THE LOGICAL COMPLEXITY OF FINITELY GENERATED COMMUTATIVE RINGS

MATTHIAS ASCHENBRENNER, ANATOLE KHÉLIF, EUDES NAZIAZENO, AND THOMAS SCANLON

Abstract. We characterize those finitely generated commutative rings which are (parametrically) bi-interpretable with arithmetic: a finitely generated commutative ring A is bi-interpretable with $(\mathbb{N}, +, \times)$ if and only if the space of non-maximal prime ideals of A is nonempty and connected in the Zariski topology and the nilradical of A has a nontrivial annihilator in $\mathbb{Z}$. Notably, by constructing a nontrivial derivation on a nonstandard model of arithmetic we show that the ring of dual numbers over $\mathbb{Z}$ is *not* bi-interpretable with $\mathbb{N}$.

Introduction

We know since Gödel that the class of arithmetical sets, that is, sets definable in the semiring $(\mathbb{N}, +, \times)$, is very rich; in particular, the first-order theory of this structure is undecidable. One expects other mathematical structures which are connected to arithmetic to share this feature. For instance, since the subset $\mathbb{N}$ of $\mathbb{Z}$ is definable in the ring $\mathbb{Z}$ of integers (Lagrange's Four Square Theorem), every subset of $\mathbb{N}^m$ which is definable in arithmetic is definable in $\mathbb{Z}$. The usual presentation of integers as differences of natural numbers (implemented in any number of ways) shows conversely that $\mathbb{Z}$ is *interpretable* in $\mathbb{N}$; therefore every $\mathbb{Z}$-definable subset of $\mathbb{Z}^n$ also corresponds to an $\mathbb{N}$-definable set. Thus the semiring $\mathbb{N}$ is interpretable (in fact, definable) in the ring $\mathbb{Z}$, and conversely, $\mathbb{Z}$ is interpretable in $\mathbb{N}$; that is, $\mathbb{N}$ and $\mathbb{Z}$ are *mutually interpretable.* However, something much stronger holds: the structures $\mathbb{N}$ and $\mathbb{Z}$ are *bi-interpretable.*

Bi-interpretability is an equivalence relation on the class of first-order structures which captures what it means for two structures (in possibly different languages) to have essentially have the same categories of definable sets and maps. (See [1] or [11, Section 5.4].) Thus in this sense, the definable sets in structures which are bi-interpretable with arithmetic are just as complex as those in $(\mathbb{N}, +, \times)$. We recall the definition of bi-interpretability and its basic properties in Section 2 below. For example, we show there that a structure $\boldsymbol{A}$ with underlying set A is bi-interpretable with arithmetic if and only if there are binary operations $\oplus$ and $\otimes$ on A such that $(\mathbb{Z}, +, \times) \cong (A, \oplus, \otimes)$, and the structures $(A, \oplus, \otimes)$ and $\boldsymbol{A} = (A, \dots)$ have the same definable sets. The reader who is not yet familiar with this notion may simply take this equivalent statement as the definition of "$\boldsymbol{A}$ is bi-interpretable with $\mathbb{N}$." Bi-interpretability between general structures is a bit subtle and sensitive, for example, to whether parameters are allowed. Bi-interpretability with $\mathbb{N}$ is more robust, but we should note here that even for natural algebraic examples, mutual

Date: October 2016.

Scanlon's work is partially supported by NSF grant DMS-1363372.

interpretability with $\mathbb{N}$ does not automatically entail bi-interpretability with $\mathbb{N}$: for instance, the Heisenberg group $\mathrm{UT}_3(\mathbb{Z})$ of unitriangular 3×3-matrices with entries in $\mathbb{Z}$, although it interprets arithmetic [21], is not bi-interpretable with it; see [12, Théorème 6] or [26, Theorem 7.16]. See [17] for interesting examples of finitely generated simple groups which *are* bi-interpretable with $\mathbb{N}$.

Returning to the commutative world, the consideration of $\mathbb{N}$ and $\mathbb{Z}$ above leads to a natural question: *are* all *infinite finitely generated commutative rings bi-interpretable with* $\mathbb{N}$*?* Indeed, each finitely generated commutative ring is interpretable in $\mathbb{N}$ (see Corollary 2.14 below), and it is known that conversely each infinite finitely generated commutative ring interprets arithmetic [28]. However, it is fairly easy to see as a consequence of the Feferman-Vaught Theorem that $\mathbb{Z} \times \mathbb{Z}$ is not bi-interpretable with $\mathbb{N}$. Perhaps more surprisingly, there are nontrivial derivations on nonstandard models of arithmetic and it follows, for instance, that the ring $\mathbb{Z}[\epsilon]/(\epsilon^2)$ of dual numbers over $\mathbb{Z}$ is not bi-interpretable with $\mathbb{N}$. (See Section 6.)

The main result of this paper is a characterization of the finitely generated commutative rings which are bi-interpretable with $\mathbb{N}$. To formulate it, we need some notation. Let A be a commutative ring (with unit). As usual, we write $\operatorname{Spec}(A)$ for the spectrum of A, i.e., the set of prime ideals of A equipped with the Zariski topology, and $\operatorname{Max}(A)$ for the subset of $\operatorname{Spec}(A)$ consisting of the maximal ideals of A. We put $\operatorname{Spec}^\circ(A) := \operatorname{Spec}(A) \setminus \operatorname{Max}(A)$, equipped with the subspace topology. (In the context of a local ring $(A, \mathfrak{m})$, the topological space $\operatorname{Spec}^\circ(A) = \operatorname{Spec}(A) \setminus \{\mathfrak{m}\}$ is known as the "punctured spectrum" of A.)

Theorem. *Suppose the ring A is finitely generated, and let N be the nilradical of A. Then A is bi-interpretable with $\mathbb{N}$ if and only if A is infinite,* $\operatorname{Spec}^\circ(A)$ *is connected, and there is some integer $d \geq 1$ with $dN = 0$.*

The proof of the theorem is contained in Sections 3–6, preceded by two preliminary sections, on algebraic background and on interpretations, respectively. Let us indicate the strategy of the proof. Clearly if A is bi-interpretable with $\mathbb{N}$, then necessarily A is infinite. Note that the theorem says in particular that if A is an infinite integral domain, then A is bi-interpretable with $\mathbb{N}$. We prove this fact in Section 3 using techniques of [38] which are unaffected by the error therein [39], as sufficiently many valuations on the field of fractions of A may be defined via ideal membership conditions in A. Combining this fact with Feferman-Vaught-style arguments, in Section 4 we then establish the theorem in the case where A is infinite and reduced (that is, $N = 0$): A is bi-interpretable with $\mathbb{N}$ iff $\operatorname{Spec}^\circ(A)$ is connected. To treat the general case, we distinguish two cases according to whether or not there exists an integer $d \geq 1$ with $dN = 0$. In Section 5, assuming that there is such a d, we use Witt vectors to construct a bi-interpretation between A and its associated reduced ring $A_{\mathrm{red}} = A/N$. Noting that A is finite if and only if A_{red} is finite, and $\operatorname{Spec}^\circ(A)$ and $\operatorname{Spec}^\circ(A_{\mathrm{red}})$ are homeomorphic, this allows us to appeal to the case of a reduced ring A. Finally, by constructing suitable automorphisms of an elementary extension of A we prove that if there is no such integer d, then A cannot be bi-interpretable with $\mathbb{N}$. (Section 6.)

Structures bi-interpretable with arithmetic are "self-aware": they know their own isomorphism type. More precisely, if a finitely generated structure $\boldsymbol{A}$ in a finite language $\mathcal{L}$ is bi-interpretable with $\mathbb{N}$, then $\boldsymbol{A}$ is *quasi-finitely axiomatizable* (*QFA*), that is, there is an $\mathcal{L}$-sentence σ satisfied by $\boldsymbol{A}$ such that every finitely generated $\mathcal{L}$-structure satisfying σ is isomorphic to $\boldsymbol{A}$; see Proposition 2.28 below. (This notion of quasi-finite axiomatizability does not agree with the one commonly used in Zilber's program, for example, in [1].) In [25], Nies first considered the class of QFA groups, which has been studied extensively since then; see, for example [16, 17, 18, 19, 27, 30, 31].

In 2004, Sabbagh [26, Theorem 7.11] gave a direct argument for the quasi-finite axiomatizability of the ring of integers. Belegradek [26, §7.6] then raised the question which finitely generated commutative rings are QFA. Building on our result that finitely generated integral domains are bi-interpretable with $\mathbb{N}$, in the last section of this paper we prove:

Corollary. *Each finitely generated commutative ring is QFA.*

This paper had a rather long genesis, which we briefly summarize. Around 2005, the second- and fourth-named authors independently realized that bi-interpretability with $\mathbb{N}$ entails QFA. The fourth-named author was motivated by Pop's 2002 conjecture [34] that finitely generated fields are determined up to isomorphism by their elementary theory. In [38] the fourth-named author attempted to establish this conjecture by showing that they are bi-interpretable with $\mathbb{N}$; however, later, Pop found a mistake in this argument, and his conjecture remains open [39]. Influenced by [38] and realizing that not all finitely generated commutative rings are bi-interpretable with $\mathbb{N}$, in 2006 the first-named author became interested in algebraically characterizing those which are. The corollary above was announced by the second-named author in [12], where a proof based on the main result of [38] was suggested. In his Ph. D. thesis [24], the third-named author later gave a proof of this corollary circumventing the flaws of [38].

We conclude this introduction with an open question suggested by our theorems above. Recall that a group G is said to be *metabelian* if its commutator subgroup $G' = [G,G]$ is abelian. If G is a metabelian group, then the abelian group G/G' can be made into a module M over the group ring $A = \mathbb{Z}[G']$ in a natural way; if moreover G is finitely generated, then the commutative ring A is finitely generated, and so is the A-module M, hence by the above, the two-sorted structure (A,M) is QFA. (Lemma 7.2.) However, no infinite abelian group is QFA [26, §7.1], and we already mentioned that the metabelian group $\mathrm{UT}_3(\mathbb{Z})$ is not bi-interpretable with $\mathbb{N}$, though it is QFA [26, §7.2]. The second-named author has shown that every non-abelian free metabelian group is bi-interpretable with $\mathbb{N}$ [13]. Each non-abelian finitely generated metabelian group interprets $\mathbb{N}$ [29].

Question. Is every non-abelian finitely generated metabelian group QFA? Which finitely generated metabelian groups are bi-interpretable with $\mathbb{N}$?

Notations and conventions. We let m, n range over the set $\mathbb{N} = \{0,1,2,\dots\}$ of natural numbers. In this paper, "ring" always means "commutative ring with unit." Rings are always viewed as model-theoretic structures in the language $\{+,\times\}$ of rings. We occasionally abbreviate "finitely generated" by "f.g." The adjective "definable" will always mean "definable, possibly with parameters."

1. Preliminaries: Algebra

In this section we gather some basic definitions and facts of a ring-theoretic nature which are used later.

1.1. **Radicals.** Let A be a ring and I be an ideal of A. We denote by $\mathrm{Nil}(I)$ the *nilradical* of I, that is, the ideal

$$\mathrm{Nil}(I) := \big\{a \in A : \exists n\ a^n \in I\big\}$$

of A, and we write

$$\mathrm{Jac}(I) := \big\{a \in A : \forall b \in A\ \exists c \in A\ (1 - ab)c \in 1 + I\big\}$$

for the *Jacobson radical* of I. It is well-known that $\mathrm{Nil}(I)$ equals the intersection of all prime ideals of A containing I, and $\mathrm{Jac}(I)$ equals the intersection of all maximal ideals of A which contain I. Evidently, $I \subseteq \mathrm{Nil}(I) \subseteq \mathrm{Jac}(I)$. The ideal I is said to be *radical* if $\mathrm{Nil}(I) = I$. For our purposes it is important to note that although the nilradical is not uniformly definable for all rings, the Jacobson radical is; more precisely, we have: if $\varphi(x)$ is a formula defining I in A, then the formula

$$\mathrm{Jac}(\varphi)(x) := \forall u \exists v \exists w \big((1 - xu)v = 1 + w\ \&\ \varphi(w)\big)$$

defines $\mathrm{Jac}(I)$ in A. We denote by $N(A)$ the nilradical of the zero ideal of A. Thus $N(A) = \bigcap_{\mathfrak{p}\in\mathrm{Spec}\,A} \mathfrak{p}$. One says that A is *reduced* if $N(A) = 0$. The ring $A_{\mathrm{red}} := A/N(A)$ is reduced, and called the associated reduced ring of A. We say that I is *nilpotent* if there is some integer $e \geq 1$ such that $I^e = 0$. The smallest such e is the *nilpotency index* of I (not to be confused with the index $[A : I]$ of I as an additive subgroup of A). If $N(A)$ is f.g., then it is nilpotent.

Lemma 1.1. *A is finite if and only if it contains a f.g. nilpotent ideal of finite index in A.* (*In particular, if $N(A)$ is f.g., then A is finite iff A_{red} is finite.*)

Proof. Let N be a f.g. ideal of A such that A/N is finite, and $e \geq 1$ such that $N^e = 0$. We show, by induction on $i = 1, \dots, e$, that A/N^i is finite. The case $i = 1$ holds by assumption. Suppose now that we have already shown that A/N^i is finite, where $i \in \{1, \dots, e - 1\}$. Then N^i/N^{i+1} is an A/N-module in a natural way, and f.g. as such, hence finite. Since $A/N^i \cong (A/N^{i+1})/(N^i/N^{i+1})$, this yields that A/N^{i+1} is also finite. □

1.2. **Jacobson rings.** *In this subsection we let A be a ring.* One calls A a *Jacobson ring* (also sometimes a *Hilbert ring*) if every prime ideal of A is an intersection of maximal ideals; that is, if $\mathrm{Nil}(I) = \mathrm{Jac}(I)$ for every ideal I of A. The class of Jacobson rings is closed under taking homomorphic images: if $A \to B$ is a surjective ring morphism and A is a Jacobson ring, then B is a Jacobson ring. Examples for Jacobson rings include all fields and the ring $\mathbb{Z}$ of integers, or more generally, every principal ideal domain with infinitely many pairwise non-associated primes. The main interest in Jacobson rings in commutative algebra and algebraic geometry is their relation with Hilbert's Nullstellensatz, an abstract version of which states that if A is a Jacobson ring, then so is any f.g. A-algebra B; in this case, the pullback of any maximal ideal $\mathfrak{n}$ of B is a maximal ideal $\mathfrak{m}$ of A, and $B/\mathfrak{n}$ is a finite extension of the field $A/\mathfrak{m}$. In particular, every f.g. ring is a Jacobson ring.

Lemma 1.2. *Suppose A is a field which is f.g. as a ring. Then A is finite.*

Proof. The pullback $\mathfrak{m}$ of the maximal ideal $\{0\}$ of A is maximal ideal of $\mathbb{Z}$, that is, $\mathfrak{m} = p\mathbb{Z}$ for some prime number p, and A is a finite extension of the finite field $\mathbb{Z}/p\mathbb{Z}$, hence finite. □

Corollary 1.3. *Suppose A is f.g. Then A is finite if and only if* $\mathrm{Spec}^\circ(A) = \emptyset$, *that is, every prime ideal of A is maximal.*

Proof. We may assume that A is nontrivial. A nontrivial ring is called zero-dimensional if it has no non-maximal prime ideals. Every nontrivial finite ring (in fact, every nontrivial artinian ring [22, Example 2, §5]) is zero-dimensional. Conversely, assume that A is zero-dimensional. Then A has only finitely many pairwise distinct maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_k$, and setting $N := N(A)$, we have $N = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k$. Each of the fields $A/\mathfrak{m}_i$ is f.g. as a ring, hence finite, by Lemma 1.2. By the Chinese Remainder Theorem, $A/N \cong (A/\mathfrak{m}_1) \times \cdots \times (A/\mathfrak{m}_k)$, thus A/N is finite. Hence by Lemma 1.1, A is finite. □

Given an element a of a ring, we say that a has infinite multiplicative order if $a^m \neq a^n$ for all $m \neq n$.

Corollary 1.4. *Every infinite f.g. ring contains an element of infinite multiplicative order.*

Proof. Let A be f.g. and infinite, and let $\mathfrak{p}$ be a non-maximal prime ideal of A, according to the previous corollary. Take $a \in A \setminus \mathfrak{p}$ such that $1 \notin (a, \mathfrak{p})$. Then a has infinite multiplicative order. □

It is a classical fact that if A is noetherian of (Krull) dimension at most n, then every radical ideal of A is the nilradical of an ideal generated by $n+1$ elements. (This is due to Kronecker [14] in the case where A is a polynomial ring over a field, and to van der Waerden in general; see [7].)

Lemma 1.5. *There exist formulas*

$$\pi_n(y_1, \dots, y_{n+1}),\ \mu_n(y_1, \dots, y_{n+1}),\ \Pi_n(x, y_1, \dots, y_{n+1})$$

with the following property: if A is a noetherian Jacobson ring of dimension at most n, then

$$\operatorname{Spec} A = \big\{\Pi_n(A, a) : a \in A^{n+1},\ A \models \pi_n(a)\big\}$$
$$\operatorname{Max} A = \big\{\Pi_n(A, a) : a \in A^{n+1},\ A \models \mu_n(a)\big\}.$$

Proof. For every n let

$$\gamma_n(x, y_1, \dots, y_n) := \exists z_1 \cdots \exists z_n (x = y_1 z_1 + \cdots + y_n z_r),$$
$$\operatorname{Jac}_n(x, y_1, \dots, y_n) := \operatorname{Jac}(\gamma_n).$$

Then for every n-tuple $a = (a_1, \dots, a_n)$ of elements of A, the formula $\gamma_n(x, a)$ defines the ideal of A generated by $a_1, \dots, a_n$, and $\operatorname{Jac}_n(x, a)$ defines its Jacobson radical. Writing y for $(y_1, \dots, y_{n+1})$, the formulas

$$\pi_n(y) := \forall v \forall w \big(\operatorname{Jac}_{n+1}(v \cdot w, y) \to (\operatorname{Jac}_{n+1}(v, y) \vee \operatorname{Jac}_{n+1}(w, y)\big),$$
$$\mu_n(y) := \forall v \exists w \big(\operatorname{Jac}_{n+1}(v, y) \vee \operatorname{Jac}_{n+1}(1 - vw, y)\big),$$
$$\Pi_n(x, y) := \operatorname{Jac}_{n+1}(x, y)$$

have the required property, by Kronecker's Theorem. □

Remarks.

(1) The previous lemma holds if the noetherianity hypothesis is dropped and $\operatorname{Spec} A$ and $\operatorname{Max} A$ are replaced with the set of f.g. prime ideals of A and the set of f.g. maximal ideals of A, respectively, by a non-noetherian analogue of Kronecker's Theorem due to Heitmann [9, Corollary 2.4, (ii) and Remark (i) on p. 168].

(2) Let π_n, μ_n, Π_n be as in Lemma 1.5, and set $\pi_n^\circ := \pi_n \wedge \neg\mu_n$. Then for every noetherian Jacobson ring A of dimension at most n we have

$$\operatorname{Spec}^\circ A = \big\{\Pi_n(A,a) : a \in A^{n+1},\ A \models \pi_n^\circ(a)\big\}.$$

Hence for every such ring A, we have $A \models \forall y_1 \cdots \forall y_{n+1} \neg\pi_n^\circ$ iff $\dim A < 1$. (Using the inductive characterization of Krull dimension from [6], one can actually construct, for each n, a sentence $\dim_{<n}$ such that for all Jacobson rings A, we have $A \models \dim_{<n}$ iff $\dim A < n$.)

1.3. **Subrings of a localization.** In this subsection we let R be a ring and D be a subring of R.

Proposition 1.6. *Suppose that D is a Dedekind domain and $D[c^{-1}] = R[c^{-1}]$ for some $c \in D \setminus \{0\}$. Then R is a f.g. D-algebra.*

This can be deduced from [32, Theorem 2.20], but we give a direct proof based on a simple lemma from this paper:

Lemma 1.7 (Onoda [32])**.** *Suppose R is an integral domain. Then the set of $c \in R$ such that $c = 0$ or $c \neq 0$ and $R[c^{-1}]$ is a f.g. D-algebra is an ideal of R.*

Proof. Since this set clearly is closed under multiplication by elements of R, we only need to check that it is closed under addition. Let $a_1, a_2 \in R \setminus \{0\}$ be such that $a_1 + a_2 \neq 0$ and the D-algebra $R[a_i^{-1}]$ is f.g., for $i = 1, 2$. So we can take a f.g. D-algebra $B \subseteq R$ such that $a_i \in B$ and $B[a_i^{-1}] \supseteq R[a_i^{-1}]$, for $i = 1, 2$. Given $x \in R$, take $n \geq 1$ such that $a_i^n x \in B$; then $(a_1 + a_2)^{2n-1} x \in B$, so $x \in B[(a_1 + a_2)^{-1}]$. Thus $R[(a_1 + a_2)^{-1}] = B[(a_1 + a_2)^{-1}]$ is a f.g. D-algebra. □

Proof of Proposition 1.6. Let c be as in the statement of the proposition, and first let S be a multiplicative subset of D with $R[S^{-1}] = D[S^{-1}]$; we claim that then there is some $s \in S$ such that $R[s^{-1}] = D[s^{-1}]$. To see this note that for each $Q \in \operatorname{Spec}(D)$ with $D_Q \not\supseteq R$ we have $c \in Q$, since otherwise $D_Q \supseteq D[c^{-1}] = R[c^{-1}] \supseteq R$, and for a similar reason we have $Q \cap S \neq \emptyset$. Let $Q_1, \dots, Q_m$ be the prime ideals Q of D with $D_Q \not\supseteq R$. For $i = 1, \dots, m$ pick some $s_i \in Q_i \cap S$ and set $s := s_1 \cdots s_m \in S \cap Q_1 \cap \cdots \cap Q_m$. Then we have $D_Q \supseteq R$ for each $Q \in \operatorname{Spec}(D)$ with $s \notin Q$, and hence $D[s^{-1}] = \bigcap_{s \notin Q} D_Q \supseteq R$. Therefore $D[s^{-1}] = R[s^{-1}]$.

