Contemporary Mathematics

Decidability and Local-Global Principles

L. Darnière

Abstract. The ambitious goal of this survey is to give a comprehensive overview of the decidability results obtained in recent years for rings (and fields) based on the use of a geometric Local-Global Principle. After an informal introduction to the main notions of this paper, we present in part I the deep theorems of algebraic geometry which provide many natural examples of rings satisfying a Local-Global Principle, in every characteristic. Part II is devoted to the numerous developments in model theory which may have been stimulated by the results of part I, and specially to decidability results for those rings.

Introduction

1. What is a Local-Global Principle?

The interest of modern number theorists in **Local-Global Principles** (**LGP** for short) mostly originates from the works of Hasse in 1923-1924.

Theorem 1.1 (Hasse). *Let q be a quadratic form defined over a number field K. The equation $q(x) = 0$ has a nontrivial solution in K (that is a solution other than $(0, \dots, 0)$) if and only if it has a nontrivial solution in every completion of K.*

Definition 1.2. A family of varieties defined over a field K is said to satisfy the **Hasse principle** with respect to a family Σ of places of K if any affine open subset of such a variety has a point in K if and only if it has a point in every completion of K with respect to the places of Σ. A variant of importance for us is the **nonsingular Hasse principle** which is the same as the Hasse principle with the word "point" replaced everywhere by "smooth point". Observe that since the smooth locus is an open affine subset, the Hasse principle implies the nonsingular Hasse principle.

Since the (nonsingular) Hasse principle doesn't work for most families of varieties over number fields, a large amount of work has been done in order to characterize what exactly the obstruction is that prevents a Hasse principle from holding

---

1991 *Mathematics Subject Classification.* Primary 11U05, 11U09; Secondary 11R04, 11G35.
The author would like to thank the organizers of the workshop on Hilbert tenth problem, Gent, November 1999, and specially Jan Denef for his encouragement. He would like also to thank Aharon Razon for his very carefull reading of a preliminary version of this paper.

for a given family. These obstructions are usually of a cohomological nature and we won't consider them here. Indeed we are concerned with fields in which a Hasse principle holds with respect to a given set of places, for *every* variety. Many examples of such fields algebraic (not of finite degree) over $\mathbb{Q}$ or $\mathbb{F}_p(t)$ have been given in recent years. Those results of algebraic geometry have their counterpart in the model theory of fields, specially on questions of decidability.

A Hasse principle reduces the problem of solving an equation in K to the same question in the completions of K, in which it is usually easier to answer. Since some complete fields, including $\mathbb{R}$, $\mathbb{Q}_p$ and their finite extensions, have decidable complete theories, there is some hope when a Hasse principle holds for a field K to deduce from it that the existential or even the complete theory of K is decidable. At least (remember that no decidability result is known for $\mathbb{F}_p((T))$) one can hope to reduce a decidablity problem over K to the same problem over various auxiliary structures including the completions of K, even if this problem is still unsolved for those simpler structures.

FACT 1.3. *Let K be any ordered field, $\bar{K}$ its real closure and $\hat{K}$ the completion of $\bar{K}$. Then an affine open set of a variety defined over K has a (smooth) $\bar{K}$-rational point if and only if it has a (smooth) $\hat{K}$-rational point. Moreover the smooth $\bar{K}$-rational points are dense among the $\hat{K}$-rational points with respect to the topology of the order.*

This follows immediatly from the model completeness of real closed fields, which real geometers know as Tarski-Seidenberg's principle.

FACT 1.4. *Let K be a valued field, K^h its henselization and $\hat{K}$ the completion of K^h. Then an affine open set of a variety defined over K has a K^h-rational smooth point if and only if it has a $\hat{K}$-rational smooth point, and moreover the former are dense among the latter with respect to the topology of the valuation.*

This was proved by Lang [**Lan51**] when the value group of the valuation embeds into the reals (that is the valuation is an absolute value) and by Greenberg [**Gre66**] when the henselian valuation ring is discrete and excellent. This statement in its full generality is probably well known but may have been unpublished before [**Dar98**, §I.5].

Facts 1.3 and 1.4 prove that in the nonsingular Hasse principle it is not necessary to use completions: real closures and henselizations are large enough. This motivates the following definition.

DEFINITION 1.5. Given a domain A with fraction field K let $\mathcal{R}(A)$ be the family of all real closures of K, and all the henselizations of the valuation rings centered (see the next section) at maximal ideals of A. Sometimes, tuples of elements of R ($R \in \mathcal{R}$) are called **local points**, and those of A are called **global points**.
We say that the **main LGP** holds for A if any affine open subset of any variety defined over K has a smooth point in A if and only if it has a smooth point in every $R \in \mathcal{R}(A)$.

The main LGP is nothing but a rephrasing of the nonsingular Hasse principle for every variety, with the sole difference that real or henselian closures replace completions, but we have seen that this is unessential.

At the other extreme, it is possible to consider an abstract LGP without topology nor variety at all. Remember that a subring A of a ring B is **relatively**

existentially closed in B if every finite system of polynomial equations an inequalities with coefficients in A having a solution in B already has a solution in A. For example an algebraically closed field is relatively existentially closed in any domain which contains it. We denote this by $A \leq_{\exists} B$. This is the form that relative existential closure takes for rings, but this notion is actually meaningfull for any elementary class of structures. Ershov introduced in [**Ers92b**] the following notion (we adapt to domains his definition given for fields). A domain A with fraction field K is **regularly closed relatively to a family** $\mathcal{R}$ of rings containing A and contained in the algebraic closure of K if and only if $A \leq_{\exists} B$ for every domain B containing A with fraction field L such that:

- L is a regular extension of K.
- $\forall R \in \mathcal{R}$, $R \leq_{\exists} R \otimes_A B$.

This fairly general Local-Global Principle has the remarkable property of being equivalent[1] to the main LGP when $\mathcal{R} = \mathcal{R}(A)$. Although it has never been used until now in its full generality, the relative regular closedness property emphasizes the deep model theoretic significance of the main LGP.

And what about the Hasse principle without smoothness assumptions? It appears that in all the results of algebraic geometry that we will mention in this paper, local points are required either to be smooth or to belong to a valuation ring with separably closed fraction field. But in this last case the existence of a point implies the existence of a smooth point by fact 1.6 below. Hence in all the known cases the Local-Global Principles coming from geometry boil down to the nonsingular Hasse principle (or some strengthening of it including for example density properties).

FACT 1.6. *Let R be a valuation ring with a separably closed fraction field F. Then any variety V defined over F which has a point in R has a smooth point in R.*

This is analogous to the well known fact that the smooth points are dense in any $\mathbb{C}$-variety with respect to the usual topology on $\mathbb{C}^n$. Indeed the same density property holds in F with the topology defined by R and since R is open for this topology the conclusion follows. For lack of a reference we give a proof.

PROOF. (For the notations see section 3.) We first suppose F to be algebraically closed. If V is a curve C, let $\mathcal{C}$ be its normalization and $\pi : \mathcal{C} \mapsto C$ the corresponding surjective morphism. Since F is algebraically closed π maps $\mathcal{C}(F)$ surjectively onto $C(F)$, and moreover it is continuous with respect to the topology of the valuation on an open subset of $\mathcal{C}(F)$. For any $y \in C(R)$ choose $x \in \pi^{-1}(B)$ where B is any open neighborhood of y in $C(F)$ small enough so that $B \subseteq C(R)$ and B does not contain any singular point of $C \setminus \{y\}$. The implicit function theorem applied to x (R is henselian, x is smooth) gives points $x' \in \mathcal{C}(F) \setminus \{x\}$ arbitrarily close to x hence in the open set $\pi^{-1}(B)$. By construction $y' = \pi(x') \in B \setminus \{y\}$, in particular $y' \in C^{\circ}(R)$. Eventually if $\dim V \geq 2$ given any $y \in V(R)$, using a Bertini type argument like in [**Rum86**, p. 129], draw a curve C on V passing through y and any smooth point of V. Since C is not contained in the singular locus V_{sing} of V the set $V_{sing} \cap C(F)$ is finite. The previous argument provides points y' in $C^{\circ}(R)$ arbitrarily close to y. Hence one can choose such a point not in $V_{sing} \cap C(F)$, that is $y' \in V^{\circ}(R)$.

[1] This equivalence is true in a more general setting, see [**Dar98**, §I.1].

If F is only separably closed let $\tilde{R}$ be the integral closure of R inside the algebraic closure of F. If $V(R) \neq \emptyset$ then by the previous case $V^\circ(\tilde{R}) \neq \emptyset$ and this implies $V^\circ(R) \neq \emptyset$ by [**Dar98**, lemma III.4.2] (or [**Darb**, lemma 3]). □

2. What is a decidability result?

Hilbert's tenth problem asks for a process to solve any finite system of diophantine equations, or at least to decide wether or not such a system has a solution in integers. In modern language (see below) this last question can be rephrased as: does the ring $\mathbb{Z}$ have a decidable existential theory? As Matjasevič proved in 1970, the answer is negative.

During the intermediate period anyhow, this question was elaborated in many ways, and adapted to many different contexts by logicians. Adaptations consist in replacing polynomials and equations, which are all the terms and relations in the language of rings, by terms and relations in any other language. For example over an ordered ring one can consider not only polynomial equations but also polynomial inequalities. Generalizations consist in replacing existential formulas, which ask for solution of a finite system of relations between terms, by arbitrary (first-order) formulas. For example in the language of rings, **first-order formulas** take the following form, up to logical equivalence modulo the axioms of ring theory [2]:

$$Q_1 x_1 \cdots Q_m x_m B(x_1, \ldots, x_m)$$

with $Q_1, \ldots, Q_m$ being any quantifier ($\exists$ or $\forall$) and the terms $B(x_1, \ldots, x_m)$ a (finite) boolean combination of polynomials equations with integral coefficients. Among first-order formulas, written as above with all the quantifiers on the left hand side, the **existential formulas** are those whose quantifiers are all existential (that is, in the above example, Q_i is $\exists$ for every $i \leq m$).

A structure, for example a ring A, has a decidable theory (resp. a decidable existential theory) if there exists an algorithm which decides whether or not any given formula (resp. existential formula) is satisfied by A. So Hilbert's tenth problem is a problem of decidability for the set of existential formulas in the language of rings. In this paper we will mostly focus on decidability results for the set of all first-order formulas. Of course when a ring has a decidable theory, its existential theory is decidable as well. A ring with a decidable (resp. undecidable) first-order theory is called a **decidable ring** (resp. an **undecidable ring**).

