniques.

The first technique consists of imposing a restriction on t that implies that t is constant, that is, $t \in R$. In this case, $t = t(r)$ for all $r \in R$, and since we already have $t(r) \in \mathcal{Z}^+$, we are done.

The second technique adds a condition on t implying that the value $t(r) = n$ does not depend on p (equivalently, on r; recall that we are taking $p = x - r + 1$). In other words, we want to force t to be a constant polynomial function. By doing this, and assuming that the ring R is infinite, we can apply Theorem 4.14 to get $t \in R$, and again we obtain $t \in \mathcal{Z}^+$.

It is reasonable to expect that the technique showed in Lemma 6.3 can be adapted in order to obtain the definability of the prime subring in other types of rings.

6.2. The case in which every nonzero integer is invertible. In this subsection we develop the first strategy discussed above. More concretely, we obtain the definability of $\mathcal{Z}^+$ in $R[x]$ when R is a reduced indecomposable ring, provided the definability of a set between $\mathcal{Z}^+$ and R. Particularly, if we take this set as the set of units of $R[x]$ together with zero, this method accounts for all cases in which every nonzero integer in the ring is invertible. This improves the result of [22, Section 2], which requires that R be a characteristic zero integral domain that is first-order definable in the ring $R[x]$[11].

PROPOSITION 6.4. *Let $S = R[x]$, with R a reduced indecomposable ring, and let P be as in Definition 5.4. Given a definable subset A of S with $A \subseteq R$, we have that*

$$\Gamma_A(t)\colon\ t \in A \wedge \forall p\big(p \in P \to \exists y \exists w[y \in \mathsf{LPOW}(p) \wedge y - 1 = (p-1)w \wedge p - 1 \mid w - t]\big)$$

defines the subset $\mathcal{Z}^+ \cap A$. In particular, Γ_A defines $\mathcal{Z}^+$ whenever $A \supseteq \mathcal{Z}^+$.

PROOF. With notation as in Definition 6.2, let $\beta = \psi$, where ψ is given by Formula (3.1), so the subset B_p of S defined by $\beta(\cdot, p)$ is equal to $\mathsf{LPOW}(p)$. Therefore, the subformula

$$\exists y \exists w[y \in \mathsf{LPOW}(p) \wedge y - 1 = (p-1)w \wedge p - 1 \mid w - t]$$

[11] This is the case if R is a field or a local domain (see Section 2.1): in the first case we have $R = \{0\} \cup R[x]^*$; in the second case, $R = \{p \in R[x]\colon\ p \in R[x]^* \text{ or } p + 1 \in R[x]^*\}$.

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

of Γ_A is precisely the formula $\exists y \exists w L_\beta(t,p,y,w)$, with $L_\beta(t,p,y,w)$ as in Definition 6.2.

If $p \in P$, then $B_p = \mathsf{LPOW}(p) = \mathsf{POW}(p)$ by item b of Theorem 5.5; in particular, $\log_p B_p = \mathcal{Z}^+$, regardless of $p \in P$. Moreover, we have that $p-1$ is regular, by the definition of P. Thus, we are in the hypotheses of Lemma 6.3b, which implies that $\exists y \exists w L_\beta(t,p,y,w)$ holds if and only if the following condition is satisfied:

$$\text{There exists } n_p \in \log_p B_p = \mathcal{Z}^+ \text{ such that } p-1 \mid t-n_p. \tag{$*$}$$

If t satisfies Γ_A, then $t \in A$ by definition. Moreover, taking $p = x \in P$ and using $(*)$ we get some $n_x \in \mathcal{Z}^+$ and some $\ell \in R[x]$ such that $t - n_x = (x-1)\ell$. However, $t - n_x \in R$, because $t \in A \subseteq R$. Thus, evaluating at $x = 1$ we conclude that necessarily $t - n_x = 0$, and consequently $t = n_x \in \mathcal{Z}^+$.

Conversely, let $t = n \in \mathcal{Z}^+ \cap A$. We want to show that $\Gamma_A(t)$ holds. Obviously $t \in A$, and if $p \in P$, then the element $n_p = n$ satisfies $n_p \in \mathcal{Z}^+ = \log_p B_p$ and $p-1 \mid 0 = t - n_p$, so that $(*)$ holds, and therefore $\exists y \exists w L_\beta(t,p,y,w)$ holds as well. ⊣

Remark 6.5. The arguments presented in the proof of Proposition 6.4 above can be adapted to prove the definability of $\mathcal{Z}^+$ (with parameters) in noncommutative rings too. For instance, let D be an integral domain, and let $q \in D \setminus \{0\}$. The *quantum plane over D with parameter q*, denoted by $S = D_q[x,y]$, is defined as the quotient of the free noncommutative D-algebra over two generators x and y, by the unique relation $yx = qxy$ (see [14, Chapter IV] for details on the case in which D is a field). One can prove that $\mathcal{Z}^+$ is definable in $(S, 0, 1, +, \cdot, x)$, provided that every nonzero integer is invertible in S: for example, when D is a field or $\mathsf{char}(D) > 0$, or in other cases such as $D = \mathbb{Q}[t]$.