Let now I be the ideal of R defined in Lemma 1.7; we need to show that $1 \in I$. Towards a contradiction assume that we have some prime ideal P of R which contains I. Put $Q := D \cap P \in \operatorname{Spec}(D)$ and $S := D \setminus Q$. Then $D_Q = R_P$ (there is no proper intermediate ring between a DVR and its fraction field). In fact, we have $D[S^{-1}] = D_Q = R[S^{-1}]$, so by the above there is some $s \in S$ with $R[s^{-1}] = D[s^{-1}]$. Hence $s \in I \setminus P$, a contradiction. □

Remark. We don't know whether the conclusion of Proposition 1.6 can be strengthened to: $R = D[r^{-1}]$ for some $r \in R \setminus \{0\}$.

For a proof of the next lemma see, e.g., [3, Proposition 7.8].

Lemma 1.8 (Artin-Tate [2])**.** *Suppose D is noetherian and R is contained in a f.g. D-algebra which is integral over R. Then the D-algebra R is also f.g.*

The following fact is used in Section 3.

Corollary 1.9. *Suppose D is a one-dimensional noetherian integral domain whose integral closure $\widetilde{D}$ in the fraction field K of D is a f.g. D-module. If $D[c^{-1}] = R[c^{-1}]$ for some $c \in D \setminus \{0\}$, then R is a f.g. D-algebra.*

Proof. Let $\widetilde{R}$ be the integral closure of R in K. Suppose $c \in D \setminus \{0\}$ satisfies $D[c^{-1}] = R[c^{-1}]$. Then $\widetilde{D}$ is a Dedekind domain and $\widetilde{D}[c^{-1}] = \widetilde{R}[c^{-1}]$. By Proposition 1.6, $\widetilde{R}$ is a f.g. $\widetilde{D}$-algebra, and hence also a f.g. D-algebra. Lemma 1.8 implies that R is a f.g. D-algebra. □

1.4. **Annihilators.** Let A be a ring. Given an A-module M we denote by

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

the annihilator of M (an ideal of A), and if x is an element of M we also write $\operatorname{ann}_A(x)$ for the annihilator of the submodule Ax of M, called the annihilator of x. The annihilator $\operatorname{ann}_{\mathbb{Z}}(A)$ of A viewed as a $\mathbb{Z}$-module is either the zero ideal, in which case we say that the characteristic of A is 0, or contains a smallest positive integer, called the *characteristic* of A. (Notation: $\operatorname{char}(A)$.)

In the following we let $N := N(A)$. We also set $A_{\mathbb{Q}} := A \otimes_{\mathbb{Z}} \mathbb{Q}$, with natural morphism

$$a \mapsto \iota(a) := a \otimes 1 \colon A \to A_{\mathbb{Q}}.$$

Its kernel is the torsion subgroup

$$A_{\text{tor}} := \big\{a \in A : \operatorname{ann}_{\mathbb{Z}}(a) \neq 0\big\}$$

of the additive group of A. Suppose that the ideal A_{tor} of A is finitely generated. Then there is some integer $e \geq 1$ such that $eA_{\text{tor}} = 0$; the smallest such e is called the *exponent* of A_{tor}. One checks easily that then

$$\iota^{-1}N(A_{\mathbb{Q}}) = (N : e) := \{a \in A : ea \in N\},$$
$$\iota^{-1}\operatorname{ann}_{A_{\mathbb{Q}}}\big(\iota(a)\big) = \operatorname{ann}_A(ea) \quad \text{for each } a \in A.$$

The following lemma on the existence of nilpotent elements with prime annihilators is used in Section 6. (Note that if ϵ is as in the conclusion of the lemma, then $\epsilon^2 = 0$ and $A/\operatorname{ann}_A(\epsilon)$ is an integral domain of characteristic zero.)

Lemma 1.10. *Suppose that A is noetherian and $\operatorname{ann}_{\mathbb{Z}}(N) = 0$. Then there is some $\epsilon \in N$ with $\operatorname{ann}_A(\epsilon)$ prime and $\operatorname{ann}_{\mathbb{Z}}(\epsilon) = 0$.*

Proof. Note that the hypothesis $\operatorname{ann}_{\mathbb{Z}}(N) = 0$ implies not only that N is nonzero, but also that some nonzero element of N remains nonzero under ι; in particular, $N(A_{\mathbb{Q}}) \neq 0$. Let $\mathcal{A}$ be the set of annihilators of nonzero elements of $N(A_{\mathbb{Q}})$. Then $\mathcal{A} \neq \varnothing$, and as $A_{\mathbb{Q}}$ is noetherian, we may find a maximal element $P \in \mathcal{A}$. Scaling if need be, we may assume that $P = \operatorname{ann}_{A_{\mathbb{Q}}}(\iota(a))$ where $a \in \iota^{-1}N(A_{\mathbb{Q}}) = (N : e)$, $e =$ exponent of A_{tor}. The ideal P is prime, as if $xy\iota(a) = 0$ while neither $x\iota(a) = 0$ nor $y\iota(a) = 0$, then $P \subseteq \operatorname{ann}_{A_{\mathbb{Q}}}(y\iota(a))$ with $x \in \operatorname{ann}_{A_{\mathbb{Q}}}(y\iota(a)) \setminus P$, contradicting maximality. Thus, $\operatorname{ann}_A(ea) = \iota^{-1}P$ is prime and $\operatorname{ann}_{\mathbb{Z}}(ea) = 0$, so $\epsilon := ea$ does the job. □

1.5. **A bijectivity criterion.** In the proof of Proposition 7.1 we apply the following criterion:

Lemma 1.11. *Let $\phi\colon A \to B$ be a morphism of additively written abelian groups. Let N be a subgroup of A. Suppose that the restriction of ϕ to N is injective, and the morphism $\overline{\phi}\colon A/N \to B/\phi(N)$ induced by ϕ is bijective. Then ϕ is bijective.*

Proof. Let $a \in A$, $a \neq 0$. If $a \in N$, then $\phi(a) \neq 0$, since the restriction of ϕ to N is injective. Suppose $a \notin N$. Then $\phi(a) \notin \phi(N)$ since $\overline{\phi}$ is injective; in particular, $\phi(a) \neq 0$. Hence ϕ is injective. To prove that ϕ is surjective, let $b \in B$. Since $\overline{\phi}$ is onto, there is some $a \in A$ such that $b - \phi(a) \in \phi(N)$, so $b \in \phi(A)$ as required. □

2. Preliminaries: Interpretations

In this section we recall the notion of interpretation, and record a few consequences (some of which may be well-known) of bi-interpretability with $\mathbb{N}$. We begin by discussing definability in quotients of definable equivalence relations. Throughout this section, we let $\boldsymbol{A} = (A, \dots)$ be a structure in some language $\mathcal{L} = \mathcal{L}_{\boldsymbol{A}}$ and $\boldsymbol{B} = (B, \dots)$ be a structure in some language $\mathcal{L}_{\boldsymbol{B}}$.

2.1. **Definability in quotients.** Let E be a definable equivalence relation on a definable set $S \subseteq A^m$, with natural surjection $\pi_E\colon S \to S/E$. Note that for $X \subseteq S$ we have $X = \pi_E^{-1}(\pi_E(X))$ iff X is *E-invariant,* that is, for all $(a, b) \in E$ we have $a \in X$ iff $b \in X$. A subset of S/E is said to be *definable* in $\boldsymbol{A}$ if its preimage under π_E is definable in $\boldsymbol{A}$; equivalently, if it is the image of some definable subset of S under π_E. A map $S/E \to S'/E'$, where E' is a definable equivalence relation on some definable set S' in $\boldsymbol{A}$, is said to be definable in $\boldsymbol{A}$ if its graph, construed as a subset of $(S/E) \times (S'/E')$, is definable. Here and below, given an equivalence relation E on a set S and an equivalence relation E' on S', we identify $(S/E) \times (S/E')$ in the natural way with $(S \times S')/(E \times E')$, where $E \times E'$ is the equivalence relation on $S \times S'$ given by

$$(a, a')\ (E \times E')\ (b, b') \quad :\Longleftrightarrow \quad aEb \text{ and } a'E'b' \qquad (a, b \in S, a', b' \in S).$$

2.2. **Interpretations.** A surjective map $f\colon M \to B$, where $M \subseteq A^m$ (for some m) is an *interpretation of $\boldsymbol{B}$ in $\boldsymbol{A}$* (notation: $f\colon \boldsymbol{A} \rightsquigarrow \boldsymbol{B}$) if for every set $S \subseteq B^n$ which is definable in $\boldsymbol{B}$, the preimage $f^{-1}(S)$ of S under the map

$$(a_1, \dots, a_n) \mapsto \big(f(a_1), \dots, f(a_n)\big)\colon M^n \to B^n,$$

which we also denote by f, is a definable subset of $M^n \subseteq (A^m)^n = A^{mn}$. It is easy to verify that a surjective map $f\colon M \to B$ ($M \subseteq A^m$) is an interpretation of $\boldsymbol{B}$ in $\boldsymbol{A}$ iff the kernel

$$\ker f := \big\{(a, b) \in M \times M : f(a) = f(b)\big\}$$

of f, as well as the preimages of the interpretations (in $\boldsymbol{B}$) of each relation symbol and the graphs of the interpretations of each function symbol from $\mathcal{L}_{\boldsymbol{B}}$, are definable in $\boldsymbol{A}$. If the parameters in the formula defining $\ker f$ and in the formulas defining the preimages of the interpretations of the symbols of $\mathcal{L}_{\boldsymbol{B}}$ in $\boldsymbol{A}$ can be chosen to come from some set $X \subseteq A$, we say that f is an X-interpretation of $\boldsymbol{B}$ in $\boldsymbol{A}$, or an interpretation of $\boldsymbol{B}$ in $\boldsymbol{A}$ over X. An interpretation $\boldsymbol{A} \rightsquigarrow \boldsymbol{A}$ is called a *self-interpretation* of $\boldsymbol{A}$. (A trivial example is the identity interpretation $\mathrm{id}_{\boldsymbol{A}}\colon A \to A$.)

We say that $\boldsymbol{B}$ *is interpretable in* $\boldsymbol{A}$ if there exists an interpretation of $\boldsymbol{B}$ in $\boldsymbol{A}$. Given such an interpretation $f\colon M \to B$ of $\boldsymbol{B}$ in $\boldsymbol{A}$, we write $\overline{M} := M/\ker f$ for the set of equivalence classes of the equivalence relation $\ker f$, and $\overline{f}$ for the bijective map $\overline{M} \to B$ induced by f. Then $\overline{M}$ is the universe of a unique $\mathcal{L}_{\boldsymbol{B}}$-structure $f^*(\boldsymbol{B})$ such that $\overline{f}$ becomes an isomorphism $f^*(\boldsymbol{B}) \to \boldsymbol{B}$. We call the $\mathcal{L}_{\boldsymbol{B}}$-structure $f^*(\boldsymbol{B})$ the *copy of* $\boldsymbol{B}$ *interpreted in* $\boldsymbol{A}$ *via the interpretation* f.

The composition of two interpretations $f\colon \boldsymbol{A} \rightsquigarrow \boldsymbol{B}$ and $g\colon \boldsymbol{B} \rightsquigarrow \boldsymbol{C}$ is the interpretation $g \circ f\colon \boldsymbol{A} \rightsquigarrow \boldsymbol{C}$ defined in the natural way: if $f\colon M \to B$ and $g\colon N \to C$, then $g \circ f\colon f^{-1}(N) \to C$ is an interpretation of $\boldsymbol{C}$ in $\boldsymbol{A}$. In this case, the restriction of f to a map $f^{-1}(N) \to N$ induces an isomorphism $(g \circ f)^*(\boldsymbol{C}) \to g^*(\boldsymbol{C})$ between the copy $(g \circ f)^*(\boldsymbol{C}) = f^{-1}(N)/\ker(g \circ f)$ of $\boldsymbol{C}$ interpreted in $\boldsymbol{A}$ via $g \circ f$ and the copy $g^*(\boldsymbol{C}) = N/\ker g$ of $\boldsymbol{C}$ interpreted in $\boldsymbol{B}$ via g which makes the diagram

$$\begin{tikzcd}
(g \circ f)^*(\boldsymbol{C}) \arrow[rr] \arrow[dr, "\overline{g \circ f}"'] & & g^*(\boldsymbol{C}) \arrow[dl, "\overline{g}"] \\
& \boldsymbol{C} &
\end{tikzcd}$$

commute. One verifies easily that the composition of interpretations makes the class of all first-order structures into the objects of a category whose morphisms are the interpretations.

Suppose $\boldsymbol{B}$ is interpretable in $\boldsymbol{A}$ via an $\emptyset$-interpretation $f\colon M \to B$. Then every automorphism σ of $\boldsymbol{A}$ induces a permutation of M and of $\ker f$, and there is a unique permutation $\overline{\sigma}$ of B such that $\overline{\sigma} \circ f = f \circ \sigma$; this permutation $\overline{\sigma}$ is an automorphism of $\boldsymbol{B}$. The resulting map $\sigma \mapsto \overline{\sigma}\colon \operatorname{Aut}(\boldsymbol{A}) \to \operatorname{Aut}(\boldsymbol{B})$ is a continuous group morphism [11, Theorem 5.3.5], denoted by $\operatorname{Aut}(f)$. We therefore have a covariant functor Aut from the category of structures and $\emptyset$-interpretations to the category of topological groups and continuous morphisms between them. (Here the topology on automorphism groups is that described in [11, Section 4.1].)

If $\boldsymbol{B}$ and $\boldsymbol{B}'$ are structures which are interpretable in $\boldsymbol{A}$, then their direct product $\boldsymbol{B} \times \boldsymbol{B}'$ is also interpretable in $\boldsymbol{A}$; in fact, if $f\colon M \to B$ ($M \subseteq A^m$) is an interpretation $\boldsymbol{A} \rightsquigarrow \boldsymbol{B}$, and $f'\colon M' \to B'$ ($M' \subseteq A^{m'}$) is an interpretation $\boldsymbol{A} \rightsquigarrow \boldsymbol{B}'$, then $f \times f'\colon M \times M' \to B \times B'$ is an interpretation $\boldsymbol{A} \rightsquigarrow \boldsymbol{B} \times \boldsymbol{B}'$.

The concept of interpretation allows for an obvious uniform variant: Let $\mathfrak{A}$ be a class of $\mathcal{L}$-structures and $\mathfrak{B}$ be a class of structures in a language $\mathcal{L}'$, for simplicity of exposition assumed to be relational. A *uniform interpretation* of $\mathfrak{B}$ in $\mathfrak{A}$ is given by the following data:

(1) $\mathcal{L}$-formulas $\sigma(z)$, $\mu(x; z)$, and $\varepsilon(x, x'; z)$; and
(2) for each n-ary relation symbol R of $\mathcal{L}'$ an $\mathcal{L}$-formula $\rho_R(y_R; z)$.

Here x, x' are m-tuples of variables (for some m), y_R as in (2) is an mn-tuple of variables, and z is a p-tuple of variables (for some p). All variables in these tuples are assumed to be distinct. For $\boldsymbol{A} \in \mathfrak{A}$ set $S^{\boldsymbol{A}} := \{s \in A^p : \boldsymbol{A} \models \sigma(s)\}$. We require that

(U1) for each $\boldsymbol{A} \in \mathfrak{A}$ and $s \in S^{\boldsymbol{A}}$, the set $M_s := \{a \in A^m : \boldsymbol{A} \models \mu(a; s)\}$ is nonempty, $\varepsilon(x, x'; s)$ defines an equivalence relation E_s on M_s, and for each $R \in \mathcal{L}'$, the set R_s defined by $\rho(y_R; s)$ in $\boldsymbol{A}$ is E_s-invariant.

Letting $\pi_s\colon M_s \to M_s/E_s$ be the natural surjection, the quotient M_s/E_s then becomes the underlying set of an $\mathcal{L}'$-structure $\boldsymbol{B}_s$ interpreted in $\boldsymbol{A}$ by π_s. We also require that

(U2) $\boldsymbol{B}_s \in \mathfrak{B}$ for each $\boldsymbol{A} \in \mathfrak{A}$, $s \in S^{\boldsymbol{A}}$, and for each $B \in \mathfrak{B}$ there are some $\boldsymbol{A} \in \mathfrak{A}$, $s \in S^{\boldsymbol{A}}$ such that $\boldsymbol{B} \cong \boldsymbol{B}_s$.

We say that $\mathfrak{B}$ is *uniformly interpretable* in $\mathfrak{A}$ if there exists a uniform interpretation of $\mathfrak{B}$ in $\mathfrak{A}$. Clearly the relation of uniform interpretability is transitive. If $\mathfrak{B} = \{\boldsymbol{B}\}$ is a singleton, we also say that $\boldsymbol{B}$ is uniformly interpretable in $\mathfrak{A}$; similarly if $\mathfrak{A}$ is a singleton.

2.3. **Homotopy and bi-interpretations.** Following [1], we say that interpretations $f\colon M \to B$ and $f'\colon M' \to B$ of $\boldsymbol{B}$ in $\boldsymbol{A}$ are *homotopic* (in symbols: $f \simeq f'$) if the pullback

$$[f = f'] := \big\{(x, x') \in M \times M' : f(x) = f'(x')\big\}$$

of f and f' is definable in $\boldsymbol{A}$; equivalently, if there exists an isomorphism

$$\alpha\colon f^*(\boldsymbol{B}) \to (f')^*(\boldsymbol{B})$$

which is definable in $\boldsymbol{A}$ such that $\overline{f'} \circ \alpha = \overline{f}$. So for example if f is a self-interpretation of $\boldsymbol{A}$, then $f \simeq \mathrm{id}_A$ if and only if the isomorphism $\overline{f}\colon f^*(\boldsymbol{A}) \to \boldsymbol{A}$ is definable in $\boldsymbol{A}$. Homotopy is an equivalence relation on the collection of interpretations of $\boldsymbol{B}$ in $\boldsymbol{A}$. Given $X \subseteq A$, we say that interpretations $f\colon \boldsymbol{A} \rightsquigarrow \boldsymbol{B}$ and $f'\colon \boldsymbol{A} \rightsquigarrow \boldsymbol{B}$ are X-homotopic if $[f = f']$ is X-definable. It is easy to verify that if the $\emptyset$-interpretations $f, f'\colon \boldsymbol{A} \rightsquigarrow \boldsymbol{B}$ are $\emptyset$-homotopic, then $\mathrm{Aut}(f) = \mathrm{Aut}(f')$.

Lemma 2.1. *Let $f, f'\colon \boldsymbol{A} \rightsquigarrow \boldsymbol{B}$ and $g, g'\colon \boldsymbol{B} \rightsquigarrow \boldsymbol{C}$. Then*

(1) *$g \simeq g' \Rightarrow g \circ f \simeq g' \circ f$; and*
(2) *if g is injective, then $f \simeq f' \Rightarrow g \circ f \simeq g \circ f'$.*

Proof. For (1), note that if $[g = g']$ is definable in $\boldsymbol{B}$, then $[g \circ f = g' \circ f] = f^{-1}\big([g = g']\big)$ is definable in $\boldsymbol{A}$, and for (2) note that if g is injective then we have $[g \circ f = g \circ f'] = [f = f']$. $\square$

Let $f\colon \boldsymbol{A} \rightsquigarrow \boldsymbol{B}$ and $g\colon \boldsymbol{B} \rightsquigarrow \boldsymbol{A}$. One says that the pair (f, g) is a *bi-interpretation* between $\boldsymbol{A}$ and $\boldsymbol{B}$ if $g \circ f \simeq \mathrm{id}_{\boldsymbol{A}}$ and $f \circ g \simeq \mathrm{id}_{\boldsymbol{B}}$; that is, if the isomorphism $\overline{g \circ f}\colon (g \circ f)^*(\boldsymbol{A}) \to \boldsymbol{A}$ is definable in $\boldsymbol{A}$, and the isomorphism $\overline{f \circ g}\colon (f \circ g)^*(\boldsymbol{B}) \to \boldsymbol{B}$ is definable in $\boldsymbol{B}$. (See Figure 1.) The relation of bi-interpretability is easily seen to be an equivalence relation on the class of first-order structures. A bi-interpretation (f, g) between $\boldsymbol{A}$ and $\boldsymbol{B}$ is an *$\emptyset$-bi-interpretation* if f, g are $\emptyset$-interpretations and $g \circ f$ and $f \circ g$ are $\emptyset$-homotopic to the respective identity interpretations. If (f, g) is such an $\emptyset$-bi-interpretation between $\boldsymbol{A}$ and $\boldsymbol{B}$, then $\mathrm{Aut}(f)$ is a continuous isomorphism $\mathrm{Aut}(\boldsymbol{A}) \to \mathrm{Aut}(\boldsymbol{B})$ with inverse $\mathrm{Aut}(g)$.

Lemma 2.2. *Let (f, g) be a bi-interpretation between $\boldsymbol{A}$ and $\boldsymbol{B}$. Then for every subset S of B^k ($k \geq 1$) we have*

$$S \text{ is definable in } \boldsymbol{B} \quad \Longleftrightarrow \quad f^{-1}(S) \text{ is definable in } \boldsymbol{A}.$$

Proof. The forward direction follows from the definition of "f is an interpretation of $\boldsymbol{B}$ in $\boldsymbol{A}$." For the converse, suppose $f^{-1}(S)$ is definable in $\boldsymbol{A}$; then the set $S' := (f \circ g)^{-1}(S) = g^{-1}\big(f^{-1}(S)\big)$ is definable in $\boldsymbol{B}$ (since g is an interpretation of $\boldsymbol{A}$ in $\boldsymbol{B}$). For $y \in B^k$ we have $y \in S$ iff $(f \circ g)(x) = y$ for some $x \in S'$. Therefore, since $[f \circ g = \mathrm{id}_B]$ and S' are definable in $\boldsymbol{B}$, so is S. $\square$

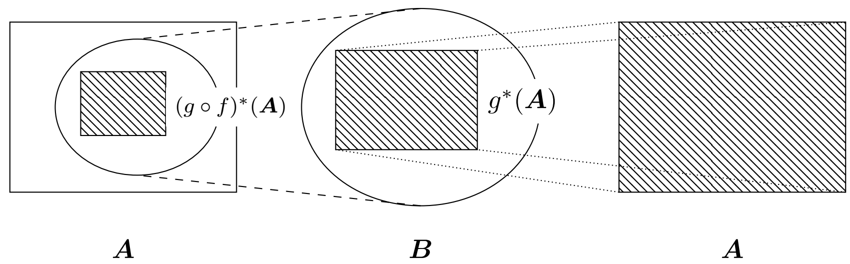

FIGURE 1. Composition $g \circ f$ of $f\colon \boldsymbol{A} \rightsquigarrow \boldsymbol{B}$ and $g\colon \boldsymbol{B} \rightsquigarrow \boldsymbol{A}$.