All the undecidability results known by the author (including Matjasevič's one) are based on the following theorem, going back to Gödel: there exists recursively enumerable sets of positive integers which are not recursive (that is whose complement is not recursively enumerable).

Now, how is proved a positive decidability result for a given structure? Mostly by using the following trick: an **axiomatization** of a structure A is a set T of formulas such that a formula φ is satisfied in A if and only if φ belongs to the set $\bar{T}$ of all logical consequences of T. If T is recursively enumerable (for short, a recursively enumerable axiomatization of a structure is called a **recursive axiomatization** of it) then so is $\bar{T}$. To decide whether or not a formula φ is satisfied by A, an algorithm then consists in enumerating all the logical consequences of T: since $\bar{T}$ is recursively enumerable this is a recursive procedure, and it must ends since either

[2] We won't give here the general definition of a first-order formula in any language, the reader being assumed to know the basics. For a short introduction to logic see [**Hod97**, Chap. 1].

φ or $\neg\varphi$ belongs to $\bar{T}$. Hence the decidability of a structure can be proved by exhibiting a recursive axiomatization[3].

EXAMPLE 2.1. An axiomatization of $\mathbb{C}$ is given by the formulas saying that $\mathbb{C}$ is an algebraically closed field of characteristic zero. This provides a recursive axiomatization of the theory of $\mathbb{C}$, hence this theory is decidable.

EXAMPLE 2.2. An axiomatization of $\mathbb{R}$ is given by the formulas saying that $\mathbb{R}$ is a real closed field. This provides a recursive axiomatization of the theory of $\mathbb{R}$, hence this theory is decidable.

EXAMPLE 2.3. A recursive axiomatization of the theory of pseudo algebraically closed fields is given by the formulas saying that any nonempty variety defined over such a field has a point in it. However this theory, which is not complete (see footnote 3), is undecidable.

As the above classical examples show, proving decidability through recursive axiomatization of a structure moves the difficulty from algorithmic, whose complexity may be unbearable, to algebra. Indeed, finding an axiomatization of a structure usually goes this way: a nice elementary class of structures is isolated, in which elementary embeddings, and hopefully elementary equivalence can be characaterized by meaningfull (algebraic) properties, and then the general study of this class applies to the special case of the given structure. All the papers of model theory which are surveyed in part II more or less follow this approach. For this reason we can not report their decidability results without giving an overview of the main auxiliary notions involved in order to construct an illuminating recursive axiomatization.

3. Notations

Our rings are commutative with unit. Given a domain A we denote by $\tilde{A}$ the integral closure of A in an algebraic closure of the fraction field $\mathrm{Frac}(A)$ of A. In particular if K is a field then $\tilde{K}$ is its algebraic closure, and if K contains A then $\tilde{A} \cap K$ is the integral closure of A inside K. We denote by K^s the separable closure of K, and by $G(K)$ the absolute Galois group of K, that is the group of K-automorphisms of K^s. Since any such automorphism has a unique extension to $\tilde{K}$, we sometimes consider the elements of $G(K)$ as K-automorphisms of $\tilde{K}$.

Our varieties are affine, geometrically irreducible and geometrically reduced. In other words, **a variety V defined over K** corresponds to a prime ideal of $\tilde{K}[X_1, \ldots, X_n]$ having a set $f = (f_1, \ldots, f_m)$ of generators in $K[X_1, \ldots, X_n]$. Our points are closed points: given any subset Ω of a K-algebra B, we call **points of V in Ω** the set $V(\Omega)$ of solutions of $f(x) = 0$ in Ω^n. Affine open subsets, dimension, smoothness (through the Jacobian criterion) and K-rational functions are defined as usual. We denote by $V^\circ(\Omega)$ the smooth points of V in Ω.

Given a maximal ideal $\mathbf{m} \in \mathrm{Specmax}(A)$, a valuation ring R with maximal ideal $m(R)$ is **centered at $\mathbf{m}$** if $A \subseteq R \subseteq \mathrm{Frac}(A)$ and $\mathbf{m} = m(R) \cap A$. A valuation v is centered at $\mathbf{m}$ if its valuation ring is centered at $\mathbf{m}$. We denote by W_A the family of all valuation rings centered at maximal ideals of A. The henselisation of a

[3]More generally, the problem of the decidability of any complete theory T, that is a theory such that for any formula φ either φ or $\neg\varphi$ belongs to T (and not both!), reduces to finding a recursive axiomatization. This is no longer true for arbitrary (non complete) theories, as example 2.3 shows.

valuation ring R is denoted by R^h. The **Jacobson radical** $J(A)$ is the intersection of all the maximal ideals of A.

A p-valuation is a valuation v on a field of characteristic 0, whose residue field is a finite extension of the finite field $\mathbb{F}_p$ with p elements and whose value group admits a least strictly positive element e (in additive notation) such that $0 < v(p) = n.e$ for some integer n. It is said to be of rank 1 if its residue field is $\mathbb{F}_p$ and $v(p) = e$. It is **p-adically closed** if it is henselian and its value group Γ is a $\mathbb{Z}$-group, that is Γ is elementarily equivalent to the ordered group $\mathbb{Z}$. A recursive axiomatization of $\mathbb{Z}$-groups is given by the formulas saying that they are linearly ordered abelian groups Γ having a smallest strictly positive element such that for every integer n, $\Gamma/n\Gamma$ has exactly n elements. A **p-adically closed field** is a field having a p-adically closed valuation. We refer the reader to [**PR84**] for the model theory of p-valued fields (of arbitrary finite rank).

The classical examples of fields satisfying a Local-Global Principle play an important role in this paper. A field K is said to be:

- PAC or pseudo algegraically closed, if K is regularly closed with respect to $\emptyset$, or equivalently to $\{\tilde{K}\}$ or to $\{K^s\}$.
- PRC or pseudo real closed, if K is regularly closed with respect to the family of all real closed fields between K and $\tilde{K}$. Observe that PAC fields are exactly those PRC fields which admit no order.
- PpC or pseudo p-adically closed, if K is regularly closed with respect to the family of all p-adically closed fields of rank 1 between K and $\tilde{K}$.
- PC$_M$ or pseudo M-adically closed, if K is regularly closed with respect to the family of all p-adically closed fields of rank 1 between K and $\tilde{K}$, with p ranging over a finite set of primes M.

Those classes of fields have been exhaustively studied. They form the background for the recent research on rings with a LGP. Their model theoretic study has always consisted of strengthening their LGP's in order to provide a recursive axiomatization of these classes and then classifying those fields inside the same class up to elementary equivalence. This classification involves certain invariants, mostly the absolute Galois group, a boolean algebra encoding the way in which the different topologies involved interact one with each other, and the **algebraic part** $\mathrm{Alg}(K)$ of a field K defined as the set of elements of K which are algebraic over its prime subfield. As we will see, this approach remains the guiding line when exploring the model theory of rings with a LGP.

PART I: ALGEBRA

4. Rumely

Given any finite place v in a number field K let us denote by K_v the completion of K and $\mathcal{O}_v$ the complete valuation ring of K_v. As usual $\tilde{\mathcal{O}}_v$ denotes the integral closure of $\mathcal{O}_v$ in the algebraic closure $\tilde{K}_v$ of K_v. Since $\mathcal{O}_v$ is known to be henselian, $\tilde{\mathcal{O}}_v$ is a valuation ring.

Let V be a variety defined over K, and for each place v of K (finite or not) let B_v be a non-empty open subset of $V(\tilde{K}_v)$ in the v-topology. We suppose that each B_v is stable under $G(K_v)$ and that there is some affine open $W \subseteq V$ defined over K such that for all but finitely many v, $W(\tilde{\mathcal{O}}_v) \subseteq B_v$.

THEOREM 4.1. *Fix a place v_0 of K. Then there exists a point $\zeta \in V(\tilde{K})$ such that for every $v \neq v_0$ all the conjugates of ζ over K belong to B_v.*

In [**Rum86**], Rumely based the proof of this theorem on the beautifull capacity theory that he developed in [**Rum89**]. He then deduced the following consequences.

COROLLARY 4.2. *A variety V defined over K has a point integral over $\mathbb{Z}$ if and only if it has a point in $\tilde{\mathcal{O}}_v$ for every finite place v of K.*

Observe that by the density theorem, the above corollary applies as well with V replaced by any affine open subset, and in particular by V°. This theorem can be restated in the following equivalent form.

COROLLARY 4.3. *A variety V defined over $\tilde{\mathbb{Q}}$ has a smooth point in $\tilde{\mathbb{Z}}$ if and only if it has a smooth point in every localization of $\tilde{\mathbb{Z}}$. In other words $\tilde{\mathbb{Z}}$ satisfies the main LGP.*

The same statement is true for $\widetilde{\mathbb{F}_p[T]}$, cf. next section, and although it was proved by Rumely only for $\tilde{\mathbb{Z}}$ we will call this statement for $\tilde{\mathbb{Z}}$ and for $\widetilde{\mathbb{F}_p[T]}$ **Rumely's LGP**.

REMARK 4.4. Cantor and Roquette anticipated Rumely's LGP for $\tilde{\mathbb{Z}}$: in [**CR84**] they proved it for unirational varieties.

Combining his LGP with decidability results for valuation rings with algebraically closed fraction fields, Rumely proved a conjecture of J. Robinson:

COROLLARY 4.5. *Hilbert's tenth problem for $\tilde{\mathbb{Z}}$ has a positive solution, in other words the existential theory of the ring $\tilde{\mathbb{Z}}$ is decidable.*

5. Moret-Bailly and Green, Pop, Roquette

The result we report here can take very different forms, depending on the authors. It was first proved by Moret-Bailly [**MB89b**] who also reproved in [**MB89a**] Rumely's density theorem (for $\tilde{\mathbb{Z}}$ and $\widetilde{\mathbb{F}_p[T]}$) without using capacity theory. The purely geometric language of those papers allows one to prove a strong LGP for stacks. On the other hand it is not widely accessible to nongeometers. For this reason it is the version later given by Green, Pop and Roquette in [**GPR95**] which is presented now.

Let K be a global field, that is a finite extension of $\mathbb{Q}$ or $\mathbb{F}_p(T)$. Let Σ be any set of places of K with the sole condition that Σ does not contain all the places of K (like in Rumely's theorem one place must be dismissed). For any $v \in \Sigma$, K_v is the completion of K and B_v its unit ball, that is the set of $z \in K_v$ such that $|z|_v \leq 1$. The unit ball of the algebraic closure $\tilde{K}_v$ of K_v is denoted by $\tilde{B}_v$. If v is a finite place (and only in that case) then B_v is a valuation ring and $\tilde{B}_v$ its integal closure in $\tilde{K}_v$, so this is consistent with our previous notation.