Theorem 6.6. *Let $S = R[x]$, with R a reduced indecomposable ring, and let P be as in Definition 5.4. The formula*

$$\Gamma(t)\colon\ t \in \{0\} \cup S^* \wedge \forall p \big(p \in P \to \exists y \exists w [y \in \mathsf{LPOW}(p) \wedge y - 1 = (p-1)w \wedge p - 1 \mid w - t]\big).$$

defines the set $\mathcal{Z}^+ \cap (\{0\} \cup S^*)$, which contains 1_S. In particular, Γ defines $\mathcal{Z}^+$ if and only if every nonzero element of $\mathcal{Z}^+$ is invertible.

Proof. Let $A = \{0\} \cup S^*$. Proposition 4.2 implies indeed that $A \subseteq R$, and therefore we can apply Proposition 6.4, after observing that $\Gamma = \Gamma_A$. ⊣

Remark 6.7. The fact that Γ defines a subset of $\mathcal{Z}^+$ containing 1_S in *arbitrary* reduced indecomposable polynomial rings will play a crucial role at the end of the section, in the construction of a unified formula that works for all such rings.

6.3. The case of nonfields of characteristic zero. In this subsection we develop the second strategy for defining $\mathcal{Z}^+$ discussed at the end of Section 6.1, which works successfully for the case where the coefficient ring is a (reduced, indecomposable) nonfield of characteristic zero. Since Theorem 6.6 covers, among others, the case in which the coefficient ring is a field or has positive characteristic (the latter by Proposition 4.8), the result of this subsection will settle all remaining cases.

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

By using definability of powers of constants with the constants themselves as parameters (Corollary 5.10), we can strengthen the formula L_β (see Definition 6.2), as was made in the previous subsection, but in another manner, in order to get rid of the requirement of having a suitable definable set of constants in $R[x]$ for defining $\mathcal{Z}^+$.

Notice that this result implies, in particular, the definability of $\mathbb{Z}$ in the ring $\mathbb{Z}[x]$, which is announced in [22, Sections 3a and 3b], but not directly proved[12] (see [17, Theorem 7.13] for an alternative proof).

PROPOSITION 6.8. *Let $S = R[x]$, with R a reduced indecomposable ring, and let P be as in Definition 5.4. Let θ be the three-variable formula defined by*

$$\theta(t,a,b)\colon \forall p[p \in P \to \exists y \exists w(y \in \mathsf{LPOW}(p) \\ \wedge y-1 = (p-1)w \wedge p-1 \mid w-t \wedge p-a \mid y-b)].$$

Let $a \in R$ be such that all powers of a are distinct. If $k \in \mathbb{Z}^+$ is such that $\theta(t,a,a^k)$ holds, then $t = k$.

PROOF. Our argument resembles closely that of the proof of Proposition 6.4: with notation as in Definition 6.2, let $\beta = \psi$, where ψ is given by Formula (3.1), so that the subset B_p of $R[x]$ defined by $\beta(\cdot,p)$ is precisely $\mathsf{LPOW}(p)$. Therefore, the subformula

$$\exists y \exists w(y \in \mathsf{LPOW}(p) \wedge y-1 = (p-1)w \wedge p-1 \mid w-t \wedge p-a \mid y-b)$$

of $\theta(t,a,b)$ is precisely the formula

$$\exists y \exists w[L_\beta(t,p,y,w) \wedge p-a \mid y-b],$$

with $L_\beta(t,p,y,w)$ as in Definition 6.2. If $p \in P$, then $B_p = \mathsf{LPOW}(p) = \mathsf{POW}(p)$ by item b of Theorem 5.5; in particular, $\log_p B_p = \mathcal{Z}^+$. Moreover, we have that $p-1$ is regular, by the definition of P. Thus, we are in the hypotheses of Lemma 6.3.

Let $r \in R$ be fixed. We will show that $t(r) = k$. If $p = x - r + 1$, then $p \in P$ by Remark 5.6. Since $\theta(t,a,a^k)$ holds, there exist $y,w \in R[x]$ such that p satisfies both the formula $L_\beta(t,p,y,w)$ and the condition $p-a \mid y-a^k$. In particular, Lemma 6.3a grants the existence of an element $n \in \log_p B_p = \mathcal{Z}^+$ (n possibly depends on r) such that $p-1 \mid t-n$ and $y = p^n$.