The previous lemma may be refined to show that a bi-interpretation between $\boldsymbol{A}$ and $\boldsymbol{B}$ in a natural way gives rise to an equivalence of categories between the category of definable sets and maps in $\boldsymbol{A}$ and the category of definable sets and maps in $\boldsymbol{B}$. (See [20].)

Corollary 2.3. *Let (f, g) be as in Lemma 2.2, and $f', f''\colon \boldsymbol{A} \rightsquigarrow \boldsymbol{B}$. If $f' \circ g \simeq f'' \circ g$, then $f' \simeq f''$.*

Proof. Note that $g^{-1}\big([f' = f'']\big) = [f' \circ g = f'' \circ g]$ and use Lemma 2.2. $\square$

2.4. **Weak homotopy and weak bi-interpretations.** The notion of bi-interpretability allows for a number of subtle variations, one of which (close to the notion of bi-interpretability used in [11, Chapter 5]) we introduce in this subsection. Given two interpretations $f\colon \boldsymbol{A} \rightsquigarrow \boldsymbol{B}$ and $f'\colon \boldsymbol{A} \rightsquigarrow \boldsymbol{B}'$ of (possibly different) $\mathcal{L}_{\boldsymbol{B}}$-structures in $\boldsymbol{A}$, we say that f and f' are *weakly homotopic* if there is an isomorphism $f^*(\boldsymbol{B}) \to (f')^*(\boldsymbol{B}')$ which is definable in $\boldsymbol{A}$; notation: $f \sim f'$. Clearly $\sim$ is an equivalence relation on the class of interpretations of $\mathcal{L}_{\boldsymbol{B}}$-structures in $\boldsymbol{A}$, and "homotopic" implies "weakly homotopic." (Note that $f \simeq f'$ only makes sense if $\boldsymbol{B} = \boldsymbol{B}'$, whereas $f \sim f'$ merely implies $\boldsymbol{B} \cong \boldsymbol{B}'$.) The following is easy to verify, and is a partial generalization of the fact that $f \simeq f'$ implies $\operatorname{Aut}(f) = \operatorname{Aut}(f')$:

Lemma 2.4. *Let $f\colon \boldsymbol{A} \rightsquigarrow \boldsymbol{B}$ and $f'\colon \boldsymbol{A} \rightsquigarrow \boldsymbol{B}'$, and let $\beta\colon f^*(\boldsymbol{B}) \to (f')^*(\boldsymbol{B}')$ be an isomorphism, definable in $\boldsymbol{A}$. Put*

$$\gamma := \overline{f'} \circ \beta \circ \overline{f}^{-1}\colon \boldsymbol{B} \xrightarrow{\cong} \boldsymbol{B}'.$$

Then $\operatorname{Aut}(f) = \gamma \operatorname{Aut}(f')\, \gamma^{-1}$.

We say that a pair (f, g), where $f\colon \boldsymbol{A} \rightsquigarrow \boldsymbol{B}$ and $g\colon \boldsymbol{B} \rightsquigarrow \boldsymbol{A}$, is a *weak bi-interpretation* between $\boldsymbol{A}$ and $\boldsymbol{B}$ if $g \circ f \sim \mathrm{id}_{\boldsymbol{A}}$ and $f \circ g \sim \mathrm{id}_{\boldsymbol{B}}$. The equivalence relation on the class of first-order structures given by bi-interpretability is finer than that of weak bi-interpretability, and in general, might be strictly finer. In Section 2.7 below we see, however, that as far as bi-interpretability with $\mathbb{N}$ is concerned, there is no difference between the two notions.

2.5. **Injective interpretations.** An *injective interpretation* of $\boldsymbol{B}$ in $\boldsymbol{A}$ is an interpretation $f\colon \boldsymbol{A} \rightsquigarrow \boldsymbol{B}$ where $f\colon M \to B$ ($M \subseteq A^m$) is injective (and hence bijective). (See [11, Section 5.4 (a)].) We also say that the structure $\boldsymbol{B}$ is *injectively interpretable in* $\boldsymbol{A}$ if $\boldsymbol{B}$ admits an injective interpretation in $\boldsymbol{A}$.

An important special case of injective interpretations is furnished by relativized reducts. Recall (cf. [11, Section 5.1]) that $\boldsymbol{B}$ is said to be a *relativized reduct* of $\boldsymbol{A}$

if the universe B of $\boldsymbol{B}$ is a subset of A^m, for some m, definable in $\boldsymbol{A}$, and the interpretations of the function and relation symbols of $\mathcal{L}_{\boldsymbol{B}}$ in $\boldsymbol{B}$ are definable in $\boldsymbol{A}$. In this case, $\boldsymbol{B}$ is injectively interpretable in $\boldsymbol{A}$, with the interpretation given by the identity map on B.

Example 2.5. The semiring $(\mathbb{N}, +, \times)$ is a relativized reduct of the ring $(\mathbb{Z}, +, \times)$. (By Lagrange's Four Squares Theorem.)

If $\boldsymbol{A}$ has uniform elimination of imaginaries, then every interpretation of $\boldsymbol{B}$ in $\boldsymbol{A}$ is homotopic to an injective interpretation of $\boldsymbol{B}$ in $\boldsymbol{A}$ [11, Theorem 5.4.1]. This applies to $\boldsymbol{A} = \mathbb{Z}$, and in combination with the fact that every infinite definable subset of $\mathbb{Z}^m$ is in definable bijection with $\mathbb{Z}$, this yields:

Lemma 2.6. *Every interpretation of an infinite structure $\boldsymbol{A}$ in the ring $\mathbb{Z}$ of integers is homotopic to an injective interpretation of $\boldsymbol{A}$ in $\mathbb{Z}$ whose domain is $\mathbb{Z}$.*

So for example, if an infinite semiring S is interpretable in $\mathbb{Z}$, then there are definable binary operations $\oplus$ and $\otimes$ on $\mathbb{Z}$ such that $(\mathbb{Z}, \oplus, \otimes)$ is isomorphic to S.

Lemma 2.7. *Every self-interpretation of $\mathbb{Z}$ is homotopic to the identity interpretation.*

Proof. Let $f \colon M \to \mathbb{Z}$ be a self-interpretation of $\mathbb{Z}$, where $M \subseteq \mathbb{Z}^m$. By Lemma 2.6 we may assume that f is bijective, $m = 1$, and $M = \mathbb{Z}$. Hence the copy of $\mathbb{Z}$ interpreted in itself via f has the form $Z = (\mathbb{Z}, \oplus, \otimes)$ where $\oplus$ and $\otimes$ are binary operations on $\mathbb{Z}$ definable in $\mathbb{Z}$. Let 0_Z and 1_Z denote the additive and multiplicative identity elements of the ring Z. The successor function $k \mapsto \sigma(k) := k \oplus 1_Z \colon \mathbb{Z} \to \mathbb{Z}$ in the ring Z is definable in $\mathbb{Z}$. Therefore the unique isomorphism $\mathbb{Z} \to Z$, given by $k \mapsto \sigma^k(0_Z)$ for $k \in \mathbb{Z}$, is computable, and hence definable in $\mathbb{Z}$; its inverse is $\overline{f}$. $\square$

Due to the previous lemma, the task of checking that a pair of interpretations forms a bi-interpretation between $\boldsymbol{A}$ and $\mathbb{Z}$ simplifies somewhat: a pair (f, g), where $f \colon \boldsymbol{A} \rightsquigarrow \mathbb{Z}$ and $g \colon \mathbb{Z} \rightsquigarrow \boldsymbol{A}$, is a bi-interpretation between $\boldsymbol{A}$ and $\mathbb{Z}$ iff $g \circ f \simeq \mathrm{id}_{\boldsymbol{A}}$.

Corollary 2.8. *If $\boldsymbol{A}$ and $\mathbb{Z}$ are bi-interpretable, then any two interpretations of $\mathbb{Z}$ in $\boldsymbol{A}$ are homotopic.*

Proof. Suppose (f, g), where $f \colon \boldsymbol{A} \rightsquigarrow \mathbb{Z}$ and $g \colon \mathbb{Z} \rightsquigarrow \boldsymbol{A}$, is a bi-interpretation between $\boldsymbol{A}$ and $\mathbb{Z}$. Let f' be an arbitrary interpretation $\boldsymbol{A} \rightsquigarrow \mathbb{Z}$. Then $f \circ g$ and $f' \circ g$ are self-interpretations of $\mathbb{Z}$. Therefore $f \circ g \simeq f' \circ g$ by Lemma 2.7 and thus $f \simeq f'$ by Corollary 2.3. $\square$

2.6. **Interpretations among rings.** *In this subsection we let A be a ring.* Familiar ring-theoretic constructions can be seen as interpretations:

Examples 2.9.

(1) Let S be a commutative semiring, and suppose A is the Grothendieck ring associated to S, that is, $A = (S \times S)/E$ where E is the equivalence relation on $S \times S$ given by $(x, y)E(x', y') :\Longleftrightarrow x + y' = x' + y$. Then the natural map $S \times S \to A$ is an interpretation of A in S.
(2) For an ideal I of A which is definable in A (as a subset of A), the residue morphism $A \to A/I$ is an interpretation of A/I in A.
(3) Suppose $A = A_1 \times A_2$ is the direct product of rings A_1, A_2. Then both factors A_1 and A_2 are interpretable in A. (By the last example applied to the ideals $I_1 = Ae_2$ respectively $I_2 = Ae_1$, where $e_1 = (1, 0)$, $e_2 = (0, 1)$.)

(4) Let S be a multiplicative subset of A (that is, $1 \in S$, $0 \notin S$, and $S \cdot S \subseteq S$). Suppose S is definable. Then the map
$$M := A \times S \to A[S^{-1}]\colon (a,s) \mapsto a/s$$
is an interpretation of the localization $A[S^{-1}]$ of A at S in A. Its kernel is the equivalence relation
$$(a,s) \sim (a',s') \qquad \Longleftrightarrow \qquad \exists t \in S \ \big(t \cdot (as' - a's) = 0\big)$$
on M. In particular, if A is an integral domain, then its fraction field is interpretable in A.

Let S be a multiplicative subset of A. One says that S is *saturated* if for all $a, b \in A$ we have $ab \in S$ if $a \in S$ and $b \in S$. Equivalently, S is saturated iff $A \setminus S$ is a union of prime ideals of A. There is a smallest saturated multiplicative subset $\overline{S}$ of A which contains S (called the *saturation* of S); here $A \setminus \overline{S}$ is the union of all prime ideals of A which do not intersect S, and $A[S^{-1}] = A[\overline{S}^{-1}]$. (See [3, Chapter 3, exercises].)

Lemma 2.10. *Suppose A is a finite-dimensional noetherian Jacobson ring, and $c \in A$. Then $A[c^{-1}]$ is interpretable in A.*

Proof. By Lemma 1.5, the union of all prime ideals of A which do not contain c is definable in A, hence so is the saturation $\overline{S}$ of the multiplicative subset $c^{\mathbb{N}} = \{c^n : n = 0,1,2,\dots\}$ of A. Thus $A[c^{-1}] = A[\overline{S}^{-1}]$ is interpretable in A by Examples 2.9, (4). □

Suppose A is noetherian. Then every finite ring extension B of A is interpretable in A: choose generators $b_1,\dots,b_m$ of B as an A-module, and let K be the kernel of the surjective A-linear map $\pi\colon A^m \to B$ given by $(a_1,\dots,a_m) \mapsto \sum_i a_i b_i$. Then K is a f.g. A-submodule of A^m, hence definable in A. The multiplication map on B may be encoded by a bilinear form on A^m. Thus π is an interpretation of B in A.

One says that A has finite rank n if each f.g. ideal of A can be generated by n elements. In this case, every submodule of R^m can be generated by mn elements [5]. Hence we obtain:

Lemma 2.11. *Suppose A is noetherian of finite rank. Then the class of finite ring extensions of A generated by m elements as A-module is uniformly interpretable in A.*

This fact, together with its corollary below, are used in the proof of Theorem 3.1.

Corollary 2.12. *Suppose A is noetherian of finite rank, and let A' be a flat ring extension of A. Then the class of rings of the form $A' \otimes_A B$, where B is a finite ring extension of A generated by m elements as an A-module, is uniformly interpretable in A'.*

Proof. Let B be a ring extension of A generated as an A-module by $b_1,\dots,b_m$. With π, K as before we have an exact sequence
$$0 \to K \xrightarrow{\subseteq} A^m \xrightarrow{\pi} B \to 0.$$
Tensoring with A' yields an exact sequence
$$0 \to A' \otimes_A K \longrightarrow (A')^m \xrightarrow{1\otimes\pi} A' \otimes_A B \to 0.$$

The image of K under $x \mapsto 1 \otimes x$ generates the A'-module $A' \otimes_A K$, and the extension of the bilinear form on the A-module A^m which describes the ring multiplication on B to a bilinear form on the A'-module $(A')^m$ also describes the ring multiplication on $A' \otimes_A B$. $\square$

We finish this subsection by recording a detailed proof of the well-known fact that all finitely generated rings are interpretable in $\mathbb{Z}$. The proof is a typical application of Gödel coding in arithmetic, and we assume that the reader is familiar with the basics of this technique; see, for example, [41, Section 6.4]. (Later in the paper, such routine coding arguments will usually only be sketched.) Let β be a Gödel function, i.e., a function $\mathbb{N}^2 \to \mathbb{N}$, definable in Peano Arithmetic (in fact, much weaker systems of arithmetic are enough), so that for any finite sequence $(a_1, \dots, a_n)$ of natural numbers there exists $a \in \mathbb{N}$ such that $\beta(a, 0) = n$ (the length of the sequence) and $\beta(a, i) = a_i$ for $i = 1, \dots, n$. It is routine to construct from β a function $\gamma\colon \mathbb{N}^2 \to \mathbb{Z}$ which is definable in $\mathbb{Z}$ and which encodes finite sequences of integers, i.e., such that for each $(a_1, \dots, a_n) \in \mathbb{Z}^n$ there exists $a \in \mathbb{N}$ with $\gamma(a, 0) = n$ and $\gamma(a, i) = a_i$ for $i = 1, \dots, n$.

Lemma 2.13. *Suppose A is interpretable in $\mathbb{Z}$, and let X be an indeterminate over A. Then $A[X]$ is also interpretable in $\mathbb{Z}$.*

Proof. For simplicity we assume that A is infinite (the case of a finite A being similar). Let $g\colon \mathbb{Z} \to A$ be an injective interpretation of A in $\mathbb{Z}$. (Lemma 2.6.) Let

$$N := \big\{a \in \mathbb{N} : \gamma(a, 0) \geq 1, \text{ and } \gamma(a, 0) \geq 2 \Rightarrow \gamma(a, \gamma(a, 0)) \neq 0\big\}$$

be the set of codes of finite sequences $(a_0, \dots, a_n) \in \mathbb{Z}^{n+1}$ such that $a_n \neq 0$ if $n \geq 1$. Clearly N is definable in $\mathbb{Z}$. It is easy to check that then the map

$$N \to A[X]\colon a \mapsto \sum_{i=0}^{\gamma(a,0)-1} g\big(\gamma(a, i+1)\big)\, X^i$$

is an injective interpretation of $A[X]$ in $\mathbb{Z}$. $\square$

The previous lemma in combination with Examples 2.9, (2) and (4) yields:

Corollary 2.14. *Every f.g. ring and every localization of a f.g. ring at a definable multiplicative subset is interpretable in $\mathbb{Z}$.*

Remarks (uniform interpretations in and of $\mathbb{Z}$)*.* The following remarks are not used later in this paper.

(1) The proof of Corollary 2.14 can be refined to show that the class of f.g. rings is *uniformly* interpretable in $\mathbb{Z}$.
(2) See [38, Section 2] for a proof that $\mathbb{Z}$ is uniformly interpretable in the class of infinite f.g. fields. By (2) and (4) of Examples 2.9, if $\mathfrak{p}$ is a prime ideal of A, then the fraction field of $A/\mathfrak{p}$ is interpretable in A. Using remark (2) following Lemma 1.5 this implies that for each n, the class of infinite fields generated (as fields) by n elements is uniformly interpretable in the class $\mathfrak{A}_n$ of infinite rings generated by n elements. Hence for each n, $\mathbb{Z}$ is uniformly interpretable in $\mathfrak{A}_n$. We do not know whether $\mathbb{Z}$ is uniformly interpretable in the class $\bigcup_n \mathfrak{A}_n$ of infinite f.g. rings. (This question was also asked in [12].)

2.7. **Bi-interpretability with $\mathbb{Z}$.** In this subsection we deduce a few useful consequences of bi-interpretability with $\mathbb{Z}$.

Suppose first that $\boldsymbol{A}$ and $\mathbb{Z}$ are weakly bi-interpretable, and let (f, g') be a weak bi-interpretation between $\boldsymbol{A}$ and $\mathbb{Z}$. By Lemma 2.6 there is an injective interpretation $g\colon \mathbb{Z} \to A$ of $\boldsymbol{A}$ in $\mathbb{Z}$ with $g \simeq g'$. By Lemma 2.1, (1) we have $g \circ f \simeq g' \circ f \sim \mathrm{id}_{\boldsymbol{A}}$, and by Lemma 2.7 we have $f \circ g \simeq \mathrm{id}_{\mathbb{Z}}$. Hence (f, g) is a weak bi-interpretation between $\boldsymbol{A}$ and $\mathbb{Z}$, and if (f, g') is even a bi-interpretation between $\boldsymbol{A}$ and $\mathbb{Z}$, then so is (f, g). Thus, if there is a weak bi-interpretation between $\boldsymbol{A}$ and $\mathbb{Z}$ at all, then there is such a weak bi-interpretation (f, g) where g is a bijection $\mathbb{Z} \to A$; similarly with "bi-interpretation" in place of "weak bi-interpretation."

As a first application of these remarks, we generalize Lemma 2.7 from $\mathbb{Z}$ to all structures bi-interpretable with $\mathbb{Z}$.

Corollary 2.15. *If $\boldsymbol{A}$ and $\mathbb{Z}$ are bi-interpretable, then every self-interpretation of $\boldsymbol{A}$ is homotopic to* $\mathrm{id}_{\boldsymbol{A}}$. (*Hence if $\boldsymbol{A}$ and $\mathbb{Z}$ are bi-interpretable, then any pair of interpretations $\boldsymbol{A} \rightsquigarrow \mathbb{Z}$ and $\mathbb{Z} \rightsquigarrow \boldsymbol{A}$ is a bi-interpretation between $\boldsymbol{A}$ and $\mathbb{Z}$.*)

Proof. Let (f, g) be a bi-interpretation between $\boldsymbol{A}$ and $\mathbb{Z}$ where g is a bijection $\mathbb{Z} \to A$, and let $h\colon \boldsymbol{A} \rightsquigarrow \boldsymbol{A}$. Then $f \circ h \circ g \simeq \mathrm{id}_{\mathbb{Z}}$ by Lemma 2.7, thus $h \circ g \simeq g$ by Lemma 2.1 (and injectivity of g), and so $h \simeq \mathrm{id}_{\boldsymbol{A}}$ by Corollary 2.3. □

For the following corollary (used in the proof of Theorem 3.1 below), suppose we are given an isomorphism $\alpha\colon \boldsymbol{A} \to \widetilde{\boldsymbol{A}}$ of $\mathcal{L}$-structures. Then α acts on definable objects in the natural way. For example, if $i\colon M \to D$ ($M \subseteq A^m$) is an interpretation of $\boldsymbol{D}$ in $\boldsymbol{A}$, then $i \circ \alpha\colon \alpha(M) \to D$ is an interpretation of $\boldsymbol{D}$ in $\widetilde{\boldsymbol{A}}$, and α induces an isomorphism $\overline{\alpha}\colon i^*(\boldsymbol{D}) \to (i \circ \alpha)^*(\boldsymbol{D})$. Note that the underlying set of $(i \circ \alpha)^*(\boldsymbol{D})$ is $\alpha(M)/\ker(i \circ \alpha^{-1})$.