For a nonempty $\mathcal{S} \subseteq \Sigma$ let $K_{\mathcal{S}}$ be the set of **totally $\mathcal{S}$-adic numbers** that is the elements of $\tilde{K}$ which belong to K_v as well as all their conjugates over K, for every $v \in \mathcal{S}$:

$$K_{\mathcal{S}} = \{x \in \tilde{K} \;/\; \forall v \in \mathcal{S}, \forall \sigma \in G(K),\ \sigma(x) \in K_v\}$$

Equivalently $K_{\mathcal{S}}$ is the set of algebraic elements whose minimal polynomial over K totally splits over each K_v, for $v \in \mathcal{S}$. Observe that since the completions are separable extensions of the global fields, $K_{\mathcal{S}}$ is always a separable extension. For this reason we let $K_{\emptyset}$ be the separable closure of K.

Eventually $B_{\Sigma,\mathcal{S}} \subseteq K_{\mathcal{S}}$ denotes the set of elements which belong to B_v as well are all their conjugates over K, for every $v \in \Sigma$.

THEOREM 5.1 (Main theorem). *With the above notations, let V be a variety defined over K and f a tuple of K-rational functions over V. Suppose that:*

1. *For every $v \in \mathcal{S}$ there is $x_v \in V^\circ(B_v)$ such that $f(x_v) \in B_v$.*
2. *For every $v \in \Sigma$ there is $x_v \in V(\tilde{B}_v)$ such that $f(x_v) \in \tilde{B}_v$.*

Then there exists a point $x \in V^\circ(B_{\Sigma,\mathcal{S}})$ such that $f(x) \in B_{\Sigma,\mathcal{S}}$.

The main theorem deals at the same time with characteristic zero and non-zero, with finite and infinite places, with finding points on varieties and dealing with additional conditions on their image by rational functions. For applications to typical examples it is convenient to separate some aspects of the main theorem from others, and for applications to logic to give it the form of a regular closedness property.

DATA 5.2. Of particular interest are the following typical cases:

- $\mathcal{O}$ is a Dedekind domain with fraction field a global field K.
- Σ is the set of all valuations centered at maximal ideals of $\mathcal{O}$, possibly augmented with some real places of K.
- $\mathcal{S}$ is any finite subset of Σ.

Then $B_{\Sigma,\mathcal{S}}$ is contained in the integral closure $\tilde{\mathcal{O}} \cap K_{\mathcal{S}}$ of $\mathcal{O}$ inside $K_{\mathcal{S}}$, and if Σ contains only valuations then $B_{\Sigma,\mathcal{S}} = \tilde{\mathcal{O}} \cap K_{\mathcal{S}}$.

FACT 5.3. *Let w be any finite place of $K_{\mathcal{S}}$, then either the restriction v of w to K belongs to $\mathcal{S}$ and the completion of $K_{\mathcal{S}}$ at w is K-isomorphic to K_v, or $v \notin \mathcal{S}$ and the completion of $K_{\mathcal{S}}$ at w is K-isomorphic to K_v^s. In particular if $\mathcal{S}$ contains only valuations then $K_{\mathcal{S}}$ admits no order.*

Those facts may be proved directly or deduced from the main theorem (5.1). They allow the following formulation of the main theorem.

COROLLARY 5.4. *Assume that in data 5.2 above, Σ contains only valuations. Then the ring $\tilde{\mathcal{O}} \cap K_{\mathcal{S}}$ satisfies the main LGP.*
More generally $\tilde{\mathcal{O}} \cap L$ satisfies the main LGP for every extension L of $K_{\mathcal{S}}$, and so does any ring A such that: $\tilde{\mathcal{O}} \cap L \subseteq A \subseteq L$, and $A \subseteq R$ for every $R \in \mathcal{R}(\tilde{\mathcal{O}} \cap L)$ whose fraction field is not separably closed.

EXAMPLE 5.5. If $\mathcal{O} = \mathbb{Z}$ (then Σ must not contain the real place) and $\mathcal{S}$ is empty, then Rumely's LGP for $\tilde{\mathbb{Z}}$ follows from corollary 5.4.

EXAMPLE 5.6. If $\mathcal{O} = \mathbb{F}_p[T]$ (then Σ must not contain the place at infinity) and $\mathcal{S}$ is empty then the integral closure of $\mathbb{F}_p[T]$ inside any separably closed field, as well as any of its localization by a multiplicative subset, satisfies the main LGP (this is essentially Rumely's LGP in positive characteristic).

EXAMPLE 5.7. The case of the ring of all totally real algebraic integers is special in many ways (see 12.2). It does not fall under the scope of the main theorem since its definition requires one to manipulate simultaneously all the places of $\mathbb{Q}$ (an algebraic number is a totally real integer if and only if it, as well as all its conjugates, lie in $\mathbb{R}$ and in $\tilde{\mathcal{O}}_v$ for every finite place of $\mathbb{Q}$). This is not surprising since the main LGP does not hold for that ring, a counter-example being given by $2x^2 + 3y^2 = 1$. This equation of a smooth curve defined over $\mathbb{Q}$ has solutions in every real closed field as well as in every valuation ring with fraction field $\tilde{\mathbb{Q}}$ (take $(2^{-1/2}, 0)$ or $(0, 3^{-1/2})$ depending on the residual characteristic). It cannot have a solution in totally real algebraic integers because for such a solution (x, y) we would have $x, y \neq 0$ hence $0 < 2x^2 = 1 - 3y^2 < 1$, this holds for every conjugate of x over $\mathbb{Q}$ because x is totally real, hence also for the norm of $2x^2$ over $\mathbb{Q}$ which is an integer since x is integral over $\mathbb{Z}$, a contradiction.

If one finite place is removed, the main theorem (5.1) provides information for many overrings of the totally real algebraic integers.

Corollary 5.8. *The main LGP holds for any integrally closed ring of algebraic numbers, which is not integral over $\mathbb{Z}$ and contains every totally real algebraic integer.*

In particular the field of all totally real algebraic numbers is pseudo real closed, hence so are all its algebraic extensions. Finally the main theorem also implies the following.

Corollary 5.9. *If K is a finite extension of $\mathbb{Q}$ and $\mathcal{S}$ a set of infinite places of K which do not contain at least one infinite place of K, then $K_{\mathcal{S}}$ is pseudo real closed and $\tilde{\mathbb{Z}} \cap K_{\mathcal{S}}$ satisfies the main LGP. The same holds for any integrally closed ring with fraction field algebraic over $K_{\mathcal{S}}$.*

6. Jarden, Razon

Let $\mathcal{O}$ be Dedekind domain with fraction field a global field K. Let $\mathcal{S}$ be a finite set of valuations centered at nonzero prime ideals of $\mathcal{O}$. Let $K_{\mathcal{S}}$ be as in the previous section and $K_{\mathcal{S}}^{ins}$ its maximal purely inseparable algebraic extension.

Jarden and Razon say that a field M between K and $K_{\mathcal{S}}^{ins}$ is **weakly P$\mathcal{S}$C over $\tilde{\mathcal{O}} \cap M$**, the integral closure of $\mathcal{O}$ inside M, if for each absolutely irreducible $h \in M[T, X]$ which is monic in X such that the roots of $h(0, X)$ are distinct and in $K_{\mathcal{S}}^{ins}$, and for each $g \in M[T]$ such that $g(0) \neq 0$, there exists $(a, b) \in (\tilde{\mathcal{O}} \cap M) \times M$ such that $h(a, b) = 0$ and $g(a) \neq 0$.

Remark 6.1. Since h is monic in X and $\tilde{\mathcal{O}} \cap M$ is integrally closed, any such $(a, b) \in (\tilde{\mathcal{O}} \cap M) \times M$ must actually belong to $(\tilde{\mathcal{O}} \cap M) \times (\tilde{\mathcal{O}} \cap M)$.
Observe also that for the same reason $K_{\mathcal{S}}^{ins}$ is always weakly P$\mathcal{S}$C over $\tilde{\mathcal{O}} \cap K_{\mathcal{S}}^{ins}$.

Theorem 6.2 ([**JR98**]). *With the above notation, if M is perfect and weakly P$\mathcal{S}$C over $\tilde{\mathcal{O}} \cap M$ then the main LGP holds for $\tilde{\mathcal{O}} \cap M$. In particular it holds for $\tilde{\mathcal{O}} \cap K_{\mathcal{S}}^{ins}$.*

In [**JR98**] the above theorem was derived from a more precise approximation theorem of local solutions by global ones which generalizes a large part of the main theorem (5.1), the two main restrictions being only that in positive characteristic $K_{\mathcal{S}}^{ins}$ replaces $K_{\mathcal{S}}$ and in characteristic zero infinite places are excluded. However the importance of theorem (5.1) appears when M is not $K_{\mathcal{S}}^{ins}$ but a proper subfield of it, in which case it provides many new examples of rings satisfying the main LGP, which do not fall under the scope of the main theorem (5.1). This is done (see below) by an argument involving the Haar probability measure defined for any profinite group, see [**FJ86**, Chapter 16].

Given a field K and any finite sequence $\sigma = (\sigma_1, \ldots, \sigma_e)$ of K-automorphisms of $\tilde{K}$ (resp. K^s), denote by $\tilde{K}(\sigma)$ (resp. $K^s(\sigma)$) the intersection of the fixed fields of the σ_i's in $\tilde{K}$ (resp. K^s). A property is said to hold **for almost all** σ if it holds for a set of σ of Haar measure 1. For example, Jarden proved in [**Jar72**] that $\tilde{\mathbb{Q}}(\sigma)$ is a PAC field for almost all σ. This result was improved by Jarden and Razon by introducing the following strengthening of the PAC property: a field K is **PAC over a subring** A if and only if for any variety V defined over K and any separable dominating rational map $\varphi : V \to \mathbb{A}^r$ over K where $r = \dim V$, there is a point $x \in V(K)$ such that $\varphi(x) \in A^r$.

