CAMbRIDGE
UNIVERSITY PRESS

## RESEARCH ARTICLE

# Decidability of the class of all the rings $\mathbb{Z} / m \mathbb{Z}$ : A problem of Ax 

Jamshid Derakhshan ${ }^{1}$ and Angus Macintyre ${ }^{2}$<br>${ }^{1}$ St Hilda's College, University of Oxford, Oxford OX4 1DY, UK; E-mail: derakhsh@maths.ox.ac.uk.<br>${ }^{2}$ School of Mathematics, University of Edinburgh, James Clerk Maxwell Building, Peter Guthrie Tait Road Edinburgh EH9 3FD, UK; E-mail: a.macintyre@ed.ac.uk.

Received: 2 July 2022; Revised: 5 January 2023; Accepted: 1 February 2023
2020 Mathematics Subject Classification: Primary - 11U05, 11T30, 03B25, 12J10, 03C60; Secondary - 11U09, 03C13, 11R56, 12L05, 12E30


#### Abstract

We prove that the class of all the rings $\mathbb{Z} / m \mathbb{Z}$ for all $m>1$ is decidable. This gives a positive solution to a problem of Ax asked in his celebrated 1968 paper on the elementary theory of finite fields [1, Problem 5, p. 270]. In our proof, we reduce the problem to the decidability of the ring of adeles $\mathbb{A}_{\mathbb{Q}}$ of $\mathbb{Q}$.


## 1. Introduction

In his classical 1968 paper on the first-order theory of finite fields, Ax asked if the first-order theory of the class of all the rings $\mathbb{Z} / m \mathbb{Z}$, for all $m>1$, is decidable [1, Problem 5, p. 270]. In that paper, Ax proved that the existential theory of this class is decidable. He proved this via his result that the theory of the class of all the rings $\mathbb{Z} / p^{n} \mathbb{Z}$ ( $p$ and $n$ varying) is decidable. This used Chebotarev's density theorem.

In this paper, we give a positive solution to Ax's problem using our work on the model theory of adeles in [6]. We use our coding of the Boolean algebra of subsets of the index set $\{$ Primes $\} \cup\{\infty\}$ in terms of idempotents in $\mathbb{A}_{\mathbb{Q}}$ together with definability in the language of rings of the set of idempotents in $\mathbb{A}_{\mathbb{Q}}$ with finite support to reduce $A x$ 's problem to the decidability of $\mathbb{A}_{\mathbb{Q}}$ proved first by Weispfenning [8] and later us [6].

## 2. Definability in adele rings

In this section, we state some results and concepts from [6],[5] on adele rings that we shall use. We only need the case $K=\mathbb{Q}$ and state the required results in this case. We denote the language of rings by $\mathcal{L}_{\text {rings }}=\{+,-, \cdot, 0,1\} . \mathbb{Q}_{p}$ denotes the field of $p$-adic numbers, $v_{p}(x)$ the $p$-adic valuation on $\mathbb{Q}_{p}$ and $\mathbb{Z}_{p}:=\left\{x \in \mathbb{Q}_{p}: v_{p}(x) \geq 0\right\}$ the valuation ring.

### 2.1. Adeles

$\mathbb{A}_{\mathbb{Q}}$ denotes the ring of adeles of $\mathbb{Q}$ and is defined as the restricted direct product of all the completions of $\mathbb{Q}$ over the index set $V_{\mathbb{Q}}=\{\infty, 2,3, \ldots\}$, the set of all primes $p$ together with $\infty$. It is the subring of the direct product of the real field $\mathbb{R}$ and all the $p$-adic fields $\mathbb{Q}_{p}$ for all primes $p$ consisting of all the elements $f$ such that $f(p)$ is in $\mathbb{Z}_{p}$ for all but finitely many $p$.

[^0]See Cassels and Frohlich [3], and especially Cassels' article [2], for properties of adele rings. We shall construe adeles as functions on $V_{\mathbb{Q}}$ taking values in the stalks $\mathbb{Q}_{p}$, where $p \in V_{\mathbb{Q}}$.
To $\infty$ corresponds the real field $\mathbb{R}$ and to finite $p$ correspond $\mathbb{Q}_{p}$. One sets $\mathbb{Q}_{\infty}=\mathbb{R}$.