Corollary 2.16. *Let $i\colon \boldsymbol{A} \rightsquigarrow \boldsymbol{D}$ and $j\colon \boldsymbol{D} \rightsquigarrow \boldsymbol{A}$, and let $\widetilde{\boldsymbol{A}} := (j \circ i)^*(\boldsymbol{A})$ and α denote the inverse of the isomorphism $\overline{j \circ i}\colon \widetilde{\boldsymbol{A}} \to \boldsymbol{A}$. Suppose $\boldsymbol{D}$ is bi-interpretable with $\mathbb{Z}$. Then $\overline{\alpha}\colon i^*(\boldsymbol{D}) \to (i \circ \alpha)^*(\boldsymbol{D})$ is definable in $\boldsymbol{A}$.*

Proof. One checks that i induces an isomorphism $(i \circ \alpha)^*(\boldsymbol{D}) \to (i \circ j)^*(\boldsymbol{D})$ which makes the diagram

$$\begin{tikzcd}
(i \circ j)^*(\boldsymbol{D}) \arrow[r, "\overline{i \circ j}"] & \boldsymbol{D} \\
(i \circ \alpha)^*(\boldsymbol{D}) \arrow[u] \arrow[r, "\overline{j \circ i}"] & i^*(\boldsymbol{D}) \arrow[u, "\overline{i}"']
\end{tikzcd}$$

commutative. By Corollary 2.15, the self-interpretation $i \circ j$ of $\boldsymbol{D}$ is homotopic to $\mathrm{id}_{\boldsymbol{D}}$, that is, $\overline{i \circ j}$ is definable in $\boldsymbol{D}$, and so $\alpha = (\overline{j \circ i})^{-1}$ is definable in $\boldsymbol{A}$. □

Let now $f\colon \boldsymbol{A} \rightsquigarrow \mathbb{Z}$ and $g\colon \mathbb{Z} \rightsquigarrow \boldsymbol{A}$, where g is a bijection $\mathbb{Z} \to A$. We are going to analyze this situation in some more detail. Let $\widetilde{\mathbb{Z}} = f^*(\mathbb{Z})$ and $\widetilde{\boldsymbol{A}} = (g \circ f)^*(\boldsymbol{A})$. We have isomorphisms $\overline{g \circ f}\colon \widetilde{\boldsymbol{A}} \to \boldsymbol{A}$ and $\overline{f}\colon \widetilde{\mathbb{Z}} \to \mathbb{Z}$. Note that as g is bijective, we have

$$\widetilde{A} = f^{-1}(\mathbb{Z})/\ker(g \circ f) = M/\ker f,$$

so $\widetilde{\boldsymbol{A}}$ and $\widetilde{\mathbb{Z}}$ have the same underlying set, and we have a commutative diagram

$$\begin{tikzcd} \mathbb{Z} \arrow[rr, "g"] & & A \\ & \widetilde{\mathbb{Z}} = \widetilde{A} \arrow[ul, "\overline{f}"] \arrow[ur, "\overline{g\circ f}"'] & \end{tikzcd}$$

which shows the subtle fact that the identity map $\widetilde{\mathbb{Z}} \to \widetilde{A}$ is an interpretation of $\widetilde{\boldsymbol{A}}$ in $\widetilde{\mathbb{Z}}$.

For the next lemma, we say that a structure with the same universe as $\boldsymbol{A}$ is *interdefinable* with $\boldsymbol{A}$ if both structures have the same definable sets.

Lemma 2.17. *The following are equivalent:*

1. $\boldsymbol{A}$ *is bi-interpretable with* $\mathbb{Z}$*;*
2. $\boldsymbol{A}$ *is weakly bi-interpretable with* $\mathbb{Z}$*;*
3. *there are binary operations* $\oplus$ *and* $\otimes$ *on* A *such that*
   (a) $(\mathbb{Z}, +, \times) \cong (A, \oplus, \otimes)$*;*
   (b) $(A, \oplus, \otimes)$ *is interdefinable with* $\boldsymbol{A} = (A, \dots)$*.*

Proof. It is clear that if we have binary operations $\oplus$ and $\otimes$ on A satisfying conditions (a) and (b) in (3), then (f, g), where $f\colon A \to \mathbb{Z}$ is the unique isomorphism $(A, \oplus, \otimes) \to (\mathbb{Z}, +, \times)$ and $g = f^{-1}$, is a bi-interpretation between $\boldsymbol{A}$ and $\mathbb{Z}$. Conversely, suppose $\boldsymbol{A}$ is weakly bi-interpretable with $\mathbb{Z}$ via a weak bi-interpretation (f, g) where g is a bijection $\mathbb{Z} \to A$. Let α be an isomorphism $\widetilde{\boldsymbol{A}} = (g \circ f)^*(\boldsymbol{A}) \to \boldsymbol{A}$, definable in $\boldsymbol{A}$. Let $\oplus$ and $\otimes$ be the binary operations on A such that β is an isomorphism $(\widetilde{\mathbb{Z}}, +, \times) \to (A, \oplus, \otimes)$. (Recall that $\widetilde{\mathbb{Z}} = \widetilde{A}$ as sets.) The operations $\oplus$ and $\otimes$ are then definable in $\boldsymbol{A}$; conversely, since α is also an isomorphism of $\mathcal{L}$-structures $\widetilde{\boldsymbol{A}} \to \boldsymbol{A}$ and the identity $\widetilde{\mathbb{Z}} \to \widetilde{A}$ is an interpretation of $\widetilde{\boldsymbol{A}}$ in $\widetilde{\mathbb{Z}}$, the interpretations of the function and relation symbols of $\mathcal{L}$ in $\boldsymbol{A}$ are definable in $(A, \oplus, \otimes)$. $\square$

As an illustration of this analysis, next we show:

Lemma 2.18. *Suppose* $\boldsymbol{A}$ *is bi-interpretable with* $\mathbb{Z}$*. Let* $\Phi\colon A \to A$ *be definable, and let* $a \in A$*. Then the orbit*

$$\Phi^{\mathbb{N}}(a) := \big\{\Phi^{\circ n}(a) : n = 0, 1, 2, \dots\big\} \qquad (\Phi^{\circ n} = n\text{th iterate of } \Phi)$$

of a *under* Φ *is definable.*

Proof. Via Gödel coding of sequences, it is easy to see that the lemma holds if $\boldsymbol{A} = \mathbb{Z}$. In the general case, suppose $\otimes, \oplus$ are binary operations on A satisfying conditions (a) and (b) of the previous lemma. Then the map Φ is also definable in $(A, \oplus, \otimes)$, hence $\Phi^{\mathbb{N}}(a)$ is definable in $(A, \oplus, \otimes)$, and thus also in $\boldsymbol{A}$. $\square$

Let us note two consequences of Lemma 2.18 for rings.

Corollary 2.19. *Let* A *be a ring of characteristic zero which is bi-interpretable with* $\mathbb{Z}$*. Then the natural image of* $\mathbb{Z}$ *in* A *is definable as a subring of* A*.*

Proof. The image of $\mathbb{Z}$ is $(x \mapsto x+1)^{\mathbb{N}}(0) \cup (x \mapsto x-1)^{\mathbb{N}}(0)$. Apply Lemma 2.18. $\square$

Corollary 2.20. *Let* A *be a ring which is bi-interpretable with* $\mathbb{Z}$*, and* $a \in A$*. Then the set* $a^{\mathbb{N}} := \{a^n : n = 0, 1, 2, \dots\}$ *of powers of* a *is definable.*

Proof. The set $a^{\mathbb{N}}$ is $(x \mapsto ax)^{\mathbb{N}}(1)$. Apply Lemma 2.18. $\square$

Here is a refinement of Lemma 2.18. For an interpretation f of $\mathbb{Z}$ in $\boldsymbol{A}$, the restriction of f to a map $f^{-1}(\mathbb{N}) \to \mathbb{N}$ is an interpretation of $\mathbb{N}$ in $\boldsymbol{A}$, and by abuse of notation we denote the copy of $\mathbb{N}$ interpreted in $\boldsymbol{A}$ via this interpretation by $f^*(\mathbb{N})$, and we write $n \mapsto \overline{n}$ for the inverse of the isomorphism $f^*(\mathbb{N}) \to \mathbb{N}$.

Lemma 2.21. *Suppose $\boldsymbol{A}$ is bi-interpretable with $\mathbb{Z}$, and let $f \colon \boldsymbol{A} \rightsquigarrow \mathbb{Z}$. Let $\Phi \colon A \to A$ be definable. Then the map*

$$(a, \overline{n}) \mapsto \Phi^{\circ n}(a) \colon A \times f^*(\mathbb{N}) \to A$$

is definable.

Proof. Let $g \colon \mathbb{Z} \to A$ be an injective interpretation $\mathbb{Z} \rightsquigarrow \boldsymbol{A}$; then (f, g) is a bi-interpretation between $\boldsymbol{A}$ and $\mathbb{Z}$. (Corollary 2.15.) Let $\oplus$ and $\otimes$ be the binary operations on A making g an isomorphism $(\mathbb{Z}, +, \times) \to (A, \oplus, \otimes)$. Then $\oplus$ and $\otimes$ satisfy (a) and (b) in Lemma 2.17 (by the proof of said lemma). The map Φ is definable in $(A, \oplus, \otimes)$, and thus

$$(a, b) \mapsto \Phi^{\circ g^{-1}(b)}(a) \colon A \times g(\mathbb{N}) \to A$$

is definable in $(A, \oplus, \otimes)$, and hence also in $\boldsymbol{A}$. Therefore, since $[g \circ f = \mathrm{id}_A]$ is definable in $\boldsymbol{A}$, so is (the graph of) the map

$$(a, b) \mapsto \Phi^{\circ f(b)}(a) \colon A \times f^{-1}(\mathbb{N}) \to A.$$

The lemma follows. $\square$

The last lemma immediately implies:

Corollary 2.22. *Let A be a ring which is bi-interpretable with $\mathbb{Z}$, and let $f \colon A \rightsquigarrow \mathbb{Z}$. Then the map*

$$(a, \overline{n}) \mapsto a^n \colon A \times f^*(\mathbb{N}) \to A$$

is definable.

2.8. **A test for bi-interpretability with $\mathbb{Z}$.** Suppose that (f, g) is a weak bi-interpretation between $\boldsymbol{A}$ and $\mathbb{Z}$ where g is a bijection $\mathbb{Z} \to A$. As remarked in the previous subsection, we then have $f^*(\mathbb{Z}) = (g \circ f)^*(A)$ as sets, so the inverse of any definable isomorphism $(g \circ f)^*(\boldsymbol{A}) \to \boldsymbol{A}$ (which exists since $g \circ f \sim \mathrm{id}_{\boldsymbol{A}}$) is a bijection $A \to f^*(\mathbb{Z})$ which is definable in $\boldsymbol{A}$. The following proposition is a partial converse of this observation:

Proposition 2.23. *Suppose that $\boldsymbol{A}$ is f.g. and the language $\mathcal{L} = \mathcal{L}_{\boldsymbol{A}}$ of $\boldsymbol{A}$ is finite. Let $f \colon \boldsymbol{A} \rightsquigarrow \mathbb{Z}$ and $g \colon \mathbb{Z} \rightsquigarrow \boldsymbol{A}$. Suppose also that there exists an injective map $A \to f^*(\mathbb{Z})$ which is definable in $\boldsymbol{A}$. Then (f, g) is a weak bi-interpretation between $\boldsymbol{A}$ and $\mathbb{Z}$.*

An important consequence of this proposition (and Lemma 2.17) is that under reasonable assumptions on $\boldsymbol{A}$ and $\mathcal{L}$, establishing bi-interpretability of $\boldsymbol{A}$ with $\mathbb{Z}$ simply amounts to showing that $\boldsymbol{A}$ is interpretable in $\mathbb{Z}$, and $\mathbb{Z}$ is interpretable in $\boldsymbol{A}$ in such a way that there is a definable way to index the elements of $\boldsymbol{A}$ with elements of the copy of $\mathbb{Z}$ in $\boldsymbol{A}$:

Corollary 2.24 (Nies)**.** *If $\boldsymbol{A}$ is f.g. and $\mathcal{L}$ is finite, then the following are equivalent:*

(1) *$\boldsymbol{A}$ is (weakly) bi-interpretable with $\mathbb{Z}$;*

(2) *$\boldsymbol{A}$ is interpretable in $\mathbb{Z}$, and there is an interpretation f of $\mathbb{Z}$ in $\boldsymbol{A}$ and an injective definable map $A \to f^*(\mathbb{Z})$.*

A proof of this corollary of Proposition 2.23 is sketched in [26, Proposition 7.12]. However, we feel that a more detailed argument is warranted. (Also note that loc. cit. does not assume $\boldsymbol{A}$ to be f.g.) Before we give a proof of Proposition 2.23, we show two auxiliary facts:

Lemma 2.25. *Let f be a self-interpretation of $\boldsymbol{A}$ which is homotopic to the identity. Then every set $X \subseteq f^*(A)^n$ which is definable in $\boldsymbol{A}$ is definable in $f^*(\boldsymbol{A})$.*

Proof. Suppose f is given by $M \to A$ where $M \subseteq A^m$ is definable. Let $\xi(x_1, \dots, x_n)$ be an $\mathcal{L}$-formula, possibly involving parameters, which defines X in $\boldsymbol{A}$; that is, for all $a \in M^n \subseteq (A^m)^n$ we have

$$\boldsymbol{A} \models \xi(a) \quad \Longleftrightarrow \quad \overline{a} \in X.$$

By hypothesis, the isomorphism $\overline{f}\colon f^*(\boldsymbol{A}) \to \boldsymbol{A}$ is definable in $\boldsymbol{A}$. Let $\varphi(x, y)$ define its graph; that is, for $a \in M$ and $b \in A$ we have

$$\boldsymbol{A} \models \varphi(a, b) \quad \Longleftrightarrow \quad \overline{f}(\overline{a}) = b.$$

Set

$$\xi^*(y_1, \dots, y_n) := \exists x_1 \cdots \exists x_n \left(\xi(x_1, \dots, x_n) \ \& \ \bigwedge_{i=1}^{n} \varphi(x_i, y_i) \right).$$

Then for $a \in M^n$ we have

$$\begin{aligned} f^*(\boldsymbol{A}) \models \xi^*(\overline{a}) &\Longleftrightarrow \boldsymbol{A} \models \xi^*(\overline{f}(\overline{a})) \\ &\Longleftrightarrow \boldsymbol{A} \models \exists x_1 \cdots \exists x_n \left(\xi(x_1, \dots, x_n) \ \& \ \bigwedge_{i=1}^{n} \varphi\big(x_i, \overline{f}(\overline{a_i})\big) \right) \\ &\Longleftrightarrow \boldsymbol{A} \models \xi(a) \iff \overline{a} \in X. \end{aligned}$$

hence ξ^* defines X in $f^*(\boldsymbol{A})$. $\square$

Lemma 2.26. *Let $\boldsymbol{A}$ be a f.g. structure in a finite language. Then any two interpretations of $\boldsymbol{A}$ in $\mathbb{Z}$ are homotopic.*

Proof. Let $f, g\colon \mathbb{Z} \rightsquigarrow \boldsymbol{A}$; by Lemma 2.6 we may assume that f and g are injective with domain $\mathbb{Z}$. Let $a_1, \dots, a_n \in A$ be generators for $\boldsymbol{A}$ and let $b_i := \overline{f}^{-1}(a_i)$, $c_i := \overline{g}^{-1}(a_i)$, for $i = 1, \dots, n$, be the corresponding elements of $f^*(A)$ and $g^*(A)$, respectively. The unique isomorphism $f^*(\boldsymbol{A}) \to g^*(\boldsymbol{A})$ given by $b_i \mapsto c_i$ ($i = 1, \dots, n$) is relatively computable and hence definable in $\mathbb{Z}$. $\square$

We now show Proposition 2.23. Thus, let $f\colon \boldsymbol{A} \rightsquigarrow \mathbb{Z}$ and $g\colon \mathbb{Z} \rightsquigarrow \boldsymbol{A}$, and let $\phi\colon A \to f^*(\mathbb{Z})$ be an injective map, definable in $\boldsymbol{A}$. By Lemma 2.7 we have $f \circ g \simeq \mathrm{id}_{\mathbb{Z}}$, so it is enough to show that $g \circ f \sim \mathrm{id}_{\boldsymbol{A}}$. Recall that g induces an isomorphism $(f \circ g)^*(\mathbb{Z}) \to f^*(\mathbb{Z})$, and thus, pulling back ϕ under $\overline{g}$ we obtain a $g^*(\boldsymbol{A})$-definable injective map $g^*(\phi)\colon g^*(A) \to (f \circ g)^*(\mathbb{Z})$ making the diagram

$$\begin{tikzcd} A \arrow[r, "\phi"] & f^*(\mathbb{Z}) \\ g^*(A) \arrow[u, "\overline{g}"] \arrow[r, "g^*(\phi)"] & (f \circ g)^*(\mathbb{Z}) \arrow[u] \end{tikzcd}$$

commute. We make its image $g^*(\phi)\big(g^*(A)\big)$ the universe of an $\mathcal{L}$-structure, which we denote by $g^*(\phi)\big(g^*(\boldsymbol{A})\big)$, such that $g^*(\phi)$ becomes an isomorphism. Note that both the underlying set $g^*(\phi)\big(g^*(A)\big)$ as well as the interpretations of the function and relation symbols of $\mathcal{L}$ in this structure are definable in $g^*(\boldsymbol{A})$, hence in $\mathbb{Z}$, and so, by Lemma 2.25, also in $(f\circ g)^*(\mathbb{Z})$. Thus we obtain an interpretation h of $\boldsymbol{A}$ in $(f\circ g)^*(\mathbb{Z})$ with $h^*(\boldsymbol{A}) = g^*(\phi)\big(g^*(\boldsymbol{A})\big)$. On the other hand, suppose g is given by $N\to A$ where $N\subseteq\mathbb{Z}^n$; then setting

$$N' := (\overline{f\circ g})^{-1}(N), \qquad g' := g\circ(\overline{f\circ g})\restriction N',$$

we have another interpretation $g'\colon (f\circ g)^*(\mathbb{Z}) \rightsquigarrow \boldsymbol{A}$. By Lemma 2.26, the interpretations h and g' are homotopic. Thus we have an isomorphism $h^*(\boldsymbol{A})\to(g')^*(\boldsymbol{A})$ which is definable in $(f\circ g)^*(\mathbb{Z})$, and hence in $g^*(\boldsymbol{A})$. Composing this isomorphism with the isomorphism $g^*(\phi)\colon g^*(\boldsymbol{A})\to h^*(\boldsymbol{A})$, which is also definable in $g^*(\boldsymbol{A})$, yields an isomorphism $g^*(\boldsymbol{A})\to(g')^*(\boldsymbol{A})$ which is definable in $g^*(\boldsymbol{A})$. It is routine to verify that the isomorphism $\overline{g}\colon g^*(\boldsymbol{A})\to\boldsymbol{A}$ maps the domain N' of g' bijectively onto the domain $f^{-1}(N)$ of $g\circ f$, and that this bijection induces a bijection $(g')^*(A)\to(g\circ f)^*(A)$ which is compatible with $\overline{g'}$ and $\overline{g\circ f}$, and hence an isomorphism $(g')^*(\boldsymbol{A})\to(g\circ f)^*(\boldsymbol{A})$. Thus our definable isomorphism $g^*(\boldsymbol{A})\to(g')^*(\boldsymbol{A})$ gives rise to an isomorphism $\boldsymbol{A}\to(g\circ f)^*(\boldsymbol{A})$ which fits into the commutative diagram

$$\begin{tikzcd}
\boldsymbol{A} \arrow[r] & (g\circ f)^*(\boldsymbol{A}) \\
g^*(\boldsymbol{A}) \arrow[u, "\overline{g}"] \arrow[r] & (g')^*(\boldsymbol{A}) \arrow[u]
\end{tikzcd}$$

and which is definable in $\boldsymbol{A}$, as required. $\square$

2.9. **Quasi-finite axiomatizability.** *In this subsection we assume that $\mathcal{L}$ is finite and $\boldsymbol{A}=(A,\dots)$ is f.g.* We say that an $\mathcal{L}$-formula $\varphi_{\boldsymbol{A}}(x_1,\dots,x_n)$ is a *QFA formula* for $\boldsymbol{A}$ with respect to the system of generators $a_1,\dots,a_n$ of $\boldsymbol{A}$ if the following holds: if $\boldsymbol{A}'$ is any f.g. $\mathcal{L}$-structure and $a_1',\dots,a_n'\in A'$, then $\boldsymbol{A}'\models\varphi_{\boldsymbol{A}}(a_1',\dots,a_n')$ iff there is an isomorphism $\boldsymbol{A}\to\boldsymbol{A}'$ with $a_i\mapsto a_i'$ for $i=1,\dots,n$. Any two QFA formulas for $\boldsymbol{A}$ with respect to the same system of generators of $\boldsymbol{A}$ are equivalent in $\boldsymbol{A}$. Moreover:

Lemma 2.27. *Let $\varphi_{\boldsymbol{A}}(x_1,\dots,x_n)$ be a QFA formula for $\boldsymbol{A}$ with respect to the system of generators $a_1,\dots,a_n$ of $\boldsymbol{A}$. Then for each system of generators $b_1,\dots,b_m$ of $\boldsymbol{A}$ there is a QFA formula for $\boldsymbol{A}$ with respect to $b_1,\dots,b_m$.*

Proof. For notational simplicity we assume that $m=n=1$ (the general case is only notationally more complicated). Let b be a generator for A. Let $s(x)$, $t(y)$ be $\mathcal{L}$-terms such that $a=t^{\boldsymbol{A}}(b)$ and $b=s^{\boldsymbol{A}}(a)$. Put $\psi(y):=\varphi(t(y))\wedge y=s(t(y))$. Then ψ is a QFA formula for $\boldsymbol{A}$ with respect to b. $\square$

A QFA formula for $\boldsymbol{A}$ is a formula $\varphi_{\boldsymbol{A}}(x_1,\dots,x_n)$ which is QFA for $\boldsymbol{A}$ with respect to some system of generators $a_1,\dots,a_n$ of $\boldsymbol{A}$. Note that if there is a QFA formula $\varphi_{\boldsymbol{A}}(x_1,\dots,x_n)$ for $\boldsymbol{A}$, then $\boldsymbol{A}$ is *quasi-finitely axiomatizable* (*QFA*), i.e., there is an $\mathcal{L}$-sentence σ such that for every $\mathcal{L}$-structure $\boldsymbol{A}'$, we have $\boldsymbol{A}'\models\sigma$ iff $\boldsymbol{A}\cong\boldsymbol{A}'$. (Take $\sigma=\exists x_1\cdots\exists x_n\varphi_{\boldsymbol{A}}$.) If A is finite, then there clearly is a QFA formula for $\boldsymbol{A}$. In this subsection we are going to show (see [26, Theorem 7.14]):

Proposition 2.28. *If $\boldsymbol{A}$ is bi-interpretable with $\mathbb{Z}$, then there is a QFA formula for $\boldsymbol{A}$.*

Before we give the proof of this proposition, we make some observations. For these, we assume that the hypothesis of Proposition 2.28 holds, that is, that we have binary operations $\oplus$ and $\otimes$ on A as in (a) and (b) of Lemma 2.17. We take $\mathcal{L}$-formulas $\varphi_\oplus(x_1, x_2, y, z)$ and $\varphi_\otimes(x_1, x_2, y, z)$, where $z = (z_1, \dots, z_k)$ for some $k \in \mathbb{N}$, and for each function symbol f of $\mathcal{L}$, of arity m, and for each function symbol R of $\mathcal{L}$, of arity n, we take formulas $\varphi_f(x_1, \dots, x_m, y)$ and $\varphi_R(x_1, \dots, x_n)$ in the language of rings, and some $c \in A^k$, such that

(1) $\varphi_\oplus(x_1, x_2, y, c)$ and $\varphi_\otimes(x_1, x_2, y, c)$ define $\oplus$ and $\otimes$ in $\boldsymbol{A}$, respectively;
(2) $\varphi_f(x_1, \dots, x_m, y)$ and $\varphi_R(x_1, \dots, x_n)$ define $f^{\boldsymbol{A}}$ and $R^{\boldsymbol{A}}$, respectively, in $(A, \oplus, \otimes)$.