THEOREM 6.3 ([**JR94**, Prop. 3.1]). *Let $\mathcal{O}$ be a countable separably Hilbertian domain with fraction field K (for example $\mathcal{O}$ can be any Dedekind domain with fraction field a global field). Then $\tilde{K}(\sigma)$ and $K^s(\sigma)$ are PAC over $\mathcal{O}$ for almost all $\sigma \in G(K)^e$.*

THEOREM 6.4 ([**JR98**]). *With the notation of theorem 6.2, if an algebraic extension M_0 of K is perfect and PAC over $\mathcal{O}$, then $M = M_0 \cap K_{\mathcal{S}}$ is weakly P$\mathcal{S}$C over $\tilde{\mathcal{O}} \cap M$. In particular, the main LGP holds for $\tilde{\mathcal{O}} \cap K^s(\sigma) \cap K_{\mathcal{S}}$ for almost all σ.*

PART II: LOGIC

7. Prestel, Schmid (model-completeness)

Prestel and Schmid defined in [**PS90**] a **radical relation** over a ring A to be a reflexive and transitive binary relation $\leq$ such that for every $a, b, c \in A$:

1. $a \leq b,\ a \leq c \Rightarrow a \leq b + c$.
2. $a \leq b \Rightarrow ac \leq bc$.
3. $1 \leq a,\ 0 \not\leq a$.
4. $a \leq b^2 \Rightarrow a \leq b$.

The typical example of a radical relation is the relation defined, for any given subset $\mathcal{P}$ of the prime spectrum of A, by $a \leq_{\mathcal{P}} b \iff \forall \mathbf{p} \in \mathcal{P}, (a \in \mathbf{p} \Rightarrow b \in \mathbf{p})$. Prestel and Schmid prove that every radical relation is of that kind, by taking for $\mathcal{P}$ the r-closed spectrum (see below). The radical relation $\leq_A$ defined by the maximal spectrum plays a special role (see remark 7.6).

An **r-ring** (resp. **r-domain**), is a ring (resp. domain) with a radical relation $(A, \leq)$. An ideal I of A is r-closed ($\leq$-closed in [**PS90**]) if and only if for every $a, b \in A$:

$$a \in I,\ a \leq b \Rightarrow b \in I$$

The r-closed spectrum $\mathrm{Spec}(A, \leq)$ is the set of r-closed prime ideals. If it contains (0) then $(A, \leq)$ is called an $\mathbf{r}_\circ$**-domain**.

Let $\mathcal{L}_{\mathrm{rad}}$ denote the language of r-rings, that is the language of rings enriched with a binary relation symbol for the radical relation. The **residual (upper semi-) lattice** of an r-ring $(A, \leq)$ is the ordered set canonically associated to the preorder of the radical relation. It is noted $L(A, \leq)$.

THEOREM 7.1. *The theory of r-domains (resp. of $r_\circ$-domains) has a model-companion in $\mathcal{L}_{\mathrm{rad}}$, which is decidable.*

This is obtained by proving that an r-domain (resp. $\mathrm{r}_\circ$-domain) $(A,\leq)$ with fraction field K is relatively existentially closed in every r-domain (resp. $\mathrm{r}_\circ$-domain) if and only if it satisfies the following five conditions:

1. K is algebraically closed.
2. A is a Bezout ring.
3. $A^* = \{a \in A \,/\, a \leq 1\}$
4. $L(A,\leq)$ is dense.
5. Given any variety V defined over K and polynomials g, p_i, q_i with coefficients in A $(0 \leq i \leq s)$, there exists $x \in V(A)$ such that $g(x) \neq 0$ and $p_i(x) \leq q_i(x)$ $(0 \leq i \leq s)$ if and only if the same holds locally everywhere, that is for every $\mathbf{p} \in \mathcal{P}, \mathbf{p} \neq (0)$ (where $\mathcal{P}$ defines $\leq$) there exists a smooth point $x_\mathbf{p} \in V^\circ(A_\mathbf{p})$ such that $g(x_\mathbf{p}) \neq 0$ and $p_i(x_\mathbf{p}) \leq q_i(x_\mathbf{p})$ $(0 \leq i \leq s)$.

Theorem 7.1 then says that the class of r-domains satisfying these properties is elementary. Applying this to decidability requires the study of elementary equivalence.

THEOREM 7.2. *Two r-domains (resp. $\mathrm{r}_\circ$-domains) satisfying the above conditions (1)-(5) are elementarily equivalent if and only if either they have the same positive characteristic, or they have both characteristic zero and their algebraic parts are isomorphic.*

The Local-Global condition (5) above can be derived from Rumely's Local-Global Principle for $\tilde{\mathbb{Z}}$, hence Prestel and Schmid re-proved after van den Dries the decidability of $\tilde{\mathbb{Z}}$ by mean of theorem 7.2. However their approach provides an intuitive axiomatization of $\tilde{\mathbb{Z}}$ and gives in addition a model completeness result.

THEOREM 7.3. *The ring of all algebraic integers is decidable. Moreover its complete theory in $\mathcal{L}_{\mathrm{rad}}$ ($\tilde{\mathbb{Z}}$ is equipped with the radical relation defined by its maximal spectrum) is model-complete.*

The same notion was adapted in [**PS91**] to the case of r-domains with a formally real (resp. p-adic) fraction field by replacing conditions (1) and (5) by:

1_r K is real closed.

1_p K is p-adically closed.

5 Given any variety V defined over K and polynomials g, p_i, q_i with coefficients in A $(0 \leq i \leq s)$, there exists $x \in V(A)$ such that $g(x) \neq 0$ and $p_i(x) \leq q_i(x)$ $(0 \leq i \leq s)$ if and only if the same holds locally everywhere, that is for every $\mathbf{p} \in \mathcal{P}, \mathbf{p} \neq (0)$ (where $\mathcal{P}$ defines $\leq$) there exists a smooth point $x_\mathbf{p} \in V^\circ(A_\mathbf{p})$ such that $g(x_\mathbf{p}) \neq 0$ and $p_i(x_\mathbf{p}) \leq q_i(x_\mathbf{p})$ $(0 \leq i \leq s)$, and $V^\circ(K) \neq \emptyset$.

Observe that the original condition (5) is equivalent to the above one when the fraction field is algebraically closed.

THEOREM 7.4. *The class of $\mathrm{r}_\circ$-domains satisying $(1)_r$-(5) (resp.$(1)_p$-(5)) is recursively axiomatizable and model complete. Its theory is the model-companion of $\mathrm{r}_\circ$-domains with a formally real (resp. p-adic) fraction field. Two such $\mathrm{r}_\circ$-domains are elementarily equivalent if and only if their algebraic parts are isomorphic.*

The integral closure of $\mathbb{Z}$ inside any real field, let us write it $\tilde{\mathbb{Z}} \cap \mathbb{R}$, satisfies the above conditions by the main theorem 5.1. The integral closure $\tilde{\mathbb{Z}} \cap \mathbb{Q}_p$ of $\mathbb{Z}$ inside a p-adically closed field of rank one does not so (this is a gap in [**PS91**]) but any of its localizations which is not contained in the p-valuation ring of $\mathbb{Q}_p$ does. From this it follows that:

THEOREM 7.5. *The rings $\tilde{\mathbb{Z}} \cap \mathbb{R}$, $\tilde{\mathbb{Z}} \cap \mathbb{Q}_p[1/p]$ are decidable. Moreover their complete theories in $\mathcal{L}_{\mathrm{rad}}$ (if they are equipped with the radical relation defined by their maximal spectra) are model-complete.*

REMARK 7.6. A fundamental remark accompanying those results is that the radical relation defined by the maximal spectrum of a ring A which we denote by $\leq_A$, is (uniformly) definable by:

$$a \leq_A b \iff \forall c\big((c,b) = 1 \Rightarrow (c,a) = 1\big)$$

where $(x, y) = 1$ stands for the formula $\exists x' \exists y'(xx' + yy' = 1)$. Now, whenever the Local-Global Principle (5) holds, the radical relation is necessarily defined by the maximal spectrum. Hence all the results on elementary equivalence, elementary embeddings and decidability of r-domains apply to their underlying domains.

8. Van den Dries, Macintyre (quantifier elimination)

A **good Rumely domain** is a domain A with fraction field K satisfying the following conditions:

Ru1: K is algebraically closed.
Ru2: Every finitely generated ideal of R is principal
Ru3: Any smooth curve $\mathcal{C}$ defined over K has a point in A if and only if it has points in $(1/a)A$ and $(1/b)A$ for some $a, b \in A$ such that $aA + bA = A$.
Ru4: For all $a, b \in A \setminus \{0\}$ there are elements a_1, b_1 in A such that $a = a_1 b_1$, $a_1 A + bA = A$ and $b \in J(b_1 A)$.
Ru5: Every nonzero nonunit in R is a product of two relatively prime nonunits.
Ru6: $R \neq K$ and R has Jacobson radical 0.

It can be proved that good Rumely domains are exactly the domains A which satisfy the main LGP, have an algebraically closed fraction field, a dense residual lattice and a zero Jacobson radical $J(A) = \{0\}$. In particular $\tilde{\mathbb{Z}}$ and $\mathbb{F}_p[T]$ are good Rumely domains, as well as many of their localizations (not all, because of the two last conditions).

THEOREM 8.1. *The class of good Rumely domains is recursively axiomatizable.*

The study of those rings by van den Dries and Macintyre then entail a quantifier elimination theorem for good Rumely domains, in the following language.

Given any two ideals I_1, I_2 of a ring A, let $I_1 : I_2$ be the ideal $\{a \in A \,/\, aI_2 \subseteq I_1\}$ and $J(I_1)$ be the Jacobson radical of I_1 that is the intersection of all the maximal ideals containing I_1.

$\mathcal{L}_{\mathrm{DM}}$ is the language of rings $\{0, 1, +, .\}$ augmented by relation symbols $rad_{k,l}$ of arity $(2k + 2l)$ for all $k, l \in \mathbb{N}^*$, to be interpreted for elements $a_1, \ldots, a_k, b_1, \ldots, b_k$, $c_1, \ldots, c_l, d_1, \ldots, d_l$ in any ring as follows:

$$rad_{k,l}(a_1, \ldots, a_k, b_1, \ldots, b_k, c_1, \ldots, c_l, d_1, \ldots, d_l)$$

$$\iff (a_1 A : b_1 A) \cap \cdots \cap (a_k A : b_k A) \subseteq J\big((c_1 A : d_1 A) + \cdots + (c_l A : d_l A)\big)$$

Note that $rad_{k,l}$ is definable in the language of rings.

THEOREM 8.2 (Quantifier Elimination).