### 2.2. Uniform definition of valuation

Each of the stalks $\mathbb{Q}_{p}$, where $p \leq \infty$, is a locally compact field of characteristic 0 , with a canonical choice of metric, and thus a canonical choice of unit ball (which is a subring in the case of $p<\infty$ ).

The following theorem shows that the unit ball $\mathbb{Z}_{p}$ is uniformly $\mathcal{L}_{\text {rings }}$-definable without parameters in $\mathbb{Q}_{p}$ for all $p<\infty$. Note that the unit ball in $\mathbb{R}$ is also $\mathcal{L}_{\text {rings }}$-definable.
Theorem 2.1 [4, Theorem 2]. There is an $\mathcal{L}_{\text {rings-formula }} \Phi_{\text {val }}(x)$ without parameters that uniformly defines the valuation ring of all Henselian valued fields with finite or pseudo-finite residue field.

### 2.3. The Boolean algebra

We denote the language of Boolean algebras by $\{\wedge, \vee, \neg, 0,1\}$. The set $\mathbb{B}_{\mathbb{Q}}=\left\{e \in \mathbb{A}_{\mathbb{Q}}: a^{2}=a\right\}$ of idempotents in $\mathbb{A}_{\mathbb{Q}}$ forms a Boolean algebra with Boolean operations

$$
\begin{gathered}
e \wedge f=e f, \\
e \vee f=1-(1-e)(1-f)=e+f-e f, \\
\neg e=1-e .
\end{gathered}
$$

$\mathbb{B}_{Q}$ carries a partial order defined by $e \leq f$ if and only if $e=e f$ (product in the ring).
An idempotent $e$ is called minimal if it is nonzero and minimal with respect to this order. Let atom $(x)$ be an $\mathcal{L}_{\text {rings }}$-formula expressing that $x$ is a minimal idempotent (i.e., an atom).

There is a bijective correspondence between subsets of $V_{\mathbb{Q}}$ and idempotents $e$ in $\mathbb{A}_{\mathbb{Q}}$ given by $X \longmapsto e_{X}$, where for $X \subseteq V_{\mathbb{Q}}$,

$$
e_{X}(p)= \begin{cases}1 & \text { if } p \in X \\ 0 & \text { if } p \notin X\end{cases}
$$

Conversely, if $e \in \mathbb{A}_{\mathbb{Q}}$ is idempotent, let $X=\left\{p \in V_{\mathbb{Q}}: e(p)=1\right\}$. Then $e=e_{X}$.

### 2.4. Idempotents with finite support

The support of an adele $a \in \mathbb{A}_{\mathbb{Q}}$ is defined by

$$
\operatorname{supp}(a):=\left\{p \in V_{\mathbb{Q}}: a(p) \neq 0\right\} .
$$

We denote by $\mathcal{F i n}_{\mathbb{Q}}$ the set of all idempotents $e$ in $\mathbb{A}_{\mathbb{Q}}$ with finite support, that is, $\operatorname{supp}(e)$ is a finite set.
A basic result in the model theory of adeles [6] is the following.
Theorem 2.2 [6]. $\mathcal{F i n}_{\mathbb{Q}}$ is an $\mathcal{L}_{\text {rings }}-$ definable subset of $\mathbb{A}_{\mathbb{Q}}$.

### 2.5. Boolean values

If $e \in \mathbb{A}_{\mathbb{Q}}$ is a minimal idempotent, then the ring $\mathbb{A}_{\mathbb{Q}} /(1-e) \mathbb{A}_{\mathbb{Q}}$ is naturally isomorphic to $e \mathbb{A}_{\mathbb{Q}}$ by the map