We now let $\alpha_0(z)$ be an $\mathcal{L}$-formula which expresses (1) and (2) above, i.e., such that $\boldsymbol{A} \models \alpha_0(c)$, and for all $\mathcal{L}$-structures $\boldsymbol{A'}$ and $c' \in (A')^k$ such that $\boldsymbol{A'} \models \alpha_0(c')$,

(1) $\varphi_\oplus(x_1, x_2, y, c')$ and $\varphi_\otimes(x_1, x_2, y, c')$ define binary operations $\oplus'$ and $\otimes'$, respectively, on A'; and
(2) $\varphi_f(x_1, \dots, x_m, y)$ and $\varphi_R(x_1, \dots, x_n)$ define $f^{\boldsymbol{A'}}$ and $R^{\boldsymbol{A'}}$, respectively, in $(A', \oplus', \otimes')$, for all function symbols f and relation symbols R of $\mathcal{L}$.

We also require that if $\boldsymbol{A'} \models \alpha_0(c')$, then

(3) $(A', \oplus', \otimes')$ is a ring which is a model of a sufficiently large (to be specified) finite fragment of $\mathrm{Th}(\mathbb{Z})$.

The ring $(A', \oplus', \otimes')$ may be *non-standard,* that is, not isomorphic to $(\mathbb{Z}, +, \times)$. However, choosing the finite fragment of arithmetic in (3) appropriately, we can ensure that we have a unique embedding $(\mathbb{Z}, +, \times) \to (A', \oplus', \otimes')$. From now on we assume that α_0 has been chosen in this way. Additionally we can choose α_0 so that finite objects, such as $\mathcal{L}$-terms and finite sequences of elements of A', can be encoded in $(A', \oplus', \otimes')$. This can be used to uniformly define term functions in $\boldsymbol{A'}$, and leads to a proof of the following (see [26, Claim 7.15] for the details):

Lemma 2.29. *There is an $\mathcal{L}$-formula $\alpha(z)$, which logically implies $\alpha_0(z)$, such that $\boldsymbol{A} \models \alpha(c)$, and whenever $\boldsymbol{A'}$ is a f.g. $\mathcal{L}$-structure and $c' \in (A')^k$, then $\boldsymbol{A'} \models \alpha(c')$ iff $(A', \oplus', \otimes')$ is standard.*

Let now $t = (t_1, \dots, t_n)$ be a tuple of constant terms in the language of rings. Given $\boldsymbol{A'} \models \alpha_0(c')$, we denote by $t(c') = \big(t_1(c'), \dots, t_n(c')\big)$ the tuple containing the interpretations of the t_i in the ring $(A', \oplus', \otimes')$. We also let α be as in the previous lemma.

Lemma 2.30. *Let $\boldsymbol{A'}$ is a f.g. $\mathcal{L}$-structure and $c' \in (A')^k$ with $\boldsymbol{A'} \models \alpha(c')$. Then the orbit of $t(c')$ under $\mathrm{Aut}(\boldsymbol{A'})$ is $\emptyset$-definable in $\boldsymbol{A'}$.*

Proof. We claim that for $a' = (a'_1, \dots, a'_n) \in (A')^n$ we have

$$\sigma(t(c')) = a' \text{ for some } \sigma \in \mathrm{Aut}(\boldsymbol{A'}) \iff t(c'') = a' \text{ for some } c'' \text{ with } \boldsymbol{A'} \models \alpha(c'').$$

Here the forward direction is clear. For the backward direction suppose $\boldsymbol{A'} \models \alpha(c'')$, and let $\oplus''$, $\otimes''$ denote the binary operations on A' defined by $\varphi_\oplus(x_1, x_2, y, c'')$, $\varphi_\otimes(x_1, x_2, y, c'')$, respectively. We then have a unique isomorphism $(A', \oplus', \otimes') \to (A', \oplus'', \otimes'')$. This isomorphism maps $t(c')$ onto $t(c'')$, and is also an automorphism of $\boldsymbol{A'}$, by condition (2) in the description of α_0 above. This shows the claim, and hence the lemma. $\square$

Proof of Proposition 2.28. Let $a_1, \dots, a_n \in A$ generate $\boldsymbol{A}$, and let $t_1, \dots, t_n$ be the constant terms in the ring language corresponding to the images of $a_1, \dots, a_n$, respectively, under the isomorphism $(A, \oplus, \otimes) \to (\mathbb{Z}, +, \times)$. Then for each f.g. $\mathcal{L}$-structure $\boldsymbol{A}'$ and $a'_1, \dots, a'_n \in A'$, there is an isomorphism $\boldsymbol{A} \to \boldsymbol{A}'$ with $a_i \mapsto a'_i$ $(i = 1, \dots, n)$ iff there is some c' such that $\boldsymbol{A}' \models \alpha(c')$ and an automorphism of $\boldsymbol{A}'$ with $t_i(c') \mapsto a'_i$ $(i = 1, \dots, n)$. By the lemma above, the latter condition is definable. □

3. Integral Domains

The goal of this section is to show the following theorem:

Theorem 3.1. *Every infinite f.g. integral domain is bi-interpretable with $\mathbb{Z}$.*

Combining this theorem with Proposition 2.28 immediately yields:

Corollary 3.2. *Every f.g. integral domain has a QFA formula.*

Although Theorem 3.1 can be deduced from the main result of [38] (and is unaffected by the error therein), we prefer to start from scratch and give a self-contained proof of this fact.

In the rest of this section we let A be an integral domain with fraction field K.

3.1. Noether Normalization and some of its applications.

Our main tool is the Noether Normalization Lemma in the following explicit form:

Proposition 3.3. *Suppose that A is a f.g. D-algebra, where D is a subring of A. Then there are a nonzero $c \in D$ and $x_1, \dots, x_n \in A$, algebraically independent over D, such that $A[c^{-1}]$ is a finitely generated $D[c^{-1}, x_1, \dots, x_n]$-module.*

If the field K is f.g., we define the *arithmetic* (or *Kronecker*) dimension of A as

$$\operatorname{adim}(A) := \begin{cases} \operatorname{trdeg}_{\mathbb{Q}}(K) + 1 & \text{if } \operatorname{char}(A) = 0, \\ \operatorname{trdeg}_{\mathbb{F}_p}(K) & \text{if } \operatorname{char}(A) = p > 0. \end{cases}$$

As a consequence of Proposition 3.3, if the integral domain A is f.g., then $\operatorname{adim}(A)$ equals the Krull dimension $\dim(A)$ of A.

Proposition 3.3 is particularly useful when combined with the following fact (a basic version of Grothendieck's "generic flatness lemma"); see [43, Theorem 2.1].

Proposition 3.4. *Suppose that A is a f.g. D-algebra, where D is a subring of A. Then there is some $c \in D \setminus \{0\}$ such that $A[c^{-1}]$ is a free $D[c^{-1}]$-module.*

The integral domain A is said to be *Japanese* if the integral closure of A in a finite-degree field extension of K is always a finitely generated A-module. Every finitely generated integral domain is Japanese; see [23, Theorem 36.5].

Lemma 3.5. *Let D be a Japanese noetherian subring of A, $x_1, \dots, x_n \in A$ be algebraically independent over D, and suppose that A is finite over $R = D[x_1, \dots, x_n]$. Then every subring of A which contains D and is algebraic over D, is finite over D.*

Proof. Let B be a subring of A with $D \subseteq B$ which is algebraic over D. We first show that B is integral over D. Let $b \in B$. Then b is integral over R, that is, satisfies an equation of the form $f(b)=0$ for some monic polynomial $f \in R[Y]$ in the indeterminate Y. With $\alpha=(\alpha_1,\dots,\alpha_n)$ ranging over $\mathbb{N}^n$, write

$$f = \sum_{\alpha} x^{\alpha} f_{\alpha}(Y) \qquad \text{where } x^{\alpha} = x_1^{\alpha_1}\cdots x_n^{\alpha_n} \text{ and } f_{\alpha}(Y) \in D[Y].$$

Since B is algebraic over D, $x_1,\dots,x_n$ remain algebraically independent over B. Hence, $f_{\alpha}(b)=0$ for all α. In particular, $f_{\mathbf{o}}(b)=0$ and the polynomial $f_{\mathbf{o}}$ is monic. Therefore, b is integral over D.

Next we note that $K=\operatorname{Frac}(A)$ is a finite-degree field extension of $L:=\operatorname{Frac}(R)$. Again because $x_1,\dots,x_n$ are algebraically independent over B, each D-linearly independent sequence $b_1,\dots,b_m$ of elements of B is also R-linearly independent and hence L-linearly independent, and so $m \leq [K:L]$. Take D-linearly independent $b_1,\dots,b_m \in B$ with m maximal, and set $M := D[b_1,\dots,b_m]$. Then M is a f.g. D-submodule of B, and the quotient module B/M is torsion. Hence $\operatorname{Frac}(B) = \operatorname{Frac}(M)$, and the degree of $\operatorname{Frac}(M)$ over $\operatorname{Frac}(D)$ is finite. Therefore the integral closure of D in $\operatorname{Frac}(B)$ is a f.g. D-module; since this integral closure contains B and D is noetherian, B is a f.g. D-module as well. $\square$

With the following lemma we establish a basic result in commutative algebra. It bears noting here that our hypothesis that the subring in question has arithmetic dimension one is necessary. It is not hard to produce non-finitely generated two-dimensional subrings of finitely generated integral domains.

Lemma 3.6. *Suppose A is finitely generated. Then every subring of A of arithmetic dimension 1 is finitely generated.*

Proof. Let B be a subring of A with $\operatorname{adim}(B)=1$. If $\operatorname{char}(A)=0$, then let $D:=\mathbb{Z}\subseteq B$. If $\operatorname{char}(A)=p>0$, pick some $t\in B$ transcendental over $\mathbb{F}_p$ and set $D:=\mathbb{F}_p[t]\subseteq B$. By Proposition 3.3 we can find some $c\in D\setminus\{0\}$ and $x_1,\dots,x_n\in A$ which are algebraically independent over D and for which $A[c^{-1}]$ is a finite integral extension of $D[c^{-1},x_1,\dots,x_n]$. Since $\operatorname{adim}(B)=1$, $B[c^{-1}]$ is algebraic over $D[c^{-1}]$. Hence by Lemma 3.5 applied to $A[c^{-1}]$, $D[c^{-1}]$ in place of A, D, respectively, $B[c^{-1}]$ is a finitely generated $D[c^{-1}]$-module. Choose generators $y_1,\dots,y_m$ of $B[c^{-1}]$ as $D[c^{-1}]$-module. Scaling by a sufficiently high power of c, we may assume that each y_i belongs to B and is integral over D. Then setting $R:=D[y_1,\dots,y_m]$ we have $R\subseteq B\subseteq B[c^{-1}]=R[c^{-1}]$. By Corollary 1.9, B is a f.g. R-algebra, hence also a f.g. ring. $\square$

3.2. **Proof of Theorem 3.1.** *In this subsection we assume that A is f.g.* We begin by showing that as an easy consequence of results of J. Robinson, R. Robinson, and Rumely, each f.g. integral domain of dimension 1 is bi-interpretable with $\mathbb{Z}$. We deal with characteristic zero and positive characteristic in separate lemmata:

Lemma 3.7. *Suppose that* $\operatorname{char}(A)=0$ *and* $\dim(A)=1$. *Then A is bi-interpretable with $\mathbb{N}$.*

Proof. The field extension $K|\mathbb{Q}$ is finite; set $d:=[K:\mathbb{Q}]$. J. Robinson showed [35] that the ring $\mathcal{O}_K$ of algebraic integers in K is definable in K, and the subset $\mathbb{Z}$ is definable in $\mathcal{O}_K$; hence $\mathbb{Z}$ is definable in A. Take an integer $c>0$ such that $A\subseteq\mathcal{O}_K[\frac{1}{c}]$. The map $n\mapsto c^n\colon\mathbb{N}\to\mathbb{N}$ is definable in A, and so is the map $\nu\colon A\to\mathbb{N}$ which associates to $a\in A$ the smallest $n:=\nu(a)\in\mathbb{N}$ such that $c^n a\in\mathcal{O}_K$. Fixing a basis $\omega_1,\dots,\omega_d\in\mathcal{O}_K$ of the free $\mathbb{Z}$-module $\mathcal{O}_K$, we obtain a definable injective map $A \hookrightarrow \mathbb{Z}^d \times \mathbb{N}$ by associating to $a \in A$ the tuple $\big(k_1(a), \dots, k_d(a), \nu(a)\big)$, where $\big(k_1(a), \dots, k_d(a)\big)$ is the unique element of $\mathbb{Z}^d$ such that $c^{\nu(a)}a = \sum_{i=1}^d k_i(a)\omega_i$. Hence, A is bi-interpretable with $\mathbb{Z}$ by Corollary 2.24. $\square$

Lemma 3.8. *Suppose that* $\operatorname{char}(A) > 0$ *and* $\dim(A) = 1$. *Then A is bi-interpretable with* $\mathbb{N}$.

Proof. Let $p := \operatorname{char}(A)$, and by Noether Normalization take some $t \in A$, transcendental over $\mathbb{F}_p$, such that A is a finite extension of $\mathbb{F}_p[t]$. Rumely [37, Theorem 2] showed that $k[t]$ is definable in K, where k is the constant field of K (i.e., the relative algebraic closure of $\mathbb{F}_p$ in K). R. Robinson [36] specified a formula $\tau(x, y)$ with the property that for each finite field $\mathbb{F}$, $\tau(x, t)$ defines the set $t^{\mathbb{N}}$ in $\mathbb{F}[t]$. It follows that the binary operations on $t^{\mathbb{N}}$ making $n \mapsto t^n : \mathbb{N} \to t^{\mathbb{N}}$ an isomorphism of semirings are definable in $\mathbb{F}[t]$. Thus, the inverse of this isomorphism is an interpretation $\mathbb{F}[t] \rightsquigarrow \mathbb{N}$. Let $N = N_p$ be the set of natural numbers of the form $n = \prod_{i\geq 1} p_i^{n_i}$ with $n_i \in \{0, 1, \dots, p-1\}$, all but finitely many $n_i = 0$, and p_i is the i^{th} prime number. Then $t^N := \{t^m : m \in N\}$ is definable in A. We have a bijection $t^N \to \mathbb{F}_p[t]$ which sends t^n, where $n = \prod_{i\geq 1} p_i^{n_i}$, to $\sum_{i\geq 0} n_i t^{i-1}$. Rumely [37, p. 211] established the definability of this map in K (and hence in A). In particular, $\mathbb{F}_p[t]$ is definable in A, and we have a definable injection $\mathbb{F}_p[t] \hookrightarrow t^{\mathbb{N}}$. Since A is a f.g. free $\mathbb{F}_p[t]$-module, we also have an $\mathbb{F}_p[t]$-linear (hence definable) bijection $A \to \mathbb{F}_p[t]^d$, for some $d \geq 1$. The lemma now follows from Corollary 2.24. $\square$

With our lemmata in place, we complete the proof of Theorem 3.1. Thus, suppose A is infinite, so $\dim(A) \geq 1$.

For each natural number n, Poonen [33] produced a formula $\theta_n(x_1, \dots, x_n)$ so that for any finitely generated field F and any n-tuple $a = (a_1, \dots, a_n) \in F^n$ one has $F \models \theta_n(a)$ if and only if the elements $a_1, \dots, a_n$ are algebraically independent. If $\operatorname{char}(A) = 0$, let

$$D := \big\{a \in A \ : \ K \models \neg\theta_1(a)\big\}.$$

If $\operatorname{char}(A) = p > 0$, then pick some $t \in A$ which is transcendental over $\mathbb{F}_p$ and set

$$D := \big\{a \in A \ : \ K \models \neg\theta_2(a, t)\big\}.$$

In both cases, D is an algebraically closed subring of A with $\operatorname{adim}(D) = 1$, definable in A. By Lemma 3.6, D is finitely generated, hence noetherian, and therefore a Dedekind domain.

By Proposition 3.3 we take some nonzero $c \in D$ and $x_1, \dots, x_m \in A$ so that $x_1, \dots, x_m$ are algebraically independent over D and $A_c := A[c^{-1}]$ is a finite integral extension of $D_c[x_1, \dots, x_m]$, where $D_c := D[c^{-1}]$. By Proposition 3.4, after further localizing at another nonzero element of D, we can also assume that A_c is a free D_c-module. Let $y_1, \dots, y_n \in A$ be generators of A_c as $D_c[x_1, \dots, x_m]$-module. Let $X = (X_1, \dots, X_m)$, $Y = (Y_1, \dots, Y_n)$ be tuples of indeterminates, and let $\mathfrak{p}$ be the kernel of the D_c-algebra morphism $D_c[X, Y] \to A_c$ given by $X_i \mapsto x_i$ and $Y_j \mapsto y_j$ for $i = 1, \dots, m$ and $j = 1, \dots, n$. Note that $\mathfrak{p} \cap D_c[X] = (0)$. Let $P_1, \dots, P_\ell$ be a sequence of generators of $\mathfrak{p}$ and let $V = V(\mathfrak{p}) \subseteq \mathbb{A}^{m+n}_{D_c}$ be the affine variety defined by $\mathfrak{p}$. Then A_c can be naturally seen as a subring of the ring of regular functions on V. For any point $a \in \mathbb{A}^m(D_c)$ there is some integral domain D' extending D_c, as a D_c-module generated by at most n elements, and some point $b \in \mathbb{A}^n(D')$ so that $(a, b) \in V(D')$.

By Lemma 2.10 we have an interpretation $D \rightsquigarrow D_c$. (We could have also used Lemma 3.7 or 3.8, in combination with Examples 2.9, (4) and Corollary 2.20.) Precomposing this interpretation with the interpretation $A \rightsquigarrow D$ given by the inclusion $D \subseteq A$ yields an interpretation of D_c in A. Lemma 2.10 also shows that A_c is interpretable in A. Every ideal of a Dedekind domain (such as D_c) is generated by two elements. Hence by Lemma 2.11 the class $\mathcal{D}$ of integral extensions of D_c generated by n elements as D_c-modules is uniformly interpretable in D_c (and hence in A), and by Corollary 2.12, the class of ring $A_c \otimes_{D_c} D'$ where $D' \in \mathcal{D}$ is uniformly interpretable in A_c (and hence in A). As a consequence the following set is definable in A:

$$\begin{aligned} E := \big\{(a, D', b, e, p) \quad : \quad & a \in \mathbb{A}^m(D_c),\ D' \in \mathcal{D},\ b \in \mathbb{A}^n(D'), \\ & (a,b) \in V(D'),\ e \in D',\ p \in A, \text{ and } p(a,b) = e\big\} \end{aligned}$$

Indeed, the condition that $(a,b) \in V(D')$ may be expressed by saying that $P_1(a,b) = \cdots = P_\ell(a,b) = 0$. That $p(a,b) = e$ is expressed by saying

$$(\exists u_1, \dots, u_m, v_1, \dots, v_n \in A_c \otimes_{D_c} D') \Big(p - e = \textstyle\sum_i v_i(x_i - a_i) + \sum_j u_j(y_j - b_j)\Big).$$

(To see this use that $A_c \otimes_{D_c} D' \cong D'[X,Y]/\mathfrak{p}D'[X,Y]$ as D'-algebras, and for all $(a,b) \in \mathbb{A}^{m+n}(D')$, the kernel of the morphism $p \mapsto p(a,b)\colon D'[X,Y] \to D'$ is generated by $X_i - a_i$ and $Y_j - b_j$.) We also note that given $p, q \in A$, we have

$$p = q \iff \begin{cases} \big(\forall a \in \mathbb{A}^m(D_c)\big)(\forall D' \in \mathcal{D})\big(\forall b \in \mathbb{A}^n(D')\big)(\forall e \in D') \\ (a, D', b, e, p) \in E \Leftrightarrow (a, D', b, e, q) \in E. \end{cases} \tag{1}$$

Let now (f,g) be a bi-interpretation between D_c and $\mathbb{N}$, let i be an interpretation of D_c in A, and let h be an interpretation of A in $\mathbb{N}$ (Corollary 2.14). Put $j := h \circ f\colon D_c \rightsquigarrow A$. Let $\widetilde{A} := (j \circ i)^*(A)$ be the copy of A interpreted via j in the copy of D_c interpreted via i in A. By Lemma 3.7 or 3.8, D_c is bi-interpretable with $\mathbb{N}$, so by Corollary 2.15, the self-interpretation $i \circ j$ of D_c is homotopic to the identity. Thus if we can show that the isomorphism $\overline{j \circ i}\colon \widetilde{A} \to A$ is definable in A, then the pair (i,j) is a bi-interpretation between A and D_c. Let α denote the inverse of $\overline{j \circ i}$. Then $i \circ \alpha$ is an interpretation of D_c in $\widetilde{A}$, and by Corollary 2.16, α induces an isomorphism $i^*(D_c) \to (i \circ \alpha)^*(D_c)$ which is definable in A. We also denote this isomorphism by α, and also denote by α the induced map on the various objects defined in $i^*(D_c)$. With this convention, put $\widetilde{E} := \alpha(E)$. Then $\widetilde{E}$ is definable in $\widetilde{A}$, and hence also in A. Therefore

$$\begin{aligned} \Gamma := \big\{(p, \widetilde{p}) \in A \times \widetilde{A} \quad : \quad & \big(\forall a \in \mathbb{A}^m(D_c)\big)(\forall D' \in \mathcal{D})\big(\forall b \in \mathbb{A}^n(D')\big)(\forall e \in D') \\ & (a, D', b, e, p) \in E \leftrightarrow \big(\alpha(a), \alpha(D'), \alpha(b), \alpha(e), \widetilde{p}\big) \in \widetilde{E}\big\} \end{aligned}$$

is definable in A, and by (1), Γ is the graph of $\alpha\colon A \to \widetilde{A}$. This implies that A is bi-interpretable with D_c, and hence with $\mathbb{N}$. □

4. Fiber Products

In this section we study finitely generated rings which can be expressed as fiber products of other rings. We first review the definition, and then successively focus on fiber products over finite rings and fiber products over infinite rings. The section culminates with a characterization of those f.g. reduced rings which are bi-interpretable with $\mathbb{Z}$.