1. *One can effectively construct for any $\mathcal{L}_{\mathrm{DM}}$-formula $\Phi(Y)$ a positive integer $N(\Phi)$ such that the equivalence $\Phi(Y) \leftrightarrow \bigvee_{i=1}^{r} \Phi_i(Y)$ holds for every good*

Rumely domain of characteristic 0 *and of characteristic* $p > N(\Phi)$, *where each* $\Phi_i(Y)$ *is of the form:*

$$\exists T\big(T^e + p_1(Y)T^{e-1} + \cdots + p_e(Y) = 0 \wedge \chi(Y,T)\big)$$

with $p_j \in \mathbb{Z}[Y]$ *and* $\chi(Y,T)$ *is a quantifier free* $\mathcal{L}_{\mathrm{DM}}$*-formula.*

2. *One can effectively construct for any prime* p *and any* $\mathcal{L}_{\mathrm{DM}}$*-formula* $\Phi(Y)$ *an equivalence* $\Phi(Y) \leftrightarrow \bigvee_{i=1}^{r} \Phi_i(Y)$ *true in every good Rumely domain of characteristic* p, *where each* $\Phi_i(Y)$ *is of the form:*

$$\exists T\big(T^e + p_1(\varphi^{-d}(Y))T^{e-1} + \cdots + p_e(\varphi^{-d}(Y)) = 0 \wedge \chi(Y,T)\big)$$

with $p_j \in \mathbb{Z}[Y]$ *and* $\chi(Y,T)$ *is a quantifier free* $\mathcal{L}_{\mathrm{DM}}$*-formula (here* φ *is the Frobenius map* $(z_1,\ldots,z_n) \mapsto (z_1^p,\ldots,z_n^p)$ *and* φ^{-d} *is the inverse of* φ^d, $d \in \mathbb{N}$*).*

This theorem has the following consequences for decidability.

THEOREM 8.3.

1. *The theory of good Rumely domains is decidable.*
2. *The theory of good Rumely domains of characteristic* $p > 0$ *is complete.*
3. *Two good Rumely domains of characteristic* 0 *are elementarily equivalent if and only if their algebraic parts are isomorphic.*
4. *The rings* $\tilde{\mathbb{Z}}$, $\widetilde{\mathbb{F}_p[T]}$ *are decidable.*

A somewhat surprising consequence of the above axiomatization underlined by their authors, is that $\widetilde{\mathbb{F}_p[T]}$ is elementarily equivalent with any of its localizations which satisfies conditions Ru4 and Ru5 (or equivalently with a dense residual lattice, in the terminology of Prestel and Schmid), although most of those rings are not isomorphic.

The quantifier elimination theorem also implies a sort of asymptotic completeness result, analogous to the celebrated transfer principle of Ax-Kochen (see [**Koc75**]).

THEOREM 8.4. *Given a sentence* Φ *(in the language of rings or in* $\mathcal{L}_{\mathrm{DM}}$*) one can construct a finite set of primes* $P(\Phi)$ *such that the theory* $T_{P(\Phi)}$ *of good Rumely domains in which every* $p \in P(\Phi)$ *is invertible, proves* Φ *or* $\neg\Phi$.

Van den Dries introduced in [**Dri88**] the notion of **algebraic boundedness** which goes as follows: a domain A is algebraically bounded if and only if for each definable $S \subseteq A^{m+1}$ there are polynomials $f_1,\ldots,f_r \in A[X_1,\ldots,X_m,Y]$ such that for every $x \in A^m$ if $S_x = \{y \in A \,/\, (x,y) \in S\}$ is finite then for some $i \le r$ we have $f_i(x,Y) \ne 0$ and $S_x \subseteq \{y \in R \,/\, f_i(x,y) = 0\}$. The importance of this notion is that the *algebraic dimension* defined for arbitrary definable sets over an algebraically bounded domain is well behaved, cf. [**Dri88**, §3, Theorem (4.15)]. Moreover, for rings integral over $\mathbb{Z}$, algebraic boundedness is closely related to decidability, cf. [**Dri88**, Proposition 3.2].

THEOREM 8.5. *Every good Rumely domain is algebraically bounded.*

9. Ershov (boolean families)

The material of this section is covered in a series of papers from [**Ers92b**] to [**Ers99**] (and a few others we do not mention). That is to say that a short summary of this more than one hundred and fifty pages can not be exhaustive.

Let W be any family of valuation rings with fraction field K. This family is equipped with the topology defined by taking $D(X) = \{R \in W \,/\, X \subseteq R\}$ for any finite subset X of K as an open basis. If $X = \{x_1, \dots, x_n\}$ we write simply $D(x_1, \dots, x_n)$ for $D(X)$. Then W is a **boolean family** if this topology makes it a boolean space (compact, totally disconnected) and if for any boolean combination B of basic opens there is an $x \in K$ such that $B = D(x)$.

Ershov introduced this definition and proved that if W is boolean then it can be recovered from its holomorphy ring $A_W = \cap W$ since then $W = W_A := \{A_{\mathbf{m}} \,/\, \mathbf{m} \in \mathrm{Specmax}(A)\}$. Moreover he characterized those rings A which are the holomorphy rings of boolean families as the **regularly Prüfer domains**, that is the Prüfer domains such that $A/J(A)$ is a von Neumann regular ring (then W_A is boolean and $A = A_{W_A}$). Hence the data of such a domain is equivalent to the data of a boolean family of valuation rings on its fraction field.

Ershov then says that $(K, W) \in RC^*$ (resp. $(K, W) \in RC$) if W is boolean and A_W (resp. K) is regularly closed relatively to the family $\mathcal{R}(W) = \{R^h \,/\, R \in W\}$ (resp. to $\mathcal{F}(W) = \{\mathrm{Frac}(R^h) \,/\, R \in W\}$). Hence $(K, W) \in RC^*$ is the same as saying that A_W is a regularly Prüfer domain satisfying the main LGP. A pair (K, W) is **maximal** if there is no proper algebraic extension L of K such that for every $R \in W$ the field L embeds over K into $\mathrm{Frac}(R^h)$.

THEOREM 9.1 ([**Ers94b**]). *The class of pairs (K, A_W) such that $(K, W) \in RC^*$ is recursively axiomatizable in the language of fields enriched with a unitary predicate symbol for A_W.*

This elementary class is much too large for general decidability results. In particular it contains the class of pairs (K, K) such that K is PAC, and the theory of PAC fields is known to be hereditary undecidable. However it is natural to extend to RC^* the classical results of the model theory of henselian valued fields, and specially the fundamental Ax-Kochen-Ershov theorems.

Remember that a valuation v is **absolutely unramified** if v is defined over a field of characteristic 0 and either its residue field has characteristic 0, or it is a p-valuation of rank 1 for some p. Ax-Kochen-Ershov theorems apply primarily to absolutely unramified valuations (although many generalizations have been achieved). For an arbitrary domain A with fraction field K let $k_A = A/J(A)$ and $\Gamma_A = K^*/A^*$ ordered by $xA^* \leq yA^* \iff xy^{-1} \in A$. Observe that if A is a valuation ring, which is a particular case of a regularly Prüfer domain, then k_A is its residue field and Γ_A with this order is its value group. There are natural diagonal embeddings of k_A (resp. Γ_A, with its order) in $\prod k_{A_{\mathbf{m}}}$ (resp. $\prod \Gamma_{A_{\mathbf{m}}}$, with the product order) those products being taken as $\mathbf{m}$ ranges over the maximal spectrum of A. Denote by RC^*_E the class of pairs $(K, W) \in RC^*$ such that the above diagonal embeddings turn k_{A_W} and Γ_{A_W} into elementary products [4] of the $k_{\mathbf{m}}$'s and $\Gamma_{\mathbf{m}}$'s respectively. Ershov gives in [**Ers94a**, Thm. 1] a natural characterization of RC^*_E as those pairs $(K, W) \in RC^*$ such that [5] for every formula φ in the language of valued fields with parameters in A_W, if $(\mathrm{Frac}(R^h), R^h) \models \varphi$ for some $R \in W$ then the same holds for every R' in a neighborhood of R inside W.

[4] See [**BW79**] or [**Ers94a**, section 2] for the definition of boolean product, elementary product and $\exists$-product.

[5] This property is called by Ershov "continuity of local elementary properties". In every theorem of decidability based on LGP a similar property is used, explicitly or not. However it can take many different forms.

THEOREM 9.2 ([**Ers94a**]). *The class of pairs* (K, A_W) *such that* $(K, W) \in RC_E^*$ *is recursively axiomatizable in the language* $\mathcal{L} \cup \{A\}$ *of fields enriched with a unary predicate symbol for* A_W. *So is the subclass* mRC_E^* *of maximal such pairs*[6].

THEOREM 9.3 (Generalization of Ax-Kochen-Ershov, [**Ers94a**]). *Let* $(K, A_W) \subseteq (K', A_{W'})$ *be two such pairs which are maximal (the inclusion of pairs means that* $K \subseteq K'$ *and* $A_W = A_{W'} \cap K$, *in other words it is an inclusion of* $(\mathcal{L} \cup \{A\})$*-structures). Assume that* W, W' *contain only absolutely unramified valuation rings and*[7] $J(A_W) = J(A_{W'}) \cap A_W$. *Then:*

$$(K, A_W) \preceq (K', A_{W'}) \iff \begin{cases} k_{A_W} \preceq k_{A_{W'}} \\ \Gamma_{A_W} \preceq \Gamma_{A_{W'}} \end{cases}$$

9.1. RC_π**-fields.** This approach specializes to several remarkable subclasses of RC^*-fields. For example let K be a field and choose $\pi \in K \setminus \{0,1\}$. Call π-valuations the valuations v whose value group has a least positive element (with additive notation) equal to $v(\pi)$. Call v a $\pi_{\mathbb{Z}}$-valuation if in addition its value group is a $\mathbb{Z}$-group. Denote by W_π (resp. $W_{\pi_{\mathbb{Z}}}$) the family of all π-valuation rings (resp. $\pi_{\mathbb{Z}}$-valuation rings) of K. The family W_π is boolean [**Ers92a**, Prop. 8]. Call K an RC_π**-field** (resp. $RC_{\pi_{\mathbb{Z}}}$-field) if $(K, W_\pi) \in RC$ (resp. $(K, W_{\pi_{\mathbb{Z}}}) \in RC$).

THEOREM 9.4 ([**Ers92b**]). *Let* $\mathcal{L}_\pi$ *be the language of fields enriched with a new constant symbol. With the above notation,* $(K, W_\pi) \in RC$ *if and only if* $(K, W_\pi) \in RC^*$, *and in that case* A_{W_π} *is (uniformly) definable in* K, *with only* π *as parameter. In particular, by theorem 9.1 the class of* RC_π*-fields is recursively axiomatizable in the language* $\mathcal{L}_\pi$.