$$
a+(1-e) \mathbb{A}_{\mathbb{Q}} \mapsto e a,
$$

and if $e$ corresponds to the prime $p \in\{$ Primes $\} \cup\{\infty\}$, then

$$
e \mathbb{A}_{\mathbb{Q}} \cong \mathbb{Q}_{p}
$$

via the map

$$
e a \mapsto a(p) .
$$

For an $\mathcal{L}_{\text {rings }}$-formula $\Phi\left(x_{1}, \ldots, x_{n}\right)$ and $a_{1}, \ldots, a_{n} \in \mathbb{A}_{\mathbb{Q}}$, the (ring-theoretic) Boolean value [ $\left.\left[\Phi\left(a_{1}, \ldots, a_{n}\right)\right]\right]$ is defined to be the supremum of all the minimal idempotents $e$ in $\mathbb{B}_{\mathbb{Q}}$ such that

$$
e \mathbb{A}_{\mathbb{Q}} \vDash \Phi\left(e a_{1}, \ldots, e a_{n}\right) .
$$

This supremum exists since $\mathbb{B}_{\mathbb{Q}}$ is a complete Boolean algebra.
For any given $\mathcal{L}_{\text {rings }}$-formula $\Phi\left(x_{1}, \ldots, x_{n}\right)$, there is another $\mathcal{L}_{\text {rings }}$-formula $\Phi^{*}\left(y, x_{1}, \ldots, x_{n}\right)$, that can be effectively constructed from $\Phi\left(x_{1}, \ldots, x_{n}\right)$, such that for any $a_{1}, \ldots, a_{n} \in \mathbb{A}_{\mathbb{Q}}$ we have

$$
(*) e \mathbb{A}_{\mathbb{Q}} \vDash \Phi\left(e a_{1}, \ldots, e a_{n}\right) \Leftrightarrow \mathbb{A}_{\mathbb{Q}} \vDash \Phi^{*}\left(e, a_{1}, \ldots, a_{n}\right) .
$$

This follows by induction on the complexity of $\Phi\left(x_{1}, \ldots, x_{n}\right)$ from the quantifier-free case which is straightforward.

The function from $\mathbb{A}_{Q}^{n}$ into $\mathbb{B}_{\mathbb{Q}}$ defined by

$$
\left(a_{1}, \ldots, a_{n}\right) \rightarrow\left[\left[\Phi\left(a_{1}, \ldots, a_{n}\right)\right]\right]
$$

is $\mathcal{L}_{\text {rings }}$-definable for any $\Phi\left(x_{1}, \ldots, x_{n}\right)$.
Indeed, the set

$$
Z=\left\{\left(x_{1}, \ldots, x_{n}, z\right) \in \mathbb{A}_{Q}^{n+1}: z=\sup \left(W_{x_{1}, \ldots, x_{n}}\right)\right\},
$$

where

$$
W_{x_{1}, \ldots, x_{n}}=\left\{w \in \mathbb{B}_{\mathbb{Q}}: \mathbb{A}_{\mathbb{Q}} \vDash \operatorname{atom}(w) \text { and } w \mathbb{A}_{\mathbb{Q}} \vDash \Phi\left(w x_{1}, \ldots, w x_{n}\right)\right\}
$$

is definable since by $(*), W_{x_{1}, \ldots, x_{n}}$ equals

$$
\left\{w \in \mathbb{B}_{\mathbb{Q}}: \mathbb{A}_{\mathbb{Q}} \mid=\operatorname{atom}(w) \text { and } \mathbb{A}_{\mathbb{Q}} \vDash \Phi^{*}\left(w, x_{1}, \ldots, x_{n}\right)\right\}
$$

and thus $Z$ is defined by the formula

$$
z=\sup \left\{w: \operatorname{atom}(w) \wedge \Phi^{*}\left(w, x_{1}, \ldots, x_{n}\right)\right\}
$$

(which is expressible as an $\mathcal{L}_{\text {rings }}$-formula since the ordering on $\mathbb{B}_{\mathbb{Q}}$ is $\mathcal{L}_{\text {rings }}$-definable).
Let $\Psi_{\mathbb{R}}$ denote a sentence that holds in $\mathbb{R}$ but does not hold in any $\mathbb{Q}_{p}$ for $p<\infty$, for example

$$
\forall x \exists y\left(x=y^{2} \vee-x=y^{2}\right) .
$$

We call a minimal idempotent $e$ real if $e \mathbb{A}_{\mathbb{Q}} \vDash \Psi_{\mathbb{R}}$.
We denote by $e_{\mathbb{R}}$ the supremum of all the real minimal idempotents (note that there is only one real minimal idempotent in $\left.\mathbb{B}_{\mathbb{Q}}\right) . e_{\mathbb{R}}$ is supported only on the set $\{\infty\}$.