Since $p-1 = x-r$, the condition $p-1 \mid t-n$ becomes $x-r \mid t-n$, which in turn is equivalent to have $t(r) = n$. Since we also have $p-a \mid y-a^k$ and obviously $p-a \mid p^n-a^n$ always holds, we conclude that $p-a$ divides $(y-a^k)-(p^n-a^n) = a^n-a^k$ (recall that $y = p^n$). Thus, there exists $\ell \in R[x]$ such that $a^n-a^k = (p-a)\ell = (x-r+1-a)\ell$. After evaluating at $x = r-1+a$ and taking into account that $a^n-a^k \in R$ (because $a \in R$), we get $a^n-a^k = 0$. As all powers of a are distinct, the equality $a^n = a^k$ forces $n = k$, hence $t(r) = n = k$, as desired.

Since k is fixed and therefore does not depend on r, we have proven that if $\theta(t,a,a^k)$ holds, then the polynomial function induced by t has constant value k.

[12] The author proves the definability of integers in quadratic rings, and claims that the method of his proof can be slightly modified in order to obtain the corresponding definability result in polynomial rings over the integers or over quadratic rings.

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

As all powers of a are distinct, it follows that R is infinite, so we can apply Theorem 4.14 to conclude that $t = k$. ⊣

THEOREM 6.9. *Let $S = R[x]$, with R being a reduced indecomposable characteristic zero ring which is not a field. Let U be as in Definition 5.4, and let $\Phi(\cdot,\cdot)$ be the formula given in Corollary 5.10, defining powers of constant elements, namely,*

$$\Phi(t,a)\colon \forall p \forall q \big([p \in U \wedge q \in U] \to \exists y \exists z [y \in \mathsf{LPOW}(p) \wedge z \in \mathsf{LPOW}(q) \wedge p - a \mid y - t \wedge q - a \mid z - t \wedge p - q \mid y - z]\big).$$

If

$$\Upsilon(t)\colon \exists b[\Phi(b,2) \wedge \theta(t,2,b)],$$

with θ as in Proposition 6.8, then Υ defines $\mathcal{Z}^+$ in S.

PROOF. We have, by Corollary 5.10, that for any $a \in R$ the formula $\Phi(\cdot,a)$ defines the set $\mathsf{POW}(a)$. Therefore, if $\Upsilon(t)$ holds, then there exists a positive integer k such that formula $\theta(t,2,2^k)$ holds. Since R has characteristic zero, all powers of 2 are distinct, and therefore we may take $a = 2$ in Proposition 6.8, obtaining $t = k \in \mathcal{Z}^+$.

Conversely, if $t \in \mathcal{Z}^+ = \mathbb{Z}^+$ (recall that $\mathsf{char}(R) = 0$), say $t = n$, then it is easy to see that $\Upsilon(t)$ holds for the choice $b = 2^n$: more specifically, the reader may check that the formula $\theta(n,2,2^n)$ holds by taking, for each $p \in P$ (where P is as in Definition 5.4), the values $y = p^n$ and $w = w_n(p)$. ⊣

6.4. The unified formula. In the previous two subsections we have provided two techniques that define $\mathcal{Z}^+$ in two different cases (Theorems 6.6 and 6.9). To sum up, let $\mathcal{H}$ be the class of reduced indecomposable polynomial rings. Let $\mathcal{H}_1$ be the subclass of rings in $\mathcal{H}$ where every nonzero integer is invertible, and let $\mathcal{H}_2$ be the subclass of rings in $\mathcal{H}$ expressible as $R[x]$, where R is a nonfield of characteristic zero. By Proposition 4.8, if S is a member of $\mathcal{H}$ not belonging to $\mathcal{H}_1$, then S belongs to $\mathcal{H}_2$, and this is equivalent to the following identity of classes:

$$\mathcal{H} = \mathcal{H}_1 \cup \mathcal{H}_2.$$

We remark that these subclasses do overlap: for example, the ring $R = \mathbb{Q}[s,t]/(st)$ (Example 4.9) is a reduced indecomposable nondomain (hence a nonfield) of characteristic zero in which every nonzero integer is invertible. Therefore, any of the two techniques developed could be used to define $\mathcal{Z}^+$ in $R[x]$.

At this point of the paper we have already proven that $\mathcal{Z}^+$ (and, consequently, the whole prime subring) is definable in all reduced indecomposable polynomial rings. However, depending on whether we work over $\mathcal{H}_1$ or $\mathcal{H}_2$, we resorted to distinct formulas, that were denoted by Γ and Υ, respectively, in order to write out the definition sought.