For $RC_{\pi_{\mathbb{Z}}}$-fields things go even better: first $(K, W_{\pi_{\mathbb{Z}}}) \in RC$ if and only if $W_{\pi_{\mathbb{Z}}} = W_\pi$ and $(K, W_\pi) \in RC$, cf. [**Ers92b**, Thm. 5]. So the class of $RC_{\pi_{\mathbb{Z}}}$-fields is contained in the class of RC_π-field, and it proves to be recursively axiomatizable in the language $\mathcal{L}_\pi$. If K is an $RC_{\pi_{\mathbb{Z}}}$-field for some $\pi \in K \setminus \{0,1\}$ then the set of $\pi' \in K \setminus \{0,1\}$ such that K is also an $RC_{\pi'_{\mathbb{Z}}}$-field is definable in K and moreover $W_\pi = W_{\pi'}$. By combining all this Ershov proves:

THEOREM 9.5 ([**Ers93**]). *The class* $RC_{\mathbb{Z}}$ *of fields* K *which are* $RC_{\pi_{\mathbb{Z}}}$*-fields for some* $\pi \in K \setminus \{0,1\}$ *is recursively axiomatisable in the language of rings.*

$RC_{\mathbb{Z}}$ is a huge elementary class which contains among others all the pseudo p-adically closed fields which are not PAC (for any p) and their generalization to finitely many values of p ranging over a finite set M, the PC_M fields. Its model theoretic properties (elementary equivalence, elementary embeddings and so on) are studied in [**Ers93**]. These properties are extended by Ershov to the following remarkable subclasses of $RC_{\mathbb{Z}}$.

9.2. Nice Local-Global fields. Ershov calls a valuation ring **quasiclassical** if it has characteristic zero, its value group is a $\mathbb{Z}$-group and either it is p-adic of rank one (that is a π-valuation with $\pi = p$ having the finite field with p elements as residue field) or its residue field is a pseudo finite field of characteristic zero. He then defines the class $NLGF$ of **nice local-global fields** as the class of fields K such that:

[6] An axiomatization of maximal RC_π fields is given in [**Ers93**]. Ershov simply mentions in [**Ers94a**] that the same is true for mRC_E^*.

[7] This last assumption is always satisfied when $(K, A_W) \preceq (K', A_{W'})$ since the Jacobson radical of a ring is uniformly definable.

1. The family W_{qc} of all quasiclassical valuation rings of K is boolean.
2. $(K, W_{qc}) \in RC^*_E$.

If K is a nice local-global field then $W_{qc} = W_\pi$ for some $\pi \in K \setminus \{0,1\}$ hence $NLGF \subseteq RC_{\mathbb{Z}}$. Conversely if W is a boolean family of absolutely unramified valuation rings with fraction field K (of characteristic 0) such that $(K, W) \in RC_{\mathbb{Z}}$ and k_{A_W} is an $\exists$-product in the axiomatic closure of the class of all finite fields, then $W = W_{qc}$ and $(K, W_{qc}) \in RC^*_E$, that is $K \in NLGF$. Combining this with previous axiomatizations proves that the class of nice local-global fields is recursively axiomatizable in the language of fields, cf. [**Ers96b**].

Remark 9.6. The class of pseudo finite fields is the smallest elementary class which contains every finite fields. By analogy it is natural to expect $NLGF$ to be the smallest elementary class containing all the the PC_M fields for every finite set M of primes. This is indeed the case, following a communication of Ershov during the conference.

Decidability results can then be obtained for various subclasses of NLGF defined by conditions on the absolute Galois group. The Δ^*-group associated to $(K, W) \in RC^*_E$ is the pair $(G(K), \mathcal{D}_W)$ where $G(K)$ is the absolute Galois group of K and $\mathcal{D}_W$ is the family of all subgroups of $G(K)$ which are the decomposition group of some $R \in W$ in the algebraic closure of K. There is a category of Δ^*-groups whose morphisms preserves the natural (continuous) action of $G(K)$ over $\mathcal{D}_W$. The definitions of **free** and of **universal** Δ^*-groups can be expressed in terms of universal problems in this category. For shortness we won't give those definitions here and refer the reader to [**Ers95, Ers96a**].

Theorem 9.7 ([**Ers96b, Ers96c**]). *The class of nice local-global fields with universal Δ^*-group (resp. a free Δ^*-group, resp. which are maximal) is recursively axiomatizable in the language of fields, and its theory is decidable.*

Theorem 9.8 ([**Ers96c, Ers97**]).

1. *Let K, K' be nice local-global fields with universal Δ^*-group (resp. with free Δ^*-group, resp. which are maximal). Let A, A' be their holomorphy rings and suppose that K' is a regular extension of K, $A = A' \cap K$ and $J(A) = J(A') \cap A$. Then:*
$$K \preceq K' \iff k_A \preceq k_{A'} \text{ and } \Gamma_A \preceq \Gamma_{A'}.$$
2. *Let K, K' be nice local-global fields with free Δ^*-group (resp. universal Δ^*-group). Then $K \equiv K'$ if and only if the algebraic parts of their holomorphy rings A, A' are isomorphic and $k_A \equiv k_{A'}$, this last elementary equivalence holding in the language of rings enriched with constant symbols for the elements of the image of $\mathrm{Alg}(A)$ in k_A (resp. of $\mathrm{Alg}(A')$ in $k_{A'}$), those two rings being identified with a common subring of k_A and $k_{A'}$ through the isomorphism induced by $\mathrm{Alg}(A) \simeq \mathrm{Alg}(A')$).*

Remark 9.9. In the maximal case, the above theorem 9.8 was handled by Ershov under more general assumptions in [**Ers93**]. Namely it holds for the class of maximal $RC_{\mathbb{Z}}$ fields K such that if W denotes the (unique) family of valuation rings of K such that $(K, W) \in RC_{\pi_{\mathbb{Z}}}$ for some $\pi \in K \setminus \{0,1\}$, every element of W is absolutely unramified, and $(K, W) \in RC^*_E$. Certain natural elementary subclasses of this larger class were also proved to have decidable theories.

Although all this can be considered as rather abstract, Ershov uses it in order to obtain decidability results for very concrete fields (and rings, cf. section 10). Let M be a finite nonempty set of primes, and denote by $\mathbb{Q}^M$ the field of totally M-adic algebraic integers, that is those algebraic integers whose minimal polynomial over $\mathbb{Q}$ splits into linear factors over $\mathbb{Q}_p$ for every $p \in M$. Then $\mathbb{Q}^M$ is a nice local-global field, and a theorem of Pop [**Pop96**] asserts that it has a free Δ^*-group. Moreover, if N is another set of primes non disjoint from M such that $M \not\subseteq N$ and $N \not\subseteq M$, the compositum $\mathbb{Q}^M\mathbb{Q}^N$ has a universal Δ^*-group.

THEOREM 9.10 ([**Ers96b**]). *With the above notation, $\mathbb{Q}^M$ is decidable, and so is $\mathbb{Q}^M\mathbb{Q}^N$ (provided $M \cap N \neq \emptyset$).*

10. Darnière and Ershov (main LGP)

A ring A satisfies the **relative LGPH** (LGPH* for short) if and only if it is a domain, given any non zero element a of A the set of all maximal ideals of A which do not contain a is compact and for every variety V defined over the fraction field K of A:

$$V^\circ(A) \neq \emptyset \quad \iff \quad \begin{cases} V^\circ(K) \neq \emptyset \text{ which we call condition } (*), \\ \forall R \in W_A,\ V^\circ(R^h) \neq \emptyset. \end{cases}$$

A satisfies the **Local-Global Principle with respect to Henselizations** (LGPH for short) if condition $(*)$ is removed from the above definition. Hence LGPH is a combination of a geometric LGP with an additionnal condition on the topology of the maximal spectrum. It is actually equivalent to the main LGP (with only henselian closures) plus various conditions, including being an nrp-ring in the sense of [**Ers99**].

The author introduced LGPH/LGPH* in his doctoral thesis [**Dar98**] as a common framework in which the model-theoretic work reported in the previous sections of this paper could be developped more uniformly and systematically in new directions. Ershov was independently lead to closely related considerations in [**Ers99**], which we present at the end of this section.

THEOREM 10.1. *The class of rings satisfying LGPH/LGPH* is elementary.*

Let $\mathcal{L}^r_{\mathrm{rad}}$ be the language of r-rings $\mathcal{L}_{\mathrm{rad}}$ enriched with r unitary predicate symbols to be interpreted by r-closed ideals. Let $T_1, \ldots, T_r$ be theories taken among the theory of non trivial valuation rings with separably closed fraction fields or the theories of valuation rings whose value groups and residue fields satisfy given inductive theories. Let Σ be the class of $\mathcal{L}^r_{\mathrm{rad}}$-structures $(A, \leq, I_1, \ldots, I_r)$ such that:

1. A satisfies the LGPH.
2. $\leq$ is defined by the maximal spectrum of A.
3. For every $k \leq r$, I_k is a nonzero proper r-closed ideal of $(A, \leq)$ such that for any maximal ideal $\mathbf{m}$ of A containing I_k: $A^h_{\mathbf{m}} \models T_k$, and $I_l \not\subseteq \mathbf{m}$ for every $l \neq k$.
4. $A^h_{\mathbf{m}}$ has a separably closed fraction field, for any maximal ideal $\mathbf{m}$ of A not containing any of the I_k's.

An element $(A, \leq, I_1, \ldots, I_r)$ of Σ is called **maximal** if in addition for any proper algebraic extension L of the fraction field of A there is some $k \leq r$ and some maximal ideal $\mathbf{m}$ of A containing I_k such that for any valuation ring R with fraction field L extending $A_{\mathbf{m}}$ (that is $R \cap K = A_{\mathbf{m}}$) $R^h \not\models T_k$. The **enriched lattice** of an element of Σ is the lattice $L(A, \leq)$ *equipped with the images of the* I_k*'s* by the canonical projection from A onto $L(A, \leq)$.

THEOREM 10.2. *The class Σ is recursively axiomatizable, as well as the subclass of its maximal elements.*
If $(A, \leq, I_1, \dots, I_r)$ and $(A', \leq', I'_1, \dots, I'_r)$ are two maximal elements of Σ with residual lattices L and L' such that $A \subseteq A'$ and the inclusion preserves the $\mathcal{L}^r_{\mathrm{rad}}$-structure (that is $I_k = I'_k \cap A$ for any $k \leq r$, and $a \leq b \iff a \leq' b$ for any $a, b \in A$) then:

$$(A, \leq, I_1, \dots, I_r) \preceq (A', \leq', I'_1, \dots, I'_r) \iff L \preceq L'.$$

In [**Dar98**] the above theorem was proved in a slightly more general setting, in order to make it easily adaptable to other local theories T_k's. For example it remains true for any complete theory of p-adically closed valuation rings. It was also followed by a similar criterion for elementary equivalence, that we won't reproduce here for shortness, which led to the following application.