We put $e_{\text {fin }}:=1-e_{\mathbb{R}}$. This idempotent is supported on the set of all primes except infinity.
We define $\left[\left[\Phi\left(a_{1}, \cdots, a_{n}\right)\right]\right]^{r e a l}$ to be the supremum of all the minimal idempotents $e$ such that

$$
e \mathbb{A}_{\mathbb{Q}} \mid=\Psi_{\mathbb{R}} \wedge \Phi\left(e a_{1}, \cdots, e a_{n}\right) .
$$

Let $\Psi_{\text {fin }}$ denote an $\mathcal{L}_{\text {rings }}$-sentence that holds in $\mathbb{Q}_{p}$ for all $p<\infty$ and does not hold in $\mathbb{R}$. For example, we can take $\Psi_{\text {fin }}$ to be the negation of the $\Psi_{\mathbb{R}}$ given above, namely

$$
\exists x \forall y\left(x \neq y^{2} \wedge-x \neq y^{2}\right)
$$

which is true in any $p$-adic field $\mathbb{Q}_{p}$ by taking $x$ to be $p$.
We define $\left[\left[\Phi\left(a_{1}, \cdots, a_{n}\right)\right]\right]^{f i n}$ to be the supremum of all the minimal idempotents $e$ such that

$$
e \mathbb{A}_{\mathbb{Q}} \vDash \Psi_{\text {fin }} \wedge \Phi\left(e a_{1}, \cdots, e a_{n}\right) .
$$

An argument similar to that above on the definability of the Boolean value $\left[\left[\Phi\left(x_{1}, \ldots, x_{n}\right)\right]\right]$ shows that the functions given by

$$
\begin{aligned}
& \left(a_{1}, \ldots, a_{n}\right) \mapsto\left[\left[\Phi\left(a_{1}, \ldots, a_{n}\right)\right]\right]^{\text {real }} \\
& \left(a_{1}, \ldots, a_{n}\right) \mapsto\left[\left[\Phi\left(a_{1}, \ldots, a_{n}\right)\right]\right]^{f i n}
\end{aligned}
$$

from $\mathbb{A}_{\mathbb{Q}}^{n}$ into $\mathbb{B}_{\mathbb{Q}}$ are $\mathcal{L}_{\text {rings }}$-definable for any $\Phi\left(x_{1}, \ldots, x_{n}\right)$.
We remark that the definability of $\mathcal{F}_{\mathbb{Q}_{\mathbb{Q}}}$ in Theorem 2.2 together with the definability of the Boolean values $\left[\left[\Phi\left(x_{1}, \ldots, x_{n}\right)\right]\right]$ imply the definability of the sets of the form

$$
\left\{\left(x_{1}, \ldots, x_{n}\right) \in \mathbb{A}_{\mathbb{Q}}^{n}:\left[\left[\Phi\left(x_{1}, \ldots, x_{n}\right)\right]\right] \in \mathcal{F i n}_{\mathbb{Q}}\right\}
$$

which occur as 'basic' sets in the quantifier elimination theorem for adele rings in [6].

## 3. Ax's problem

Theorem 3.1. The class of all $\mathbb{Z} / m \mathbb{Z}$ is uniformly interpretable in $\mathbb{A}_{\mathbb{Q}}$.
Proof. Our proof consists of two parts.
Part 1. By uniform definability of the $\mathbb{Z}_{p}$ in $\mathbb{Q}_{p}$ for $p<\infty$ using the formula $\Phi_{\text {val }}(x)$, the set of elements of $\mathbb{A}_{\mathbb{Q}}$ whose $\mathbb{Q}_{p}$-component lies in $\mathbb{Z}_{p}$ for each $p<\infty$ is definable since it equals

$$
\left\{a \in \mathbb{A}_{\mathbb{Q}}:\left[\left[\Phi_{\mathrm{val}}(a)\right]\right]^{f i n}=e_{f i n}\right\}
$$