4.1. **Definition and basic properties.** Let $\alpha\colon A \to C$ and $\beta\colon B \to C$ be two ring morphisms. The *fiber product* of A and B over C is the subring

$$A \times_C B = \big\{(a,b) \in A \times B : \alpha(a) = \beta(b)\big\}$$

of the direct product $A \times B$. The natural projections $A \times B \to A$ and $A \times B \to B$ restrict to ring morphisms $\pi_A\colon A \times_C B \to A$ and $\pi_B\colon A \times_C B \to B$, respectively. Note that if α is surjective, then π_B is surjective; similarly, if β is surjective, then so is π_A. *In the following we always assume that α, β are surjective.* We do allow C to be the zero ring; in this case, $A \times_C B = A \times B$.

Example 4.1. Let I, J be ideals of a ring R. Then the natural morphism $R/(I \cap J) \to (R/I) \times (R/J)$ maps $R/(I \cap J)$ isomorphically onto the fiber product $A \times_C B$ of $A = R/I$ and $B = R/J$ over $C = R/(I+J)$, where α and β are the natural morphisms $A = R/I \to C = R/(I+J)$ respectively $B = R/J \to C = R/(I+J)$.

Lemma 4.2. *Suppose A and B are noetherian. Then $A \times_C B$ is noetherian.*

Proof. Let $I = \ker \pi_A$, $J = \ker \pi_B$, and $R := A \times_C B$. Since $I \cap J = 0$, we have a natural embedding of R into the ring $(R/I) \times (R/J)$. The ring morphism π_A, π_B induce isomorphisms $R/I \to A$, $R/J \to B$. Thus R/I and R/J are noetherian as rings and hence as R-modules. So the product $(R/I) \times (R/J)$, and hence its submodule R, is a noetherian R-module as well. □

Corollary 4.3. *Suppose A and B are noetherian. Then π_A is an interpretation of A in $A \times_C B$, and π_B is an interpretation of B in $A \times_C B$, and hence $\pi_A \times \pi_B$ is an interpretation of $A \times B$ in $A \times_C B$.*

Proof. By the previous lemma, the ideals $I = \ker \pi_A$ and $J = \ker \pi_B$ of $A \times_C B$ are f.g., and hence (existentially) definable in $A \times_C B$. □

Lemma 4.4. *Suppose A and B are interpretable in $\mathbb{Z}$ and C is f.g. Then $A \times_C B$ is interpretable in $\mathbb{Z}$.*

Proof. Let $f\colon \mathbb{Z} \rightsquigarrow A$ and $g\colon \mathbb{Z} \rightsquigarrow B$; then $f \times g$ is an interpretation $\mathbb{Z} \rightsquigarrow A \times B$. Both $\alpha \circ f$ and $\beta \circ g$ are interpretations $\mathbb{Z} \rightsquigarrow C$; so by Lemma 2.26 (and the assumption that C is f.g.), the set

$$[\alpha \circ f = \beta \circ g] = (f \times g)^{-1}(A \times_C B)$$

is definable in $\mathbb{Z}$. Hence the restriction of $f \times g$ to a map $(f \times g)^{-1}(A \times_C B) \to A \times_C B$ is an interpretation of $A \times_C B$ in $\mathbb{Z}$. □

4.2. **Fiber products over finite rings.** Every fiber product of noetherian rings over a finite ring is bi-interpretable with the direct product of those rings:

Lemma 4.5. *Let $\alpha\colon A \to C$ and $\beta\colon B \to C$ be surjective morphisms of noetherian rings, where C is finite. Then the pair (f, g), where f is the natural inclusion $A \times_C B \to A \times B$ and $g = \pi_A \times \pi_B$, is a bi-interpretation between $A \times B$ and $A \times_C B$.*

Proof. We first observe that the subset $M := A \times_C B$ of $A \times B$ is definable in the ring $A \times B$ (and hence that f is indeed an interpretation $A \times B \rightsquigarrow A \times_C B$). To see this first note that the map $\Pi_A\colon A \times B \to A \times 0$ given by $(a,b) \mapsto (a,0) = (a,b) \cdot (1,0)$ is definable in $A \times B$ (with the parameter $(1,0)$); similarly, the map $(a,b) \mapsto \Pi_B(a,b) = (0,b)\colon A \times B \to 0 \times B$ is definable in $A \times B$. Let $n = |C|$ and let $a_1, \dots, a_n \in A$ be representatives for the residue classes of $A/\ker\alpha$ and $b_1, \dots, b_n \in$

B be representatives for the residue classes of $B/\ker\beta$ such that $\alpha(a_i)=\beta_i(b_i)$ for $i=1,\dots,n$. Then M is seen to be definable as the set of all $(a,b)\in A\times B$ such that for each $i\in\{1,\dots,n\}$,

$$(a,b)\in(a_i,0)+\Pi_A^{-1}(\ker\alpha) \quad\Longleftrightarrow\quad (a,b)\in(0,b_i)+\Pi_B^{-1}(\ker\beta).$$

The self-interpretation $g\circ f$ of $A\times B$ is the map

$$\big((a,b),(a',b')\big)\mapsto \Pi_A(a,b)+\Pi_B(a',b')=(a,b')\colon M\times M\to A\times B$$

and hence definable in $A\times B$. Similarly, the self-interpretation $f\circ g$ of $A\times_C B$ is the map

$$\big((a,b),(a',b')\big)\mapsto (a,b')\colon g^{-1}(M)\to A\times_C B,$$

and since

$$(f\circ g)\big((a,b),(a',b')\big)=(a'',b'') \iff (a'',b'')\in\big((a,b)+\ker\pi_A\big)\cap\big((a',b')+\ker\pi_B\big),$$

we also see that $f\circ g\simeq \mathrm{id}_{A\times_C B}$. □

The previous lemma leads us to the study of the bi-interpretability class of the direct product of two f.g. rings. We first observe that a product of a ring B with a finite ring is (parametrically) bi-interpretable with B itself:

Lemma 4.6. *Let A be a direct product $A=B\times R$ of a ring B with a finite ring R. Then A and B are bi-interpretable.*

Proof. The surjective ring morphism $(b,r)\mapsto b\colon A\to B$ is an interpretation $f\colon A\rightsquigarrow B$ with $\ker f=A\cdot(0,1)$. (See Example 2.9, (2).) Pick a bijection $g\colon R'\to R$ where $R'\subseteq B^n$ for some $n>0$. Then the bijection

$$(b,r')\mapsto \big(b,g(r')\big)\colon B\times R'\to B\times R=A,$$

in the following also denoted by g, is an interpretation $B\rightsquigarrow A$ (since the addition and multiplication tables of the finite ring R are definable). Now $f\circ g\colon B\times R'\to B$ is given by $(b,r')\mapsto b$ and hence definable in B, and

$$g\circ f\colon A\times f^{-1}(R')=f^{-1}(B\times R')\to A$$

is given by

$$\big((b,r),(b_1,r_1),\dots,(b_m,r_m)\big)\mapsto \big(b,g(b_1,\dots,b_m)\big)$$

and thus definable in A, since $(b,r)\cdot(1,0)=(b,0)$ and $(b,r)\cdot(0,1)=(0,r)$ for all $b\in B$, $r\in R$. This shows that (f,g) is a bi-interpretation between A and B. □

On the other hand, the direct product of two infinite f.g. rings is never bi-interpretable with $\mathbb{Z}$:

Lemma 4.7. *Let A and B be infinite finitely generated rings. Then $A\times B$ is not bi-interpretable with $\mathbb{Z}$.*

Proof. Let $a\in A$ and $b\in B$ be elements of infinite multiplicative order. (See Corollary 1.4.) Suppose $A\times B$ is bi-interpretable with $\mathbb{Z}$. Then by Corollary 2.20, the set $(a,b)^{\mathbb{N}}$ of powers of (a,b) is definable in $A\times B$. By the Feferman-Vaught Theorem [11, Corollary 9.6.4] there are $N\in\mathbb{N}$ and formulas $\varphi_i(x)$, $\psi_i(y)$ ($i=1,\dots,N$), possibly with parameters, such that for all $(a',b')\in A\times B$, we have

$$(a',b')\in(a,b)^{\mathbb{N}} \quad\Longleftrightarrow\quad A\models\varphi_i(a') \text{ and } B\models\psi_i(b'), \text{ for some } i\in\{1,\dots,N\}.$$

By the pigeon hole principle, there are $m \neq n$ and some $i \in \{1, \dots, N\}$ such that $A \models \varphi_i(a^m) \wedge \varphi_i(a^n)$ and $B \models \psi_i(b^m) \wedge \psi_i(b^n)$. But then $A \models \varphi_i(a^m)$ and $B \models \psi_i(b^n)$, so $(a^m, b^n) \in (a, b)^{\mathbb{N}}$, a contradiction to $m \neq n$. □

Combining the results in this subsection immediately yields the following consequences:

Corollary 4.8. *The fiber product of a noetherian ring A with a finite ring is bi-interpretable with A.*

Corollary 4.9. *The fiber product of two infinite f.g. rings over a finite ring is* not *bi-interpretable with $\mathbb{Z}$.*

4.3. **Fiber products over infinite rings.** In this subsection we show:

Theorem 4.10. *Let $\alpha\colon A \to C$ and $\beta\colon B \to C$ be surjective ring morphisms. If A and B are both bi-interpretable with $\mathbb{Z}$, and C is f.g. and infinite, then $A \times_C B$ is also bi-interpretable with $\mathbb{Z}$.*

For the proof, which is based on the criterion for bi-interpretability with $\mathbb{Z}$ from Corollary 2.24, we need:

Lemma 4.11. *Let A be bi-interpretable with $\mathbb{Z}$, and $a \in A$ be of infinite multiplicative order. Then there exists a definable bijection $A \to a^{\mathbb{N}}$, and hence definable binary operations $\oplus$ and $\otimes$ on $a^{\mathbb{N}}$ making $a^{\mathbb{N}}$ into a ring isomorphic to $\mathbb{Z}$.*

Proof. Take an interpretation $f\colon \boldsymbol{A} \rightsquigarrow \mathbb{Z}$ and a definable bijective map $\iota\colon A \to f^*(\mathbb{Z})$. (See the beginning of Section 2.8.) Choose a definable bijection $f^*(\mathbb{Z}) \to f^*(\mathbb{N})$. By Corollary 2.22, the map $\overline{n} \mapsto a^n\colon f^*(\mathbb{N}) \to a^{\mathbb{N}}$ is definable. Thus the composition

$$A \xrightarrow{\iota} f^*(\mathbb{Z}) \to f^*(\mathbb{N}) \xrightarrow{\overline{n} \mapsto a^n} a^{\mathbb{N}}$$

is a definable bijection as required. The rest follows from Lemma 2.17. □

We also use the following number-theoretic fact:

Theorem 4.12 (Scott [40, Theorem 3])**.** *Let p, q be distinct prime numbers and $c \in \mathbb{Z}$. Then there is at most one pair (m, n) with $p^{2m} - q^{2n} = c$.*

We now show Theorem 4.10. Thus, assume that A and B are bi-interpretable with $\mathbb{Z}$, and C is f.g. and infinite. By Lemma 4.4, $R := A \times_C B$ is interpretable in $\mathbb{Z}$, so by Corollary 2.24, in order to see that R is bi-interpretable with $\mathbb{Z}$, it is enough to show that we can interpret $\mathbb{Z}$ in the ring R such that R can be mapped definably and injectively into the interpreted copy Z of $\mathbb{Z}$ in R.

To see this, let $a \in A$ and $b \in B$ so that $\alpha(a) = \beta(b)$ has infinite multiplicative order in C. Then $Z := (a, b)^{\mathbb{N}}$ is definable in R as

$$Z = \left\{ r \in R : \pi_A(r) \in a^{\mathbb{N}} \text{ and } \pi_B(r) \in b^{\mathbb{N}} \right\}.$$

(Clearly, Z is contained in the set on the right-hand side of this equation; conversely, if r is any element of this set, then $r = (a^m, b^n)$ for some m and n, with $\alpha(a^m) = \beta(b^n)$, and then $\alpha(a)^m = \alpha(a)^n$, as $\alpha(a) = \beta(b)$, forcing $m = n$ since $\alpha(a)$ has infinite multiplicative order.)

Recall from Corollary 4.3 that π_A is an interpretation $R \rightsquigarrow A$. We denote by $\overline{A} := \pi_A^*(A) = R/\ker \pi_A$ the copy of A in R interpreted via π_A, and by $x \mapsto \overline{x}\colon A \to \overline{A}$ the natural isomorphism; similarly with B in place of A. The natural surjection $R \to \overline{A}$

restricts to a bijection $Z = (a,b)^{\mathbb{N}} \to \overline{a}^{\mathbb{N}}$; we denote by e_A its inverse, and we define e_B similarly. Note that e_A and e_B are definable in R. By Lemma 4.11 there are binary operations on $\overline{a}^{\mathbb{N}}$, definable in $\overline{A}$, which make $\overline{a}^{\mathbb{N}}$ into a ring isomorphic to $(\mathbb{Z},+,\times)$. Equip Z with binary operations $\oplus$, $\otimes$ making e_A a ring isomorphism; then $\oplus$, $\otimes$ are definable in R, and $(Z,\oplus,\otimes) \cong (\mathbb{Z},+,\times)$.

It remains to specify a definable injective map $R \to Z$. Let $f_A \colon \overline{A} \to \overline{a}^{\mathbb{N}}$ and $f_B \colon \overline{B} \to \overline{b}^{\mathbb{N}}$ be definable bijections, according to Lemma 4.11, and let F_A and F_B be the composition of f_A, f_B with the natural surjection $R \to \overline{A}$ and $R \to \overline{B}$, respectively; then F_A, F_B are definable in R. From Corollary 2.22 and the fact that exponentiation is definable in $\mathbb{N}$, we see that the maps $t_A \colon \overline{a}^{\mathbb{N}} \to \overline{a}^{\mathbb{N}}$ and $t_B \colon \overline{b}^{\mathbb{N}} \to \overline{b}^{\mathbb{N}}$ given by $t_A(\overline{a}^m) = \overline{a}^{2^{2m}}$ and $t_B(\overline{b}^n) = \overline{b}^{3^{2n}}$ are definable. It is now easy to verify, using Theorem 4.12, that the definable map

$$r \mapsto (e_A \circ t_A \circ F_A)(r) \cdot (e_B \circ t_B \circ F_B)(r) \colon R \to Z$$

is injective. □

Remark. Below we apply Theorem 4.10 in a situation where we know a priori that the ring $A \times_C B$ is f.g. We do not know whether the fiber product of two f.g. rings is always again f.g.

4.4. **The graph of minimal non-maximal prime ideals.** Let A be a ring. We denote by $\operatorname{Min}(A)$ the set of minimal prime ideals of A; we always assume that $\operatorname{Min}(A)$ is finite. (This is the case if A is noetherian.) We define a (simple, undirected) graph $\mathcal{G}_A = (V,E)$ whose vertex set is the set $V = \operatorname{Min}(A) \setminus \operatorname{Max}(A)$ of all minimal non-maximal prime ideals of A, and whose edge relation is defined by

$$(\mathfrak{p},\mathfrak{q}) \in E \quad :\Longleftrightarrow \quad \text{there is a non-maximal prime ideal of } A \text{ containing } \mathfrak{p}+\mathfrak{q}.$$

Note that if A is f.g., then V is the set of minimal prime ideals of A of infinite index in A (so $V \neq \emptyset$ iff A is infinite), and $(\mathfrak{p},\mathfrak{q}) \in E$ iff $\mathfrak{p}+\mathfrak{q}$ is of infinite index in A. (See Corollary 1.3.)

We first relate connectedness of the graph $\mathcal{G}_A$ with connectedness of the topological space $\operatorname{Spec}^\circ(A) = \operatorname{Spec}(A) \setminus \operatorname{Max}(A)$ considered in the introduction.

Lemma 4.13. *Let $I_1,\dots,I_m,J_1,\dots,J_n$ be ideals of A, where $m,n \geq 1$, and $I = I_1 \cap \cdots \cap I_m$, $J = J_1 \cap \cdots \cap J_n$. Suppose that every prime ideal containing $I_i + J_j$ is maximal, for all $i = 1,\dots,m$ and $j = 1,\dots,n$. Then every prime ideal containing $I+J$ is maximal.*

Proof. Let $\mathfrak{p} \supseteq I+J$ be a prime ideal. If a prime ideal contains an intersection of finitely many ideals, then it contains one of them. Hence there are i and j such that $\mathfrak{p} \supseteq I_i + J_j$, and thus $\mathfrak{p}$ is maximal. □

Given an ideal I of A we let $V(I)$ be the closed subset of $\operatorname{Spec}(A)$ consisting of all $\mathfrak{p} \in \operatorname{Spec}(A)$ containing I.

Corollary 4.14. *$\mathcal{G}_A$ is connected iff* $\operatorname{Spec}^\circ(A)$ *is connected.*

Proof. Suppose first that $\operatorname{Spec}^\circ(A)$ is disconnected, that is, there are nonempty closed subsets X, X' partitioning $\operatorname{Spec}^\circ(A)$. Then both X and X' contain a non-maximal minimal prime ideal. Let C be the set of non-maximal minimal prime ideals contained in X, and $C' := V \setminus C$. For $\mathfrak{p} \in C$ and $\mathfrak{p}' \in C'$, we have

$$\operatorname{Spec}^\circ(A) \cap V(\mathfrak{p}+\mathfrak{p}') = \operatorname{Spec}^\circ(A) \cap V(\mathfrak{p}) \cap V(\mathfrak{p}') \subseteq X \cap X' = \emptyset$$

and thus $(\mathfrak{p}, \mathfrak{p}') \notin E$. Hence $\mathcal{G}_A$ is disconnected.

Conversely, suppose $\mathcal{G}_A$ is disconnected. Let C, C' be nonempty sets partitioning V such that $(\mathfrak{p}, \mathfrak{p}') \notin E$ for all $\mathfrak{p} \in C$, $\mathfrak{p}' \in C'$. Put $I := \bigcap C$, $I' := \bigcap C'$. Then $X := V(I) \cap \operatorname{Spec}^\circ(A)$, $X' := V(I') \cap \operatorname{Spec}^\circ(A)$ are nonempty closed subsets of $\operatorname{Spec}^\circ(A)$ with $X \cup X' = \operatorname{Spec}^\circ(A)$, and by the previous lemma we have $X \cap X' = \emptyset$. Thus $\operatorname{Spec}^\circ(A)$ is disconnected. $\square$

Remark. In the case where A is a local ring, the graph $\mathcal{G}_A$ has been considered in different contexts. (See, e.g., [10, Definition 3.4] or [42, Remark 2.3].)

The following lemma allows us to analyze the graph $\mathcal{G}_A$ by splitting off a single vertex:

Lemma 4.15. *Let* $\mathfrak{p}_0 \in \operatorname{Min}(A)$,

$$I_0 := \bigcap \{\mathfrak{p} \in \operatorname{Min}(A) : \mathfrak{p} \neq \mathfrak{p}_0\},$$

and $A_0 := A/I_0$, *with natural surjection* $a \mapsto \overline{a} = a + I_0 \colon A \to A_0$. *Then*

$$\mathfrak{p} \mapsto \overline{\mathfrak{p}} \colon \operatorname{Min}(A) \setminus \{\mathfrak{p}_0\} \to \operatorname{Min}(A_0)$$

is a bijection. Moreover, for $\mathfrak{p}, \mathfrak{q} \in \operatorname{Min}(A) \setminus \{\mathfrak{p}_0\}$ *the natural surjection* $A \to A_0$ *induces an isomorphism* $A/(\mathfrak{p} + \mathfrak{q}) \to A_0/(\overline{\mathfrak{p}} + \overline{\mathfrak{q}})$.

Proof. The map $\mathfrak{p} \mapsto \overline{\mathfrak{p}}$ is an inclusion-preserving correspondence between the set $V(I_0)$ of prime ideals of A containing I_0 and the set of all prime ideals of A_0. Clearly $\operatorname{Min}(A) \setminus \{\mathfrak{p}_0\} \subseteq V(I_0)$, and if $\mathfrak{p} \supseteq I_0$ is a minimal prime ideal of A, then $\overline{\mathfrak{p}}$ is a minimal prime ideal of A_0. To show surjectivity, let $\overline{\mathfrak{q}}$ be a minimal prime ideal of A_0, where $\mathfrak{q} \in V(I_0)$. Then $\mathfrak{q} \supseteq \mathfrak{p} \supseteq I_0$ for some $\mathfrak{p} \in \operatorname{Min}(A)$ with $\mathfrak{p} \neq \mathfrak{p}_0$, and so $\mathfrak{q} = \mathfrak{p}$ by minimality of $\overline{\mathfrak{q}}$. The rest of the lemma is easy to see. $\square$

Given a graph $\mathcal{G} = (V, E)$ and a vertex $v \in V$, we denote by $\mathcal{G} \setminus v$ the graph obtained from $\mathcal{G}$ by removing v, i.e., the graph with vertex set $W = V \setminus \{v\}$ and edge set $E \cap (W \times W)$. If $\mathfrak{p}_0$ is a minimal non-maximal prime of A and I_0 and A_0 are as in Lemma 4.15, then $\mathfrak{p} \mapsto \overline{\mathfrak{p}}$ is an isomorphism $\mathcal{G}_A \setminus \mathfrak{p}_0 \to \mathcal{G}_{A_0}$.