In what follows we merge Γ and Υ into a single formula, defining $\mathcal{Z}^+$ in any reduced indecomposable polynomial ring, covering this way the whole class $\mathcal{H}$ uniformly. To this end, we begin by constructing an auxiliary sentence that characterizes nonmembership in $\mathcal{H}_1$, and therefore forces membership in $\mathcal{H}_2$.

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press

LEMMA 6.10. *Let $S = R[x]$, with R a reduced indecomposable ring. Let $C = \mathcal{Z}^+ \cap (\{0\} \cup S^*)$ be the set defined by the formula Γ as in Theorem 6.6, and define*

$$\Xi\colon \exists t(t \in C \wedge t+1 \notin C).$$

We have that $C = \mathcal{Z}^+$ if and only if Ξ does not hold. Moreover, if Ξ holds in S, then R is a nonfield of characteristic zero.

PROOF. By Theorem 6.6 we have that C is a subset of $\mathcal{Z}^+$ containing 1, and therefore $C = \mathcal{Z}^+$ if and only if C is closed under the successor function $t \mapsto t+1$, which is equivalent to negating Ξ, proving the first assertion. For the second assertion, if R is a field or R has positive characteristic, then every nonzero integer in S is invertible (by Proposition 4.8 in the latter case). Therefore C coincides with $\mathcal{Z}^+$ in these cases, and so Ξ is false. ⊣

What follows is the main result of our work: there is a formula defining the prime subring in all reduced indecomposable rings $R[x]$, regardless of the coefficient ring R. As mentioned in Remark 6.7, we stress how the result of Theorem 6.6 plays a critical role in the proof of our final claim, for it guarantees that $1 \in C \subseteq \mathcal{Z}^+$, regardless of the coefficient ring R.

THEOREM 6.11. *Let $S = R[x]$, with R a reduced indecomposable ring. Let*

$$\Omega(t)\colon [\neg\Xi \wedge \Gamma(t)] \vee [\Xi \wedge \Upsilon(t)],$$

where Γ and Υ are the formulas given by Theorems 6.6 and 6.9, respectively, and Ξ is given by Lemma 6.10. We have that Ω defines the set $\mathcal{Z}^+$ in S.

PROOF. Observe that

$$\Omega(t)\colon \begin{cases} t \in C, & \text{if } \Xi \text{ is false;} \\ \Upsilon(t), & \text{if } \Xi \text{ is true,} \end{cases}$$

with C as in Lemma 6.10. If Ξ is false, then $C = \mathcal{Z}^+$ by Lemma 6.10. Otherwise, R is a nonfield of characteristic zero, again by Lemma 6.10, hence Υ defines $\mathcal{Z}^+$ by Theorem 6.9. In either case, we have proven that $\Omega(t)$ holds if and only if $t \in \mathcal{Z}^+$. ⊣

Acknowledgements. We would like to express our sincere thanks and appreciation to Thomas W. Scanlon, Alexandra Shlapentokh, and Carlos Videla, for their kindness and inspiring advice. We are grateful to the anonymous referee for her/his attention and precious recommendations. We are also indebted to Remy van Dobben de Bruyn and William F. Sawin (from MathOverflow) and Robin Denis Arthan (Mathematics Stack Exchange) for their help with some questions we raised on the websites mentioned. The second author is supported by FACEPE Grant APQ-0892-1.01/14.

REFERENCES

[1] R. ARTHAN, *Is $\mathbb{Z}$ first-order definable in (the ring) $\mathbb{Z} \times \mathbb{Z}$?*. *Mathematics Stack Exchange*, version: 2016-01-23. Available at https://math.stackexchange.com/q/1623441.

[2] M. Aschenbrenner, A. Khélif, E. Naziazeno, and T. Scanlon, *The logical complexity of finitely generated commutative rings*. ***International Mathematics Research Notices***, vol. 2020 (2018), no. 1, pp. 112–166.

[3] A. Blass, *Injectivity, projectivity, and the axiom of choice*. ***Transactions of the American Mathematical Society***, vol. 255 (1979), pp. 31–59.

[4] P. M. Cohn, ***Basic Algebra: Groups, Rings and Fields***, Springer-Verlag London, Ltd., London, 2003.

[5] J. Denef, *The Diophantine problem for polynomial rings and fields of rational functions*. ***Transactions of the American Mathematical Society***, vol. 242 (1978), pp. 391–399.