(and is isomorphic to $\mathbb{R} \times \widehat{\mathbb{Z}}$ ).
Consider a positive integer $m$. Suppose $m$ factors as a nontrivial product of coprime prime powers $q_{j}^{r_{j}}$.
Consider the element $g$ which takes value 1 at all minimal idempotents (including that corresponding to the infinite place $\infty$ ) except those corresponding to the $q_{j}$, and takes value $q_{j}^{r_{j}}$ at $q_{j}$. Then $g-1$ is an element of finite support (and the stated conditions on $g$ can be expressed by $\mathcal{L}_{\text {rings }}$-formulas).

The quotient $(\mathbb{R} \times \hat{\mathbb{Z}}) /(g)$ is naturally isomorphic to the product over the finitely many $j$ of the quotients $\mathbb{Z}_{q_{j}} / q_{j}^{r_{j}} \mathbb{Z}_{q_{j}}$, and this is isomorphic to the product of the finitely many $\mathbb{Z} / q_{j}^{r_{j}} \mathbb{Z}$, which is obviously isomorphic to $\mathbb{Z} / m \mathbb{Z}$. Note that the set of all $g$ satisfying the conditions above is $\mathcal{L}_{\text {rings }}$-definable in $\mathbb{A}_{\mathbb{Q}}$.

Part 2. Suppose $g-1$ is an element of finite support. In addition, suppose that $g$ takes values in $\mathbb{Z}_{p}$ for all $p<\infty$ and at some prime $p<\infty, g$ takes as value a $p$-adic nonunit. These conditions can be stated as

$$
g-1 \in \mathcal{F i n}_{\mathbb{Q}}
$$

and

$$
\left[\left[\Phi_{\mathrm{val}}(g)\right]\right]^{\text {fin }}=e_{\text {f in }} \wedge\left[\left[\Phi_{\mathrm{val}}(g) \wedge \neg \Phi_{\mathrm{val}}\left(g^{-1}\right)\right]\right]^{\text {fin }} \neq 0,
$$

where 0 denotes the zero element of the Boolean algebra $\mathbb{B}_{\mathbb{Q}}$ and 1 denotes the top element of the Boolean algebra $\mathbb{B}_{\mathbb{Q}}$ (namely, the adele with 1 at every coordinate). These conditions can be expressed by $\mathcal{L}_{\text {rings }}$-formulas (using Theorem 2.2).

Then $g$ takes value 1 at all but finitely many elements of $V_{\mathbb{Q}}$. Assume that $g$ takes value 1 at the infinite prime, and note that this is a definable condition on $g$ since the set

$$
\left\{h \in \mathbb{A}_{\mathbb{Q}}: h(\infty)=1\right\}
$$

is $\mathcal{L}_{\text {rings }}$-definable in $\mathbb{A}_{\mathbb{Q}}$ (since $h(\infty)=1$ is equivalent to $e_{\mathbb{R}} h=e_{\mathbb{R}}$ ).
Now, consider $(\mathbb{R} \times \hat{\mathbb{Z}}) /(g)$. It is clear that this quotient is a product over finitely many primes $q_{j}$ of quotients of $\mathbb{Z}_{q_{j}}$ by the ideal generated by an element of $\mathbb{Z}_{q_{j}}$. When that element is a unit the quotient is the trivial ring and can be discarded. For at least one prime, the element is not a unit and then generates the same ideal as some power of the prime $q_{j}$. Then as in Part $1,(\mathbb{R} \times \hat{\mathbb{Z}}) /(g)$ is isomorphic to $\mathbb{Z} / m \mathbb{Z}$ for some $m>1$.

The assumptions imposed on $g$ are all $\mathcal{L}_{\text {rings }}$-definable in $\mathbb{A}_{\mathbb{Q}}$ because of the $\mathcal{L}_{\text {rings }}$-definability of $\mathcal{F} \mathcal{F i n}_{\mathbb{Q}}$ and of the Boolean values in $\mathbb{A}_{\mathbb{Q}}$, and the uniform $\mathcal{L}_{\text {rings }}$-definability of $\mathbb{Z}_{p}$ in $\mathbb{Q}_{p}$ (Theorems 2.1 and 2.2).