We now return to bi-interpretability issues:

Lemma 4.16. *Suppose A is infinite and f.g. Let $C \subseteq V$, $C \neq \emptyset$, such that the induced subgraph $\mathcal{G}_A \restriction C$ of $\mathcal{G}_A$ with vertex set C is connected, and let $I = \bigcap C$. Then A/I is bi-interpretable with $\mathbb{Z}$.*

Proof. We proceed by induction on the size of C. If $|C| = 1$, then I is a prime ideal of infinite index, and the claim holds by Theorem 3.1. So suppose $|C| > 1$. It is well-known that each non-trivial finite connected graph $\mathcal{G}$ contains a non-cut vertex, i.e., a vertex v such that $\mathcal{G} \setminus v$ is still connected. Thus, let $\mathfrak{p}_0$ be a non-cut vertex of $\mathcal{G}_A \restriction C$, and let $C_0 := C \setminus \{\mathfrak{p}_0\}$, $I_0 := \bigcap C_0$. Choosing $\mathfrak{p} \in C_0$ such that $(\mathfrak{p}, \mathfrak{p}_0) \in E$, we have $I_0 + \mathfrak{p}_0 \subseteq \mathfrak{p} + \mathfrak{p}_0$ and $A/(\mathfrak{p} + \mathfrak{p}_0)$ is infinite; hence $A/(I_0 + \mathfrak{p}_0)$ is infinite. By Example 4.1, the rings $A/I = A/(I_0 \cap \mathfrak{p}_0)$ and $(A/I_0) \times_{A/(I_0 + \mathfrak{p}_0)} (A/\mathfrak{p}_0)$ are naturally isomorphic, where A/I_0 and $A/\mathfrak{p}_0$ are both bi-interpretable with $\mathbb{Z}$, by inductive assumption and Theorem 3.1, respectively. Hence A/I is bi-interpretable with $\mathbb{Z}$ by Theorem 4.10. $\square$

For the next lemma note that the graphs $\mathcal{G}_A$ and $\mathcal{G}_{A_{\mathrm{red}}}$ are naturally isomorphic.

Lemma 4.17. *Let $\mathfrak{p}_0 \in \operatorname{Min}(A)$ be of finite index in A, and let I_0 and A_0 be as in Lemma 4.15. Then the reduced rings $A_{\mathrm{red}} = A/N(A)$ and A_0 are bi-interpretable, and the graphs $\mathcal{G}_A$ and $\mathcal{G}_{A_0}$ are naturally isomorphic.*

Proof. We may assume that $I_0 \not\subseteq \mathfrak{p}_0$ (since otherwise $I_0 = N(A)$ and so $A = A_0$). Then $A = I_0 + \mathfrak{p}_0$, since $\mathfrak{p}_0$ is a maximal ideal of A (every finite integral domain is a field). So the natural morphism $A \to A_0 \times R$, where $R = A/\mathfrak{p}_0$, is surjective (by the Chinese Remainder Theorem) with kernel $N(A) = \bigcap \operatorname{Min}(A) = I_0 \cap \mathfrak{p}_0$. The first claim now follows from Lemma 4.6. For the second claim note that the prime ideals of $A_0 \times R$ are the ideals of this ring having the form $\mathfrak{p} \times R$ where $\mathfrak{p} \in \operatorname{Spec}(A_0)$ or $A_0 \times \mathfrak{q}$ where $\mathfrak{q} \in \operatorname{Spec}(R)$, and the latter all have finite index. $\square$

4.5. **Characterizing the reduced rings which are bi-interpretable with $\mathbb{Z}$.** Combining the results obtained so far in this section, we obtain the following characterization of those finitely generated reduced rings which are (parametrically) bi-interpretable with $\mathbb{Z}$.

Theorem 4.18. *Let A be an infinite finitely generated reduced ring. Then A is bi-interpretable with $\mathbb{Z}$ if and only if the graph $\mathcal{G}_A$ is connected.*

Proof. After applying lemmata 4.15 and 4.17 sufficiently often, we can reduce to the situation that no minimal prime of A is maximal, i.e., the vertex set of the graph $\mathcal{G}_A$ equals $\operatorname{Min}(A)$. In this case, if $\mathcal{G}_A$ is connected, then by Lemma 4.16, the ring A is bi-interpretable with $\mathbb{Z}$. Conversely, suppose that $\mathcal{G}_A$ is not connected. Let $C \subseteq V$ be a connected component of the graph $\mathcal{G}_A = (V, E)$. Then for each $\mathfrak{p} \in C$ and $\mathfrak{q} \in V \setminus C$ we have $(\mathfrak{p}, \mathfrak{q}) \notin E$, i.e., $\mathfrak{p} + \mathfrak{q}$ has finite index in A. Thus by Corollary 1.3 and Lemma 4.13, setting $I := \bigcap C$, $J := \bigcap (V \setminus C)$, the ideal $I + J$ has finite index in A. Since $I \cap J = N(A) = 0$, by Example 4.1, the rings A and $(A/I) \times_{A/(I+J)} (A/J)$ are naturally isomorphic, and by Lemma 4.16, both A/I and A/J are infinite. Hence by Corollary 4.9, A is not bi-interpretable with $\mathbb{Z}$. $\square$

5. Finite Nilpotent Extensions

Throughout this section we let B be a ring with nilradical N. Our main goal for this section is the proof of the following theorem:

Theorem 5.1. *Suppose B is f.g. and $\operatorname{ann}_{\mathbb{Z}}(N) \neq 0$. Then the rings $B_{\mathrm{red}} = B/N$ and B are bi-interpretable.*

In particular, if B is f.g. and has positive characteristic, then B_{red} and B are bi-interpretable. Our bi-interpretation between B_{red} and B passes through a truncation of Cartier's ring of big Witt vectors over B_{red}; therefore we first briefly review this construction. (See [4, IX, §1] or [8, §17] for missing proofs of the statements in the next subsection.)

5.1. **Witt vectors.** In the rest of this section we let $d, i, j \geq 1$ be integers. Let $X_1, X_2, \ldots$ be countably many pairwise distinct indeterminates, and for each j set $X_{|j} := (X_i)_{i|j}$. The j-th *Witt polynomials* $w_j \in \mathbb{Z}[X_{|j}]$ are defined by

$$w_j := \sum_{i|j} i X_i^{j/i}.$$

Let now $Y_1, Y_2, \dots$ be another sequence of pairwise distinct indeterminates. Then for any polynomial $P \in \mathbb{Z}[X,Y]$ in distinct indeterminates X, Y there is a sequence (P_i) of polynomials $P_i \in \mathbb{Z}[X_{|i}, Y_{|i}]$ such that

$$P\big(w_i(X_{|i}), w_i(Y_{|i})\big) = w_i\big(P_1(X_1,Y_1), \dots, P_i(X_{|i}, Y_{|i})\big) \quad \text{for all } i.$$

In particular, there are sequences (S_i) and (M_i) of polynomials $S_i \in \mathbb{Z}[X_{|i}, Y_{|i}]$ and $M_i \in \mathbb{Z}[X_{|i}, Y_{|i}]$ such that

$$\begin{aligned} w_i(X_{|i}) + w_i(Y_{|i}) &= w_i\big(S_1(X_1,Y_1), \dots, S_i(X_{|i}, Y_{|i})\big), \\ w_i(X_{|i}) \cdot w_i(Y_{|i}) &= w_i\big(M_1(X_1,Y_1), \dots, M_i(X_{|i}, Y_{|i})\big) \end{aligned}$$

for all i. For example, $S_1 = X_1 + Y_1$, $M_1 = X_1 \cdot Y_1$, and if p is a prime, then

$$S_p = X_p + Y_p - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} X_1^i Y_1^{p-i}, \qquad M_p = X_1^p Y_p + X_p Y_1^p + p X_p Y_p.$$

Let A be a ring. We let $A^{|d}$ be the set of sequences $a = (a_i)$ indexed by all $i|d$, and for $a = (a_i) \in A^{|d}$ and $j|d$ let $a_{|j} := (a_i)_{i|j} \in A^{|j}$. We define binary operations $+$ and $\cdot$ on $A^{|d}$ by

$$\begin{aligned} a + b &:= \big(S_1(a_1,b_1), \dots, S_j(a_{|j}, b_{|j}), \dots\big), \\ a \cdot b &:= \big(M_1(a_1,b_1), \dots, M_j(a_{|j}, b_{|j}), \dots\big) \end{aligned}$$

for $a = (a_i), b = (b_i) \in A^{|d}$. Equipped with these operations, $A^{|d}$ becomes a ring (with 0 and 1 given by $(0,0,0,\dots)$ and $(1,0,0,\dots)$ respectively), which we call the d-th *ring of Witt vectors* over A, denoted by $W_d(A)$. Every ring morphism $f\colon A \to B$ induces a componentwise map $A^{|d} \to B^{|d}$, and this map is a ring morphism $W_d(f)\colon W_d(A) \to W_d(B)$. Thus W_d is a functor from the category of rings to itself. The polynomials w_j define (functorial) ring morphisms

$$a \mapsto w_j(a_{|j})\colon W_d(A) \to A,$$

and hence give rise to a ring morphism

$$a \mapsto w_*(a) := \big(w_j(a_{|j})\big)\colon W_d \to A^{|d},$$

where $A^{|d}$ carries the product ring structure. If no $i|d$ is a zero-divisor in A, then w_* is injective, and if all $i|d$ are units in A, then w_* is bijective. Note that the underlying set of $W_d(A) = A^{|d}$ is simply a finite-fold power of A, and $A^{|d}$ is integral over the image of $W_d(A)$ under w_*. Moreover:

Lemma 5.2. *If A is f.g, then so is $W_d(A)$.*

Proof. Using that A is the image of a polynomial ring over $\mathbb{Z}$, we first reduce to the case that $\operatorname{char}(A) = 0$, so w_* is injective. Since $A^{|d}$ is integral over $B := w_*\big(W_d(A)\big)$, if the ring A is f.g., then so is B, by the Artin-Tate Lemma 1.8, and hence so is $W_d(A)$. □

Note also that the identity map $A^{|d} \to W_d(A)$ furnishes us with an interpretation $A \rightsquigarrow W_d(A)$ of the ring $W_d(A)$ in the ring A.

5.2. **A bi-interpretation between B and B_{red}.** Let I be an ideal of B with $I^2 = 0$ and $d \geq 1$ an integer such that $dI = 0$. Put $A := B/I$. The residue morphism $B \to A$ induces a surjective ring morphism $r\colon W_d(B) \to W_d(A)$, and we also have a ring morphism

$$b = (b_i) \mapsto w(b) := w_d(b) = \sum_{i|d} i b_i^{d/i} \colon W_d(B) \to B.$$

The morphism w descends to $W_d(A)$:

Lemma 5.3. *There is a unique ring morphism $t\colon W_d(A) \to B$ such that $w = t \circ r$.*

Proof. Let $b = (b_i)$ and $b' = (b'_i)$ be elements of $W_d(B)$ such that $r(b) = r(b')$, that is, $x_i := b'_i - b_i \in I$ for each $i|d$. Then for $i|d$ we have

$$i(b'_i)^{d/i} = i b_i^{d/i} + i(d/i) b_i^{d/i-1} x_i + \text{multiples of } x_i^2,$$

and since $x_i^2 = 0$ and $i(d/i)x_i = dx_i = 0$, we obtain $i(b'_i)^{d/i} = i b_i^{d/i}$. This yields $w_d(b) = w_d(b')$. So given $a \in W_d(A)$ we can set $t(a) := w_d(b)$ where b is any element of $W_d(B)$ with $r(b) = a$. One verifies easily that then $t\colon W_d(A) \to B$ has the required property. The uniqueness part is clear. □

In the following we view B as a $W_d(A)$-module via the morphism t from the previous lemma.

Lemma 5.4. *Suppose B is f.g. Then the $W_d(A)$-module B is f.g.*

Proof. First note that the image W of $W_d(A)$ under t contains all d-th powers of elements of B. Hence B is integral over its subring W: each $b \in B$ is a zero of the monic polynomial $X^d - b^d$ with coefficients in W. Since B is a f.g. W-algebra, this implies that B is a f.g. $W_d(A)$-module [3, Corollary 5.2]. □

In the rest of this subsection we assume that B is f.g. Let $b_1, \dots, b_m$ be generators for the $W_d(A)$-module B, and consider the surjective $W_d(A)$-bilinear map

$$(a_1, \dots, a_m) \mapsto \sum_{j=1}^{m} a_j b_j \colon W_d(A)^m \to B. \tag{2}$$

By Lemma 5.2, the ring $W_d(A)$ is f.g., hence noetherian, so the kernel of (2) is f.g. Using $W_d(A)$-bilinearity, the preimage of the graph of multiplication in B under the map (2) is definable in $W_d(A)$. Hence the map (2) is an interpretation of B in $W_d(A)$. Composing this interpretation $W_d(A) \rightsquigarrow B$ with the interpretation $A \rightsquigarrow W_d(A)$ from the previous subsection, we obtain an interpretation $f\colon A \rightsquigarrow B$. Since the ideal I is f.g., the residue morphism $b \mapsto \overline{b}\colon B \to A = B/I$ is an interpretation $g\colon B \rightsquigarrow A$. With these notations, we have:

Lemma 5.5. *The pair (f, g) is a bi-interpretation between A and B.*

Proof. The self-interpretation $f \circ g$ of B is the map $(B^{\lfloor d})^m \to B$ given by

$$(\beta_1, \dots, \beta_m) \mapsto \sum_{j=1}^{m} w_d(\beta_j) b_j$$

and hence definable in B. One also checks easily that the self-interpretation $g \circ f$ of A is the map $(A^{|d})^m \to A$ given by

$$(\alpha_1, \dots, \alpha_m) \mapsto \sum_{j=1}^{m} w_d(\alpha_j)\overline{b_j},$$

hence definable in A. $\square$

We can now prove the main result of this section:

Proof of Theorem 5.1. Since $\operatorname{ann}_{\mathbb{Z}}(N) \neq 0$, we can take some $d \geq 1$ with $dN = 0$. Since B is f.g. and hence noetherian, we can take some $e \in \mathbb{N}$ with $N^{2^e} = 0$. We proceed by induction on e to show that B and $B_{\mathrm{red}} = B/N$ are bi-interpretable. If $e = 0$ then $N = 0$, and there is nothing to show, so suppose $e \geq 1$. By the above applied to the ideal $I := N^{2^{e-1}}$ of B (so $I^2 = 0$), the f.g. rings $A := B/I$ and B are bi-interpretable. Now the nilradical of A is $N(A) = N + I$, so $dN(A) = 0$ and $N(A)^{2^{e-1}} = 0$. Hence by inductive hypothesis applied to A in place of B, the rings $A_{\mathrm{red}} = A/N(A)$ and A are bi-interpretable. Since A_{red} and B_{red} are isomorphic and the relation of bi-interpretability is transitive, this implies that B_{red} and B are bi-interpretable. $\square$

6. Derivations on Nonstandard Models

In this section we shall construct derivations on nonstandard models of finitely generated rings. Our appeal to ultralimits is not strictly speaking necessary as a simple compactness argument would suffice, but the systematic use of ultralimits permits us to avoid some syntactical considerations.

6.1. **Ultralimits.** Let us recall some of the basic formalism of ultralimits. Let I be a nonempty index set, $\mathcal{U}$ be an ultrafilter on I, and $\boldsymbol{M} = (M, \dots)$ be a structure (in some first-order language). We denote by $\boldsymbol{M}^{\mathcal{U}}$ the ultrapower $\boldsymbol{M}^I/\mathcal{U}$ of $\boldsymbol{M}$ relative to $\mathcal{U}$ and by $\Delta_{\boldsymbol{M}}$ the diagonal embedding of $\boldsymbol{M}$ into $\boldsymbol{M}^{\mathcal{U}}$, that is, that is, the embedding $\boldsymbol{M} \to \boldsymbol{M}^{\mathcal{U}}$ induced by the map $M \to M^I$ which associates to an element a of M the constant function $I \to M$ with value a. We define the ordinal-indexed directed system of ultralimits $\operatorname{Ult}_{\mathcal{U}}(\boldsymbol{M}, \alpha)$ by

(1) $\operatorname{Ult}_{\mathcal{U}}(\boldsymbol{M}, 0) := \boldsymbol{M}$,
(2) $\operatorname{Ult}_{\mathcal{U}}(\boldsymbol{M}, \alpha+1) := \big(\operatorname{Ult}_{\mathcal{U}}(\boldsymbol{M}, \alpha)\big)^{\mathcal{U}}$, and
(3) $\operatorname{Ult}_{\mathcal{U}}(\boldsymbol{M}, \lambda) := \varinjlim_{\alpha<\lambda} \operatorname{Ult}_{\mathcal{U}}(\boldsymbol{M}, \alpha)$ for a limit ordinal λ.

For us, in (3) only the case of $\lambda = \omega$ is relevant. By way of notation, if I and $\mathcal{U}$ are understood, then by an ultralimit we mean $\operatorname{Ult}_{\mathcal{U}}(\boldsymbol{M}, \omega)$ and we shall write

$${}^*\boldsymbol{M} := \operatorname{Ult}_{\mathcal{U}}(\boldsymbol{M}, \omega).$$

By definition of the direct limit, the structure ${}^*\boldsymbol{M}$ comes with a family of embeddings $\operatorname{Ult}_{\mathcal{U}}(\boldsymbol{M}, n) \to {}^*\boldsymbol{M}$ which commute with the diagonal embeddings

$$\Delta_{\operatorname{Ult}(\boldsymbol{M},n)} \colon \operatorname{Ult}_{\mathcal{U}}(\boldsymbol{M}, n) \to \operatorname{Ult}_{\mathcal{U}}(\boldsymbol{M}, n+1).$$

We identify $\boldsymbol{M}$ with its image in ${}^*\boldsymbol{M}$ under the embedding

$$\boldsymbol{M} = \operatorname{Ult}_{\mathcal{U}}(\boldsymbol{M}, 0) \to {}^*\boldsymbol{M}.$$

For fixed $\mathcal{U}$, the ultralimit construction commutes with taking reducts, and is functorial on the category of sets. Given a set N and a map $f \colon M \to N$, we write

${}^*f\colon {}^*M \to {}^*N$ for the ultralimit of f. In particular, if $\boldsymbol{N}$ is a substructure of $\boldsymbol{M}$, then the ultralimit of the natural inclusion $N \to M$ is an embedding ${}^*\boldsymbol{N} \to {}^*\boldsymbol{M}$ (compatible with the inclusions of $\boldsymbol{N}$ and $\boldsymbol{M}$ into their respective ultralimits), by which we identify ${}^*\boldsymbol{N}$ with a substructure of ${}^*\boldsymbol{M}$. From the universal property of the direct limit, we have the curious and useful fact that ${}^*\mathrm{Ult}_{\mathcal{U}}(\boldsymbol{M},1) = {}^*\boldsymbol{M}$ where by equality we mean canonical isomorphism.

6.2. **Constructing derivations on elementary extensions.** With the next two lemmata we show that every non-principal ultrapower of an integral domain of characteristic zero admits an ultralimit carrying a derivation which is nontrivial on the ultralimit of the non-standard integers. We let R be an integral domain of characteristic zero and $k \subseteq R$ be a subring.

Lemma 6.1. *Suppose R is a f.g. k-algebra, and let $t \in R$ be transcendental over k. Then there is a k-derivation $\partial\colon R \to R$ with $\partial(t) \neq 0$.*

Proof. Present R as $R = k[t_1,\dots,t_n]$ where $t_1 = t$. Since t is transcendental over k, there is a k-derivation $D\colon K \to K$ on the field of fractions K of R satisfying $D(t) = 1$. (See, e.g., [15, Proposition VIII.5.2].) Write $D(t_i) = a_i/b_i$ where $a_i \in R$ and $b_i \in R$, $b_i \neq 0$. Let ∂ be the restriction of $\left(\prod_{i=1}^n b_i\right) D$ to R, a k-derivation on R possibly taking values in K. Since R is an integral domain, $\partial(t) = \prod_i b_i \neq 0$, and visibly $\partial(t_i) = a_i \prod_{j\neq i} b_j \in R$ for each $i = 1,\dots,n$. Hence, for any $f \in R$, writing $f = F(t_1,\dots,t_n)$ for some polynomial F over k, we see that $\partial(f) = \sum_{i=1}^n \frac{\partial F}{\partial X_i}(t_1,\dots,t_n)\partial(t_i) \in R$. ☐

Taking an ultralimit of the above derivations, we find interesting derivations on ultralimits.

Lemma 6.2. *Let $t \in R$ be transcendental over k. Then there is an ultralimit ${}^*R$ of R and a k-derivation $\partial\colon {}^*R \to {}^*R$ with $\partial(t) \neq 0$.*

Proof. Let I be the set of finite subsets of R. For $S \in I$, let

$$(S) := \{S' \in I : S \subseteq S'\},$$

and let $\mathcal{C} := \big\{(S) : S \in I\big\}$. Observe that $\mathcal{C}$ has the finite intersection property: $(S_1) \cap (S_2) = (S_1 \cup S_2)$ for all $S_1, S_2 \in I$. Hence $\mathcal{C}$ extends to an ultrafilter $\mathcal{U}$ on I.