[6] ———, *The Diophantine problem for polynomial rings of positive characteristic*, ***Logic Colloquium '78 (Mons, 1978)*** (M. Boffa, D. Dalen, and K. Mcaloon, editors), Studies in Logic and the Foundations of Mathematics, vol. 97, North-Holland, Amsterdam, 1979, pp. 131–145.

[7] D. Eisenbud, ***Commutative Algebra: With a View Toward Algebraic Geometry***, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995.

[8] C. Good and I. J. Tree, *Continuing horrors of topology without choice*. ***Topology and Its Applications***, vol. 63 (1995), no. 1, pp. 79–90.

[9] W. Hodges, *Six impossible rings*. ***Journal of Algebra***, vol. 31 (1974), pp. 218–244.

[10] ———, *Krull implies Zorn*. ***The Journal of the London Mathematical Society. Second Series***, vol. 19 (1979), no. 2, pp. 285–287.

[11] ———, ***Model theory***, Encyclopedia of Mathematics and Its Applications, vol. 42, Cambridge University Press, Cambridge, 1993.

[12] P. Howard and J. E. Rubin, ***Consequences of the Axiom of Choice***, Mathematical Surveys and Monographs, vol. 59, American Mathematical Society, Providence, RI, 1998.

[13] T. W. Hungerford, ***Algebra***, Graduate Texts in Mathematics, vol. 73, Springer-Verlag, New York, 1980, reprint of the 1974 original.

[14] C. Kassel, ***Quantum Groups***, Graduate Texts in Mathematics, vol. 155, Springer-Verlag, New York, 1995.

[15] J. Koenigsmann, *Undecidability in number theory*, ***Model Theory in Algebra, Analysis and Arithmetic*** (H. D. Macpherson and C. Toffalori, editors), Lecture Notes in Mathematics, vol. 2111, Springer, Heidelberg, 2014, pp. 159–195.

[16] J. V. Matijasevič, *The Diophantineness of enumerable sets*. ***Doklady Akademii Nauk SSSR***, vol. 191 (1970), pp. 279–282.

[17] A. Nies, *Describing groups*. ***The Bulletin of Symbolic Logic***, vol. 13 (2007), no. 3, pp. 305–339.

[18] T. Pheidas, *Decision problems in algebra and analogues of Hilbert's tenth problem*, ***Model Theory with Applications to Algebra and Analysis, vol. 2***, (Z. Chatzidakis, D. Macpherson, A. Pillay, and A. Wilkie, editors), London Mathematical Society Lecture Note Series, vol. 350, Cambridge University Press, Cambridge, 2008, pp. 207–235.

[19] T. Pheidas and K. Zahidi, Undecidable existential theories of polynomial rings and function fields. ***Communications in Algebra***, vol. 27 (1999), no. 10, pp. 4993–5010.

[20] B. Poonen, *Undecidability in number theory*. ***Notices of the American Mathematical Society***, vol. 55 (2008), no. 3, pp. 344–350.

[21] J. Robinson, *Definability and decision problems in arithmetic*, this Journal, vol. 14 (1949), pp. 98–114.

[22] R. M. Robinson, *Undecidable rings*. ***Transactions of the American Mathematical Society***, vol. 70 (1951), pp. 137–159.

[23] W. Sawin, *Rings for which no polynomial induces the zero function*. *MathOverflow*, version: 2014-03-21. Available at https://mathoverflow.net/q/161057.

[24] A. Shlapentokh, *Diophantine definitions for some polynomial rings*. ***Communications on Pure and Applied Mathematics***, vol. 43 (1990), no. 8, pp. 1055–1066.

[25] ———, Defining integers. ***The Bulletin of Symbolic Logic***, vol. 17 (2011), no. 2, pp. 230–251.

[26] J. Utreras, *Interpreting arithmetic in the first-order theory of addition and coprimality of polynomial rings*, this Journal, vol. 84 (2019), no. 3, pp. 1194–1214.

[27] R. van Dobben de Bruyn, *Do there exist nonzero identically vanishing polynomials over infinite (or characteristic zero) reduced indecomposable commutative rings*? *MathOverflow*, version: 2017-05-02. Available at https://mathoverflow.net/q/268753.

DEPARTAMENTO DE MATEMÁTICA
UNIVERSIDADE FEDERAL DE PERNAMBUCO
AVENIDA JORNALISTA ANÍBAL FERNANDES
S/N - CIDADE UNIVERSITÁRIA
RECIFE/PE 50740-560, BRAZIL
E-mail: marco.barone@ufpe.br
E-mail: jorge.caro@ufpe.br
E-mail: eudes.naziazeno@ufpe.br

https://doi.org/10.1017/jsl.2020.50 Published online by Cambridge University Press