This argument gives the intended interpretation of the class of all $\mathbb{Z} / m \mathbb{Z}$ (for all $m>1$ ) in $\mathbb{A} \mathbb{Q}$.
Corollary 3.1. The class of all $\mathbb{Z} / m \mathbb{Z}(m>1)$ is decidable.
Proof. Let $\mathfrak{X}$ denote the set of all $g$ in $\mathbb{A}_{\mathbb{Q}}$ such that $g-1$ has finite support, $g$ takes value 1 at the infinite prime, $g$ takes values in $\mathbb{Z}_{p}$ for all $p<\infty$, and $g$ takes as value a $p$-adic nonunit at some $p<\infty$. By Part 2 of the proof of Theorem 3.1, $\mathfrak{X}$ is an $\mathcal{L}_{\text {rings }}$-definable subset of $\mathbb{A}_{\mathbb{Q}}$.

By Parts 1 and 2 of the proof of Theorem 3.1, any ring from the class $\{\mathbb{Z} / m \mathbb{Z}: m>1\}$ is isomorphic to a ring from the class

$$
\{(\mathbb{R} \times \hat{\mathbb{Z}}) /(g): g \in \mathfrak{X}\}
$$

and conversely any $(\mathbb{R} \times \hat{\mathbb{Z}}) /(g)$, where $g \in \mathfrak{X}$, is isomorphic to $\mathbb{Z} / m \mathbb{Z}$ for some $m>1$.
Thus, deciding whether an $\mathcal{L}_{\text {rings }}$-sentence $\Psi$ holds in $\mathbb{Z} / m \mathbb{Z}$ for all $m$ is equivalent to deciding whether $\Psi$ holds in $(\mathbb{R} \times \hat{\mathbb{Z}}) /(g)$ for all $g \in \mathfrak{X}$. Since $\mathbb{R} \times \hat{\mathbb{Z}}$ and $\mathfrak{X}$ are definable in $\mathbb{A}_{\mathbb{Q}}$, this decision procedure can be carried out because of the decidability of $\mathbb{A}_{\mathbb{Q}}$.

For a proof of the decidability of $\mathbb{A}_{\mathbb{Q}}$, see [6, Section 7.1] or [8].
We would like to end with some remarks on the connection between our work and that of Ax [1] and Feferman-Vaught [7] and the role (and need) for the model theory and definability in adele rings from [6].

One might have thought that an easier solution to Ax's problem could be given without adeles using Ax's decidability results for the $\mathbb{Z} / p^{n} \mathbb{Z}$ for $p$ and $n$ varying [1] combined with the Feferman-Vaught technology for products [7]. But, as we describe below, this would require redoing variants of proofs that are analogous to our proof of decidability of adeles in [6], going back into details of Feferman-Vaught and making ad hoc adjustments and giving interpretations similar to those given in this paper but in a not very meaningful context. There would be a subtle flaw if one would just try to combine the results in [1] and [7] because of the following points.

Feferman-Vaught [7] work with products of families of $L$-structures $\left(\mathfrak{H}_{i}\right)_{i \in I}$, for varying index sets $I$ and some fixed first-order language $L$. There is the associated Boolean algebra Powerset ( $I$ ) consisting of subsets of $I$ in an extension $\mathfrak{S}$ of the language of Boolean algebras (e.g., with a predicate for the ideal of finite subsets of $I$ ). One then equips the products $\prod_{i \in I} \mathfrak{H}_{i}$ with relations defined using $\mathfrak{S}$ and Boolean values of $L$-formulas in the Boolean algebra Powerset $(I)$, thus obtaining the generalized product $\mathcal{P}(\mathfrak{A}, \mathfrak{\Im})$. A general procedure attaches to definitions in the generalized products $\mathcal{P}(\mathfrak{A}, \mathfrak{S})$ definitions in the Boolean structure $\mathfrak{\Im}$, by the intermediary of the Boolean values of $L$-formulas.

The relevant Feferman-Vaught theorem for decidability of a class consisting of products from a decidable class of structures is the following.