THEOREM 10.3. *Let $p_1, \dots, p_r$ be distinct primes, π their product and K be any maximal RC_π field algebraic over $\mathbb{Q}$. Equip the integral closure $\tilde{\mathbb{Z}} \cap K$ of $\mathbb{Z}$ inside K with the radical relation defined by its maximal spectrum and the ideals $I_k = p_k(\tilde{\mathbb{Z}} \cap K)$. Let L be the enriched residual lattice of this structure. Then $\tilde{\mathbb{Z}} \cap K$ is decidable if and only if K and L are decidable.*

The author has to confess that he does not know why in [**Dar98**, section V.6] this theorem which follows immediatly from [**Dar98**, cor. V.5.4] is stated only in the particular case of a RC_π-field having for each $k \leq r$ a unique p_k-valuation. Maybe because he was mostly motivated by the following application:

THEOREM 10.4. *The integral closure of $\mathbb{Z}$ inside $\mathbb{Q}_p$ is decidable.*

Theorem 10.2 can be found only in [**Dar98**]. However a more direct proof of the above application to the decidability of the p-adic algebraic integers can be found in [**Dara**]. Similarly the following results which slightly improve those of [**Dar98**] will appear in [**Darb**].

Let us call a domain A a **PAC* domain** if it satisfies LGPH* and the fraction field of the henselization of $A_{\mathbf{m}}$ is separably closed, for every nonzero maximal ideal of A. For such a domain it is equivalent to satisfy LGPH or to have a PAC fraction field, in which case we call it a **PAC domain**. We say that a field K is **restricted RC-local** if it is regularly closed relatively to the family of all its real closures and p-adic closures (possibly of rank > 1) and if any elementary extension of K remains so. This includes PAC fields, PRC fields, PpC and PC_M fields. Moreover it allows bounded ramification on the p-adic closures. PAC* domains with restricted RC-local fraction fields, and among them PAC domains, have very nice model-theoretic properties.

Given a domain A equipped with a radical relation, we denote by $\mathrm{Alg}(A, \leq)$ the r-domain $\mathrm{Alg}(A)$ equipped with the restriction of the radical relation of A. Its residual lattice is denoted by $\mathrm{Alg}(L(A, \leq))$. When $B \subseteq A$ and B is equipped with a radical relation which coincides with the restriction of the radical relation of A, then $L(B, \leq)$ can be naturally identified with a sublattice of $L(A, \leq)$. Similarly, any isomorphism between two r-domains (that is an isomorphism of rings wich preserves the radical realtion) induces an isomorphism of their residual lattices.

THEOREM 10.5. *Let A, A' be PAC* domains with restricted RC-local fraction fields K and K' respectively. Equip them with the radical relations defined by their maximal spectra and let L, L' be the corresponding residual lattices. Assume that $J(A) = (0) \iff J(A') = (0)$.*

1. *Suppose $A \subseteq A'$, then $A \preceq A'$ if and only if the restriction to A of the radical relation of A' coincides with the radical relation of A and:*
$$\begin{cases} K \preceq K' \\ L \preceq L' \end{cases}$$
2. *If K (or K') has positive characteristic p, then $A \equiv A'$ if and only if:*
$$\begin{cases} K \equiv K' \\ L \equiv L' \end{cases}$$
3. *If K, K' have characteristic zero, then $A \equiv A'$ if and only if:*
$$\begin{cases} K \equiv K' \\ \mathrm{Alg}(A, \leq) \simeq \mathrm{Alg}(A', \leq) \text{ and}^{8}\ L \underset{\mathrm{Alg}(L)}{\equiv} L' \end{cases}$$

We turn now to applications of the above to decidability.

THEOREM 10.6. *A PAC domain of positive characteristic is decidable if and only if its fraction field is decidable.*
In particular any integrally closed ring whose fraction field is separably closed and algebraic over $\mathbb{F}_p(t)$ is decidable.

Given a finite family $\mathcal{F}_0$ of fields taken from among $\mathbb{R}$ and the finite extensions of the $\mathbb{Q}_p$'s, let:
$$\mathcal{F} = \{\mathrm{Alg}(F)^\tau \,/\, \tau \in G(\mathbb{Q}),\ F \in \mathcal{F}_0\}.$$
Define $\mathbb{Q}_\mathcal{F}$ as the field of all algebraic numbers whose minimal polynomial splits into linear factors in $F[X]$ for every $F \in \mathcal{F}_0$ or equivalently:
$$\mathbb{Q}_\mathcal{F} = \bigcap \{F \,/\, F \in \mathcal{F}\}.$$
The integral closure of $\mathbb{Z}$ inside $\mathbb{Q}_\mathcal{F}$ is denoted by $\mathbb{Z}_\mathcal{F}$.

If $\mathcal{F}_0 = \{\mathbb{Q}_p \,/\, p \in M\}$ for a given finite set M of primes, then $\mathbb{Q}_\mathcal{F}$ is exactly what is denoted $\mathbb{Q}^M$ by Ershov in the previous section. If $\mathcal{F}_0 = \{\mathbb{R}\}$ then $\mathbb{Q}_\mathcal{F}$ is exactly the field of all totally real algebraic numbers (see the appendices).

THEOREM 10.7.

1. *If $\mathbb{R} \notin \mathcal{F}_0$ then $\mathbb{Z}_\mathcal{F}$ is decidable if and only if $\mathbb{Q}_\mathcal{F}$ is decidable.*
In particular the integral closure of $\mathbb{Z}$ inside $\mathbb{Q}^M$ is decidable (here we use Ershov's theorem that $\mathbb{Q}^M$ is decidable).
2. *Let $\mathcal{N}$ be any nonempty set of prime numbers. If $\mathcal{F}_0 = \{\mathbb{R}\}$ then $\mathbb{Z}_\mathcal{F}[1/n]_{n \in \mathcal{N}}$ is decidable if and only if $\mathcal{N}$ is recursive (here we use* **[FHV94]***, see theorem 13.1 below).*

[8] This last condition reads "L is elementarily equivalent to L' over $\mathrm{Alg}(L)$" in other words L and L' are elementarily equivalent in the language of lattices enriched with constant symbols which parametrize the elements of $\mathrm{Alg}(L)$. Indeed, since $\mathrm{Alg}(A, \leq) \simeq \mathrm{Alg}(A', \leq)$ their residual lattices $\mathrm{Alg}(L)$ and $\mathrm{Alg}(L')$ are isomorphic, hence $\mathrm{Alg}(L)$ can be considered as a common sublattice of L and L'.

Remark 10.8. In both cases in the above theorem, a relative decidability is proved: a certain ring is decidable if and only if its fraction field is decidable. Nothing is assumed on the decidability of the fraction field but of course it is expected to be decidable, otherwise this relative result would be of little interest. This is the case for $\mathbb{Q}^M$ and the field of all totally real algebraic numbers.

The attentive reader may have noticed that since $\mathbb{Z}_\mathcal{F}$ is not at all a PAC* domain, it is a little bit surprising that the above result follows from theorem 10.5. This is due to a simple trick, namely that $\mathbb{Z}_\mathcal{F}$ is definable inside $\mathbb{Z}_\mathcal{F}[1/p]_{p\in M}$, and this last ring is indeed PAC*.

10.1. Near regularly Prüfer domains. As already mentioned in the beginning of this section, Y. Ershov has introduced in his recent paper [**Ers99**] a generalization of regularly Prüfer rings he calls near regularly Prüfer (studied independently in [**Dar98**] under the name of locally complemented Prüfer domains) which allows him to deal with larger families of valuation rings than only the boolean ones. The results related to decidability which are handled by Y. Ershov and by the author are:

1. LGPH is recursively axiomatizable.
2. Given a finite set M of primes, the integral closure of $\mathbb{Z}$ inside $\mathbb{Q}^M$ is decidable.

In addition to this Ershov proved the following (which for simplicity we present in our terminology):

Theorem 10.9 (Ershov). *The theory* $\mathrm{K_{Ru}}$ *(resp.* $\mathrm{K_{Ru,0}}$, $\mathrm{K_{Ru,p}}$*) of PAC rings with an algebraically closed fraction field (resp. of characteristic* 0*, of characteristic* p*) is decidable.*
$\mathrm{K_{Ru,0}}$ *(resp.* $\mathrm{K_{Ru,p}}$*) is exactly the theory of those integrally closed ring whose fraction field is the algebraic closure of* $\mathbb{Q}$ *(resp. of* $\mathbb{F}_p(T)$*).*

11. Razon (probabilistic decidability)

Let $\mathcal{O}$ be a Dedekind domain with Jacobson radical the zero ideal, and $K = \mathrm{Frac}(\mathcal{O})$ a global field. Let μ be the Haar measure on the absolute Galois group $G(K)$ of K. Razon introduces in [**Raz95**, pp 4-5] the notion of **effectively computable domain**, which extends [**FJ86**, Def. 17.1]. This technical definition allows one to speak more precisely about primitive recursive decidability for theories in $\mathcal{L}(\mathcal{O})$. The rings $\mathbb{Z}$, $\mathbb{F}_p[T]$ and their fraction fields are effectively computable domains, and so are their localizations by many (not all) multiplicative sets.

Theorem 11.1 ([**Raz95**], pp 86-87). *Given a sentence* θ *in the language of rings with parameters in* $\mathcal{O}$*, let* $S(e,\theta)$ *be the set of elements* σ *of* $G(K)^e$ *such that* $\tilde{\mathcal{O}}(\sigma) \models \theta$*, where* $\tilde{\mathcal{O}}(\sigma)$ *denotes the integral closure of* $\mathcal{O}$ *inside the field* $\tilde{K}(\sigma)$ *(see section 6).*

1. $\mu(S(e,\theta))$ *is a rational number. If* $\mathcal{O}$ *is effectively computable and* θ *is explicitly given, then* $\mu(S(e,\theta)$ *can be effectively (that is primitive recursively) computed.*
2. *If* $\mathcal{O}$ *is effectively computable then the ring* $\tilde{\mathcal{O}}$ *is decidable. Moreover its theory is primitive recursive.*
3. *Let* $\mathrm{Almost}(\mathcal{O},e)$ *be the set of sentences* θ *such that* $\mu(S(e,\theta)) = 1$*. If* $\mathcal{O}$ *is effectively computable then* $\mathrm{Almost}(\mathcal{O},e)$ *is primitive recursive.*

Razon also introduced independently of the author a notion of PAC domains, which can be defined as the PAC domains in our sense, see section 10, whose residual lattice (associated to the radical relation defined by the maximal spectrum) is dense. In order to avoid confusions we will call them **Razon domains** in this section. This notion combined with PAC fields over subrings introduced by Jarden and Razon, cf. section 6, gives an explicit recursive axiomatization of the theory $\mathrm{Almost}(\mathbb{Z}, e)$.