For each $S \in I$, by Lemma 6.1 we may find a k-derivation $\partial_S\colon k[t,S] \to k[t,S]$ with $\partial_S(t) \neq 0$, and these k-derivations combine to a k-derivation $\prod_{S\in I} \partial_S$ on the k-subalgebra $\prod_{S\in I} k[t,S]$ of R^I, which in turn induces a k-derivation ∂_{fin} with $\partial_{\mathrm{fin}}(t) \neq 0$ on the image R_{fin} of this subalgebra under the natural surjection $R^I \to R^I/\mathcal{U} = \mathrm{Ult}_{\mathcal{U}}(R,1)$. By definition of $\mathcal{C}$, the image of Δ_R is contained in R_{fin}. Thus

$$D := \partial_{\mathrm{fin}} \circ \Delta_R\colon R \to \mathrm{Ult}_{\mathcal{U}}(R,1)$$

is a k-derivation and $D(t) \neq 0$. Then

$$\partial := {}^*D\colon {}^*R \to {}^*\mathrm{Ult}_{\mathcal{U}}(R,1) = {}^*R$$

is our desired derivation. ☐

We specialize the above result to obtain our derivation which is nontrivial on the non-standard integers. Below we fix an arbitrary non-principal ultrafilter $\widetilde{\mathcal{U}}$ (on some unspecified index set), and given a ring A we write $\widetilde{A} = A^{\widetilde{\mathcal{U}}}$.

Corollary 6.3. *There is a k-derivation ∂ on an ultralimit ${}^*\widetilde{R}$ of $\widetilde{R}$ such that $\partial(t) \neq 0$ for some $t \in \widetilde{\mathbb{Z}}$.*

Proof. Let $t \in \widetilde{\mathbb{Z}} \setminus \mathbb{Z}$ be an arbitrary new element of $\widetilde{\mathbb{Z}}$. Then t is transcendental over k, and the previous lemma applies to $\widetilde{R}$ in place of R. □

Combining the previous corollary with Lemma 1.10, we conclude that noetherian rings having torsion-free nilpotent elements have elementary extensions with an automorphism moving the nonstandard integers.

Lemma 6.4. *Let A be a noetherian ring with nilradical $N = N(A)$, and suppose that $\operatorname{ann}_{\mathbb{Z}}(N) = 0$. Then there is an ultralimit ${}^*\widetilde{A}$ of $\widetilde{A}$ and an automorphism σ of ${}^*\widetilde{A}$ over A for which $\sigma({}^*\widetilde{\mathbb{Z}}) \nsubseteq {}^*\widetilde{\mathbb{Z}}$.*

Proof. Let ϵ be an element of N with $\operatorname{ann}_A(\epsilon) =: \mathfrak{q}$ prime and $\operatorname{ann}_{\mathbb{Z}}(\epsilon) = 0$, given by Lemma 1.10. Let $\pi \colon A \to A/\mathfrak{q} =: R$ be the natural quotient map. By Corollary 6.3, we can find a limit ultrapower ${}^*\widetilde{R}$ of $\widetilde{R}$ and an R-derivation $\partial \colon {}^*\widetilde{R} \to {}^*\widetilde{R}$ which is nontrivial on ${}^*\widetilde{\mathbb{Z}}$. Note that $A\epsilon$ is an R-module in a natural way, and so ${}^*\widetilde{A}\epsilon$ is an ${}^*\widetilde{R}$-module. We thus may define a map $\sigma \colon {}^*\widetilde{A} \to {}^*\widetilde{A}$ by $x \mapsto x + \partial({}^*\pi(x))\epsilon$; one checks easily that σ is an automorphism over A. We have $A\varepsilon \cap \mathbb{Z} = 0$ and $\operatorname{ann}_R(\epsilon) = 0$, hence ${}^*\widetilde{A}\varepsilon \cap {}^*\widetilde{\mathbb{Z}} = 0$ and $\operatorname{ann}_{{}^*\widetilde{R}}(\epsilon) = 0$. Since ∂ is nontrivial on ${}^*\widetilde{\mathbb{Z}}$, it follows that $\sigma({}^*\widetilde{\mathbb{Z}}) \nsubseteq {}^*\widetilde{\mathbb{Z}}$. □

We conclude that rings as in the previous lemma are not bi-interpretable with $\mathbb{Z}$.

Corollary 6.5. *No noetherian ring with nilradical N for which $\operatorname{ann}_{\mathbb{Z}}(N) = 0$ is bi-interpretable with $\mathbb{Z}$.*

Proof. Combine Lemma 6.4 and Corollary 2.19. □

We finish this subsection by remarking that although it may not be obvious from the outset, a non-trivial derivation on a proper elementary extension of $\widetilde{R}$ as constructed in Corollary 6.3 has some unexpected properties (not exploited in the present paper):

Lemma 6.6. *Let $Z \succeq \mathbb{Z}$ and $\partial \colon Z \to Z$ be a derivation. Then $\partial(Z) \subseteq \bigcap_{n \geq 1} nZ$.*

Proof. Let $a \in Z$ and $n \geq 1$; we need to show that $\partial(a)$ is divisible by n, and for this we may assume that $a \geq 0$. By the Hilbert-Waring Theorem we may write $a = \sum_{i=1}^{g} b_i^n$ for some $b_i \in Z$ (where $g = g(n)$ only depends on n), and differentiating both sides of this equation yields $\partial(a) = n \sum_{i=1}^{g} b_i^{n-1} \partial(b_i)$. □

6.3. **Finishing the proof of the main theorem.** We now complete the proof of the main theorem stated in the introduction, along the lines of the argument sketched there: Let A be a f.g. ring, $N = N(A)$. Suppose $\operatorname{ann}_{\mathbb{Z}}(N) \neq 0$. Then by Theorem 5.1 (applied to A in place of B), the rings A and A_{red} are bi-interpretable, and by Theorem 4.18, the reduced ring A_{red} is bi-interpretable with $\mathbb{N}$ if and only if A_{red} is infinite and $\operatorname{Spec}^\circ(A_{\text{red}})$ is connected. The latter is equivalent to A being infinite and $\operatorname{Spec}^\circ(A)$ being connected. If $\operatorname{ann}_{\mathbb{Z}}(N) = 0$, then A is not bi-interpretable with $\mathbb{Z}$, by Corollary 6.5. □

7. Quasi-Finite Axiomatizability

In this section we show the corollary stated in the introduction, in a slightly more precise form:

Proposition 7.1. *Every f.g. ring has a QFA formula.*

Throughout this section we let A, B be f.g. rings.

Lemma 7.2. *Suppose there is a QFA formula for A, and let M be a f.g. A-module. Then there is a QFA formula for the A-module M viewed as a two-sorted structure.*

Proof. Let $\varphi_A(x)$ be a QFA formula for A, where $x = (x_1, \dots, x_m)$. So we can take generators $a_1, \dots, a_m$ of A such that for each f.g. ring A' and $a'_1, \dots, a'_m \in A'$, we have $A' \models \varphi_A(a'_1, \dots, a'_m)$ iff there is an isomorphism $A \to A'$ with $a_i \mapsto a'_i$ for $i = 1, \dots, m$. (Note that there is at most one such isomorphism $A \to A'$.) Let also $b_1, \dots, b_n$ be generators for M. Since A is noetherian, the syzygies of these generators are f.g., that is, there are a_{jk} ($j = 1, \dots, n$, $k = 1, \dots, p$) of A such that for all $\alpha_1, \dots, \alpha_n \in A$ we have

$$\sum_{j=1}^{n} \alpha_j b_j = 0 \quad \Longleftrightarrow$$

$$\text{there are } \beta_1, \dots, \beta_p \in A \text{ such that } \alpha_j = \sum_{k=1}^{p} \beta_k a_{jk} \text{ for all } j = 1, \dots, n.$$

For $j = 1, \dots, n$, $k = 1, \dots, p$ pick polynomials $P_{jk} \in \mathbb{Z}[x]$ such that $a_{jk} = P_{jk}(a)$, where $a = (a_1, \dots, a_m)$. Let $y = (y_1, \dots, y_n)$ be a tuple of distinct variables of the module sort, u be another variable of the module sort, and $u_1, \dots, u_p, z_1, \dots, z_n$ be distinct new variables of the ring sort. Let $\gamma(y)$ be the formula

$$\forall u \exists z_1 \cdots \exists z_n \left(u = \sum_{i=1}^{n} z_i y_i \right)$$

and $\zeta(x, y)$ be the formula

$$\forall z_1 \cdots \forall z_n \left(\sum_{j=1}^{n} z_n y_n = 0 \longleftrightarrow \exists u_1 \cdots \exists u_p \left(\bigwedge_{j=1}^{n} z_j = \sum_{k=1}^{p} u_k P_{jk}(x) \right) \right).$$

Finally, let α be a sentence expressing that A is a ring and M is an A-module. One verifies easily that

$$\varphi_M(x, y) := \alpha \wedge \varphi_A(x) \wedge \gamma(y) \wedge \zeta(x, y)$$

is a QFA formula for the two-sorted structure (A, M). $\square$

Lemma 7.3. *Let $a_1, \dots, a_n$ be generators for A. There is a formula $\mu(x_1, \dots, x_n)$ such that for all rings A' and $a'_1, \dots, a'_n \in A'$, we have: $A' \models \mu(x_1, \dots, x_n)$ iff there is a morphism $A \to A'$ with $a_i \mapsto a'_i$ for $i = 1, \dots, n$.*

Proof. Let $x = (x_1, \dots, x_n)$ and $\pi \colon \mathbb{Z}[x] \to A$ be the (surjective) ring morphism satisfying $\pi(x_i) = a_i$ for $i = 1, \dots, n$. Let $P_1, \dots, P_m \in \mathbb{Z}[x]$ generate the kernel of π and let $\mu(x)$ be the formula $P_1(x) = \cdots = P_m(x) = 0$. $\square$

Lemma 7.4. *Let I, J be ideals of B such that $IJ = 0$. If there are QFA formulas for B/I and for B/J, then there is one for B.*

Proof. Let $\varphi_I(x)$ be a QFA formula for $A = B/I$, where $x = (x_1, \dots, x_m)$, and take a system $a = (a_1, \dots, a_m)$ of generators of A such that for each f.g. ring A' and $a' = (a'_1, \dots, a'_m) \in (A')^m$, we have $A' \models \varphi_I(a')$ iff there is an isomorphism $A \to A'$ with $a \mapsto a'$. Take generators $b_1, \dots, b_m, f_1, \dots, f_p$ for the ring B such that $a_i = b_i + I$ for $i = 1, \dots, m$ and $I = (f_1, \dots, f_p)$. Put $b = (b_1, \dots, b_m)$, $f = (f_1, \dots, f_p)$. From our QFA formula $\varphi_I(x)$ for A we easily construct a formula $\psi_I(x, u)$ (where $u = (u_1, \dots, u_p)$) such that for each f.g. ring B' and $b' = (b'_1, \dots, b'_m) \in (B')^m$, $f' = (f'_1, \dots, f'_p) \in (B')^p$, the following are equivalent, with $I' := (f'_1, \dots, f'_p) \subseteq B'$:

(1) $B' \models \psi_I(b', f')$;
(2) there is an isomorphism $A \to B'/I'$ with $a \mapsto b' + (I')^m$.

(See Example 2.9, (2).) By the preceding lemma, there is also a QFA formula for the two-sorted structure $(B/J, I)$. Hence as before, we can take generators $c_1, \dots, c_n, g_1, \dots, g_q$ of B such that the cosets $c_1 + J, \dots, c_n + J$ generate the ring B/J and $g_1, \dots, g_q$ generate the ideal J, as well as a formula $\psi_J(y, u, v)$, where $y = (y_1, \dots, y_n)$, $v = (v_1, \dots, v_q)$, such that for each f.g. ring B' and tuples $c' = (c'_1, \dots, c'_n)$, $f' = (f'_1, \dots, f'_p)$, and $g' = (g'_1, \dots, g'_q)$ of elements of B', the following statements are equivalent, with $J' := (g'_1, \dots, g'_q) \subseteq B'$:

(3) $B' \models \psi_J(c', f', g')$;
(4) there is an isomorphism $(B/J, I) \to (B'/J', I')$ with $c + J^n \mapsto c' + (J')^n$ and $f \mapsto f'$.

Now by Lemma 7.3 let $\mu(x, y, u, v)$ be a formula such that for each f.g. ring B' and tuples $b' = (b'_1, \dots, b'_m)$, $c' = (c'_1, \dots, c'_n)$, $f' = (f'_1, \dots, f'_p)$, $g' = (g'_1, \dots, g'_q)$ of elements of B', the following are equivalent:

(5) $B' \models \mu(b', c', f', g')$;
(6) there is a morphism $B \to B'$ with $b \mapsto b'$, $c \mapsto c'$, $f \mapsto f'$, and $g \mapsto g'$.

Then by Lemma 1.11 and the equivalences of (1), (3), (5) with (2), (4), (6), respectively, the formula $\psi_I(x, u) \wedge \psi_J(y, u, v) \wedge \mu(x, y, u, v)$ is QFA for B with respect to the system of generators b, c, f, g of B. $\square$

Corollary 7.5. *Let $N_1, \dots, N_e$ $(e \geq 1)$ be ideals of B such that $N_1 \cdots N_e = 0$. Suppose that for $k = 1, \dots, e$, there is a QFA formula for the f.g. ring B/N_k. Then there is a QFA formula for B.*

Proof. We proceed by induction on e. The case $e = 1$ being trivial, suppose that $e \geq 2$ and put $I := N_1 \cdots N_{e-1}$, $J := N_e$, so $IJ = 0$. By assumption, there is a QFA formula for $B/J = B/N_e$. Consider the f.g. ring $\overline{B} := B/I$ and the ideals $\overline{N_k} := N_k + I$ $(k = 1, \dots, e-1)$ of $\overline{B}$. We have $\overline{N_1} \cdots \overline{N_{e-1}} = 0$, and the residue map $B \to \overline{B}$ induces an isomorphism $B/N_k \to \overline{B}/\overline{N_k}$. Hence by the inductive hypothesis applied to $\overline{B}$ and $\overline{N_1}, \dots, \overline{N_{e-1}}$, there is a QFA formula for $\overline{B} = B/J$. Now by the proposition above, there is a QFA formula for B. $\square$

We can now prove Proposition 7.1. First, applying the previous corollary to $N_1 = \cdots = N_e = N(B)$ where $e =$ nilpotency index of $N(B)$ yields that if there is a QFA formula for B_{red}, then there is a QFA formula for B. Thus to show that B has a QFA formula we may assume that B is reduced. Let $P_1, \dots, P_e$ be the minimal prime ideals of B. Then $P_1 \cdots P_e = P_1 \cap \cdots \cap P_e = 0$, and by Corollary 3.2, for each $k = 1, \dots, e$ there is a QFA formula for the f.g. integral domain B/P_k. Hence again by the preceding corollary, there is a QFA formula for B. $\square$

References

[1] G. Ahlbrandt and M. Ziegler, Quasi-finitely axiomatizable totally categorical theories, *Ann. Pure Appl. Logic* **30** (1986), no. 1, 63–82.

[2] E. Artin and J. Tate, A note on finite ring extensions, *J. Math. Soc. Japan* **3** (1951), 74–77.

[3] M. F. Atiyah and I. G. Macdonald, Introduction to Commutative Algebra, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[4] N. Bourbaki, Éléments de Mathématique. Algèbre Commutative, Chapîtres 8 & 9, Masson, Paris, 1983.

[5] I. S. Cohen, Commutative rings with restricted minimum condition, *Duke Math. J.* **17** (1950), 27–42.

[6] T. Coquand, H. Lombardi, and M.-F. Roy, An elementary characterization of Krull dimension, in: L. Crosilla and P. Schuster (eds.), From Sets and Types to Topology and Analysis, pp. 239–244, Oxford Logic Guides, vol. 48, Oxford Univ. Press, Oxford, 2005.

[7] D. Eisenbud and E. G. Evans, Jr., Every algebraic set in n-space is the intersection of n hypersurfaces, *Invent. Math.* **19** (1973), 107–112.

[8] M. Hazewinkel, Formal Groups and Applications, Pure and Applied Mathematics, vol. 78, Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], New York-London, 1978.

[9] R. Heitmann, Generating non-Noetherian modules efficiently, *Michigan Math. J.* **31** (1984), no. 2, 167–180.

[10] M. Hochster and C. Huneke, Indecomposable canonical modules and connectedness, in: W. Heinzer et al. (eds.), Commutative Algebra: Syzygies, Multiplicities, and Birational Algebra (South Hadley, MA, 1992), pp. 197–208, Contemp. Math., vol. 159, Amer. Math. Soc., Providence, RI, 1994.

[11] W. Hodges, Model Theory, Encyclopedia of Mathematics and its Applications, vol. 42, Cambridge University Press, Cambridge, 1993.

[12] A. Khelif, Bi-interprétabilité et structures QFA: étude de groupes résolubles et des anneaux commutatifs, *C. R. Math. Acad. Sci. Paris* **345** (2007), no. 2, 59–61.

[13] ———, A free metabelian group of rank at least 2 is bi-interpretable with the ring of integers, in: A. Nies (ed.), Logic Blog, 2015, Part 7, Section 14, available at `http://arxiv.org/abs/1602.04432`

[14] L. Kronecker, Grundzüge einer arithmetischen Theorie der algebraischen Größen, *J. Reine Angew. Math.* **92** (1882), 1–123.

[15] S. Lang, Algebra, 2nd ed., Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1984.

[16] C. Lasserre, Polycyclic-by-finite groups and first-order sentences, *J. Algebra* **396** (2013), 18–38.

[17] ———, R. J. Thompson's groups F and T are bi-interpretable with the ring of the integers, *J. Symbolic Logic* **79** (2014), no. 3, 693–711.

[18] ———, On the direct products of quasi-finitely axiomatizable groups, *J. Group Theory* **18** (2015), no. 3, 435–453.

[19] C. Lasserre and F. Oger, Direct products and elementary equivalence of polycyclic-by-finite groups, *J. Algebra* **418** (2014), 213–226.

[20] M. Makkai and G. E. Reyes, First Order Categorical Logic. Model-Theoretical Methods in the Theory of Topoi and Related Categories, Lecture Notes in Mathematics, vol. 611, Springer-Verlag, Berlin-New York, 1977.

[21] A. Mal′cev, On a correspondence between rings and groups, *Amer. Math. Soc. Transl.* **45** (1965), 221–231.

[22] H. Matsumura, Commutative Ring Theory, Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1986.

[23] M. Nagata, Local Rings, Interscience Tracts in Pure and Applied Mathematics, vol. 13, Interscience, New York-London (1962).

[24] E. Naziazeno, A Class of QFA Rings, PhD thesis, Universidade Federal de Pernambuco, Recife, 2011.

[25] A. Nies, Separating classes of groups by first-order sentences, *Internat. J. Algebra Comput.* **13** (2003), no. 3, 287–302.

[26] ———, Describing groups, *Bull. Symbolic Logic* **13** (2007), no. 3, 305–339.

[27] ———, Comparing quasi-finitely axiomatizable and prime groups, *J. Group Theory* **10** (2007), no. 3, 347–361.
[28] G. A. Noskov, The elementary theory of a finitely generated commutative ring, *Math. Notes* **33** (1983), no. 1–2, 12–15.
[29] ———, The elementary theory of a finitely generated almost solvable group, *Math. USSR Izv.* **22** (1984), no. 3, 465–482.
[30] F. Oger, Quasi-finitely axiomatizable groups and groups which are prime models, *J. Group Theory* **9** (2006), no. 1, 107–116.
[31] F. Oger and G. Sabbagh, Quasi-finitely axiomatizable nilpotent groups, *J. Group Theory* **9** (2006), no. 1, 95–106.
[32] N. Onoda, Subrings of finitely generated rings over a pseudogeometric ring, *Japan. J. Math.* (*N.S.*) **10** (1984), no. 1, 29–53.
[33] B. Poonen, Uniform first-order definitions in finitely generated fields, *Duke Math. J.* **138** (2007), no. 1, 1–22.
[34] F. Pop, Elementary equivalence versus isomorphism, *Invent. Math.* **150** (2002), no. 2, 385–408.
[35] J. Robinson, The undecidability of algebraic rings and fields, *Proc. Amer. Math. Soc.* **10** (1959), 950–957.
[36] R. Robinson, Undecidable rings, *Trans. Amer. Math. Soc.* **70** (1951), 137–159.
[37] R. Rumely, Undecidability and definability for the theory of global fields, *Trans. Amer. Math. Soc.* **262** (1980), no. 1, 195–217.
[38] T. Scanlon, Infinite finitely generated fields are biinterpretable with $\mathbb{N}$, *J. Amer. Math. Soc.* **21** (2008), no. 3, 893–908.
[39] ———, erratum to "Infinite finitely generated fields are biinterpretable with $\mathbb{N}$," *J. Amer. Math. Soc.* **24** (2011), no. 3, 917.
[40] R. Scott, On the equations $p^x - b^y = c$ and $a^x + b^y = c^z$, *J. Number Theory* **44** (1993), no. 2, 153–165.
[41] J. R. Shoenfield, Mathematical Logic, reprint of the 1973 second printing, Association for Symbolic Logic, Urbana, IL; A K Peters, Ltd., Natick, MA, 2001.
[42] A. Singh and U. Walther, A connectedness result in positive characteristic, *Trans. Amer. Math. Soc.* **360** (2008), no. 6, 3107–3119.
[43] W. Vasconcelos, Flatness testing and torsionfree morphisms, *J. Pure Appl. Algebra* **122** (1997), 313–321.

University of California, Los Angeles, Department of Mathematics, Box 951555, Los Angeles, CA 90095-1555, USA
E-mail address: `matthias@math.ucla.edu`

Équipe de Logique Mathématique, Université Paris Diderot, UFR de mathématiques case 7012, site Chevaleret, 75205 Paris Cedex 13, France
E-mail address: `khelif@math.univ-paris-diderot.fr`

Departamento de Matemática, Universidade Federal de Pernambuco, Av. Jornalista Anibal Fernandes, s/n, Cidade Universitária, 50740-560, Recife-PE, Brasil
E-mail address: `eudes@dmat.ufpe.br`

University of California, Berkeley, Department of Mathematics, Evans Hall, Berkeley, CA 94720-3840, USA
E-mail address: `scanlon@math.berkeley.edu`