Theorem 3.2 [7, Theorem 5.6]. Let $\mathcal{K}$ be a class of L-structures. Let $\mathcal{P}_{\mathcal{K}, \mathcal{S}}$ be the class of all structures $\mathcal{P}(\mathfrak{A}, \mathfrak{S})$ which are generalized products of an indexed family $\mathfrak{A}=\left(\mathfrak{A}_{\mathfrak{i}}\right)_{i \in I}$, where $\mathfrak{S}$ is an expansion of

Powerset(I) and belongs to a fixed class $\mathcal{S}$ of Boolean expansions of the sets Powerset(I) where I is a nonempty set, and for each $i \in I, \mathfrak{Y}_{\mathfrak{i}} \in \mathcal{K}$. Suppose the theory of $\mathcal{K}$ is decidable and the theory of $\mathcal{S}$ is decidable. Then the theory of $\mathcal{P}_{\mathcal{K}, \mathcal{S}}$ is decidable.

For Ax's problem, what does one take for the class $\mathcal{K}$ and the enriched Boolean structure? It is no good simply to take $\mathcal{K}$ as the set of all $\mathbb{Z} / p^{n} \mathbb{Z}$ for $p$ and $n$ varying and the Boolean structure to be atomic Boolean algebras with a predicate for the ideal of finite sets. Among the products one would get are rings which are products of factors which are not simply a $\mathbb{Z} / p^{n} \mathbb{Z}$ but can be nontrivial powers of such rings, and so one does interpret more than the $\mathbb{Z} / m \mathbb{Z}$. We do get a decidability result, but for a class bigger than the class of all $\mathbb{Z} / m \mathbb{Z}$, for $m>1$. A similar problem arises if we try to work with generalized products of the $\mathbb{Q}_{p}$ or $\mathbb{Z}_{p}$ instead of the $\mathbb{Z} / p^{n} \mathbb{Z}$.

There are devices for doing better in the ring formalism, by considering axioms excluding that distinct minimal idempotents have distinct finite characteristics for the residue fields of the stalks at these idempotents. But this is an infinite set of axioms, and the naive decidability does not immediately combine with it to give the decidability one wants.

In this paper, we get a short and intelligible solution to Ax's problem via decidability and definability in $\mathbb{A}_{\mathbb{Q}}$, but we have to work quite hard to get such a solution without using adeles and definability results from [6]. We remark that [6] uses Feferman-Vaught [7] and Ax [1].

We believe that the interpretations given in the proofs of Theorem 3.1 and Corollary 3.1 between $\mathbb{A}_{\mathbb{Q}}$ and the finite rings $\mathbb{Z} / m \mathbb{Z}$ should be of an independent interest.

Acknowledgement. Angus Macintyre was supported by a Leverhulme Emeritus Fellowship.
Competing interest. The authors have no competing interest to declare.

## References

[1] J. Ax, 'The elementary theory of finite fields’, Ann. of Math. (2) 88 (1968), 239-271.
[2] J. W. S. Cassels, 'Global fields', in Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965) (Thompson, Washington, DC, 1967), 42-84.
[3] J. W. S. Cassels and A. Fröhlich, eds. Algebraic Number Theory (Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London, 1986). Reprint of the 1967 original.
[4] R. Cluckers, J. Derakhshan, E. Leenknegt and A. Macintyre, 'Uniformly defining valuation rings in Henselian valued fields with finite or pseudo-finite residue fields', Ann. Pure Appl. Logic 16412 (2013), 1236-1246.
[5] J. Derakhshan and A. Macintyre, 'Some supplements to Feferman-Vaught related to the model theory of adeles', Ann. Pure Appl. Logic 16511 (2014), 1639-1679.
[6] J. Derakhshan and A. Macintyre, 'Model theory of adeles I', Ann. Pure Appl. Logic 1733 (2022), Paper No. 103074, 43.
[7] S. Feferman and R. L. Vaught, 'The first order properties of products of algebraic systems', Fund. Math. 47 (1959), 57-103.
[8] V. Weispfenning, 'Model theory of lattice products', Habilitation, Universitat Heidelberg (1978).


[^0]:    © The Author(s), 2023. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