THEOREM 11.2 ([**Raz97**]). *A ring A models* $\mathrm{Almost}(\mathbb{Z}, e)$ *if and only if:*

- *A is a Razon domain with a zero Jacobson radical.*
- *Any element of A which is algebraic over $\mathbb{Q}$ is integral over $\mathbb{Z}$.*

APPENDICES

12. From Julia Robinson to Rumely via ... Kronecker!

Contrary to the case of $\tilde{\mathbb{Z}}$, it is well known that the integral closure of $\mathbb{Z}$ inside any finite extension of $\mathbb{Q}$ is undecidable (see [**Rob64a**] for a short presentation of this). A celebrated result of Julia Robinson concerns the integral closure of $\mathbb{Z}$ inside totally real fields, not necessarily finite over $\mathbb{Q}$. She calls such a ring a totally real algebraic integer ring and writes $a \ll b$ when $a \leq b$ for every order.

THEOREM 12.1 (J. Robinson). *The natural numbers can be defined arithmetically in any totally real algebraic integer ring A such that there is a smallest interval $[0, s[$ with s real or ∞, which contains infinitely many complete conjugate sets of numbers of A, i.e. infinitely many $x \in A$ with $0 \ll x \ll s$.*
In particular such a ring is undecidable.

From this she deduced one of her most famous results:

COROLLARY 12.2 (J. Robinson). *The ring of all totally real algebraic integers is undecidable.*

In [**Rob64a**] this corollary follows immediatly from theorem 12.1 by applying a result of Kronecker: in [**Kro57**] he explicitly described all the real algebraic integers in $[-2, 2]$. From this description it follows immediatly that $[0, s[$ contains infinitely many complete conjugate sets of algebraic integers if and only if $s \geq 4$.

Kronecker's theorem inspired many people to generalize it to arbitrary real intervals (Pólya, Schur, R.M. Robinson) and to other subsets of $\mathbb{C}$. Fekete placed the problem in proper perspective by introducing the transfinite diameter of a compact $E \subseteq \mathbb{C}$:

$$\gamma(E) = \lim_{n \to \infty} \max_{\{z_1, \ldots, z_n\} \subseteq E} \left(\prod_{i \neq j} |z_i - z_j| \right)^{1/(n^2 - n)}$$

THEOREM 12.3 (Fekete, Szegö). *Let $E \subseteq \mathbb{C}$ be a compact set, stable under complex conjugation.*

1. *If $\gamma(E) < 1$ then there is some neighborhood of E which contains only finitely many complete conjugate sets of algebraic integers.*
2. *If $\gamma(E) \geq 1$ then every neighborhood of E contains infinitely many such sets.*

Knowing that the transfinite diameter of a real interval $[a, b]$ is $(b-a)/4$, the connection with Kronecker's theorem becomes clear. For a complete genealogy of the Fekete-Szegö's theorem see [**Rob64b**].

It is precisely a generalization of the Fekete-Szegö theorem that motivated Rumely in developing his fascinating capacity theory [**Rum89**], and it is from this generalization that he deduced in [**Rum86**] his LGP for $\tilde{\mathbb{Z}}$. We conclude that, surprisingly enough, the undecidability of the ring of all totally real algebraic integers and the decidability of the ring of all algebraic integers have a common origin which is the above mentioned theorem of Kronecker.

13. More about the totally real algebraic numbers

We already noticed that the ring of all totally real algebraic integers is different in many ways from the other examples of "large" rings integral over $\mathbb{Z}$ which occur in most of the results surveyed in this paper: the main LGP doesn't hold for it (example 5.7) and it is undecidable (theorem 12.2). On the other hand, its fraction field is not so bad:

THEOREM 13.1 (Fried, Haran, Völklein). *The field of all totally real algebraic numbers is decidable.*

Since this field is known to be pseudo real closed by the main theorem, its decidability is deduced in [**FHV94**] from a very deep investigation on its absolute Galois group. So the ring of all totally real algebraic integers is an example of an undecidable ring whose fraction field is decidable, a situation which is rather exceptionnal for a ring integral over $\mathbb{Z}$. Moreover many of its overrings are decidable, as (2) of theorem 10.7 shows.

References

[BW79] S. Burris and H. Werner, *Sheaf constructions and their elementary properties*, Trans. Amer. Math. Soc. **248** (1979), no. 2, 269–309.

[CR84] D. Cantor and P. Roquette, *On diophantine equations over the ring of all algebraic integers*, J. Number Theory **18** (1984), 1–26.

[Dara] L. Darnière, *Nonsingular Hasse principle for rings*, to appear in J. reine und angew. Math.

[Darb] L. Darnière, *Pseudo algebraically closed rings*, to appear in Manuscripta Math.

[Dar98] L. Darnière, *étude modèle-théorique d'anneaux satisfaisant un principe de hasse non singulier*, Phd thesis, Université de Rennes 1, January 1998.

[Dri88] L. van den Dries, *Elimination theory for the ring of algebraic integers*, J. reine und angew. Math. **388** (1988), 189–205.

[Ers92a] Y.-L. Ershov, *Boolean families of valuation rings*, Algebra and Logic **31** (1992), no. 3, 170–181.

[Ers92b] Y.-L. Ershov, *Relative regular closeness and π-valuations*, Algebra and Logic **31** (1992), no. 6, 342–360.

[Ers93] Y.-L. Ershov, *Maximal RC_π-fields*, Algebra and Logic **32** (1993), no. 5, 267–278.

[Ers94a] Y.-L. Ershov, *Fields with continuous local elementary properties I*, Algebra and Logic **33** (1994), no. 6, 351–365.

[Ers94b] Y.-L. Ershov, *RC^*-fields*, Algebra and Logic **33** (1994), 205–215.

[Ers95] Y.-L. Ershov, *Fields with continuous local elementary properties II*, Algebra and Logic **34** (1995), no. 3, 140–146.

[Ers96a] Y.-L. Ershov, *Free Δ^*-groups*, Algebra and Logic **35** (1996), no. 2, 86–95.

[Ers96b] Y.-L. Ershov, *Nice local-global fields I*, Algebra and Logic **35** (1996), no. 4, 229–235.

[Ers96c] Y.-L. Ershov, *Nice local-global fields II*, Algebra and Logic **35** (1996), no. 5, 281–295.

[Ers97] Y.-L. Ershov, *Nice local-global fields III*, Siberian Math. J. **38** (1997), no. 3, 449–454.

[Ers99] Y.-L. Ershov, *Near regularly Prüfer rings*, Siberian Adv. Math. **9** (1999), no. 1, 1–45.

[FHV94] M. Fried, D. Haran, and H. Völklein, *Real hilbertianity and the field of totally real numbers*, Contemporary Mathematics **74** (1994), 1–34.

[FJ86] M. Fried and M. Jarden, *Field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer-Verlag, 1986.

[GPR95] B. Green, F. Pop, and P. Roquette, *On Rumely's local-global principle*, Jber. d. Dt. Math-Verein **97** (1995), 43–74.

[Gre66] M. Greenberg, *Rational points in Henselian discrete valuation rings*, Inst. Hautes Études Sci. Publ. Math. (1966), no. 31, 59–64.

[Hod97] W. Hodges, *A shorter model theory*, Cambridge University Press, 1997.

[Jar72] Moshe Jarden, *Elementary statements over large algebraic fields*, Trans. Amer. Math. Soc. **164** (1972), 67–91.

[JR94] M. Jarden and A. Razon, *Pseudo algebraically closed fields over rings*, Israel J. Math. **86** (1994), 25–59.

[JR98] M. Jarden and A. Razon, *Rumely's local global principle for algebraic PSC fields over rings*, Trans. Amer. Math. Soc. **350** (1998), no. 1, 55–85.

[Koc75] S. Kochen, *The model theory of local fields*, ISILC Logic Conference, Kiel, 1974, Lecture Notes in Math., vol. 499, 1975, pp. 384–425.

[Kro57] L. Kronecker, *Zwei sätze über gleichungen mit ganzzahligen coefficienten*, J. reine und angew. Math. **53** (1857), 173–75.

[Lan51] S. Lang, *On quasi algebraic closure*, Ann. of Math. **55** (1951), 373–390.

[MB89a] L. Moret-Bailly, *Groupes de Picard et problèmes de Skolem I*, Ann. scien. Ec. Norm. Sup **22** (1989), no. 4, 181–194.

[MB89b] L. Moret-Bailly, *Groupes de Picard et problèmes de Skolem II*, Ann. scien. Ec. Norm. Sup **22** (1989), no. 4, 181–194.

[Pop96] F. Pop, *Embedding problems over large fields*, Ann. of Math. (2) **144** (1996), no. 1, 1–34.

[PR84] A. Prestel and P. Roquette, *Formally p-adic fields*, Lecture Notes in Math., vol. 1050, Springer-Verlag, 1984.

[PS90] A. Prestel and J. Schmid, *Existentially closed domains with radical relations*, J. reine und angew. Math. **407** (1990), 178–201.

[PS91] A. Prestel and J. Schmid, *Decidability of the rings of real algebraic and p-adic algebraic integers*, J. reine und angew. Math. **414** (1991), 141–148.

[Raz95] A. Razon, *Primitive recursive decidability for large rings of algebraic integers*, Phd thesis, Tel Aviv, 1995.

[Raz97] A. Razon, *Existentially closed r-domains in regular extensions*, preprint 8, Institut für Experimentelle Mathematik, Universität GH Essen, 1997.

[Rob64a] J. Robinson, *On the decision problem for algebraic rings*, Studies in mathematical analysis and related topics, Stanford Univ. Press, 1964, pp. 297–304.

[Rob64b] R. M. Robinson, *Intervals containing infinitely many sets of conjugate algebraic integers*, Studies in mathematical analysis and related topics, Stanford Univ. Press, 1964, pp. 305–315.

[Rum86] R. Rumely, *Arithmetic over the ring of all algebraic integers*, J. reine und angew. Math. **368** (1986), 127–133.

[Rum89] R. Rumely, *Capacity theory of algebraic curves*, Lecture Notes in Math., vol. 1378, Springer-Verlag, 1989.

Département de Mathématiques, UFR Sciences, Université d'Angers, 2 Bd Lavoisier, 49000 Angers, France

E-mail address: Luck.Darniere@univ-angers.fr