Glasgow Math. J.: page 1 of 6. © The Author(s) 2020. Published by Cambridge University Press on behalf of Glasgow Mathematical Journal Trust.
doi:10.1017/S001708952000018X.

PRIMITIVE RECURSIVE DECIDABILITY FOR THE RING OF INTEGERS OF THE COMPOSITUM OF ALL SYMMETRIC EXTENSIONS OF $\mathbb{Q}$

MOSHE JARDEN
Tel Aviv University, Tel Aviv, Israel
e-mail: jarden@tauex.tau.ac.il

and AHARON RAZON
Elta Systems Ltd, Ashdod, Israel
e-mail: razona@elta.co.il

In memory of Wulf-Dieter Geyer (1939–2019)

(Received 23 January 2019; revised 25 November 2019; accepted 8 April 2020)

Abstract. Let $\mathbb{Q}_{\mathrm{symm}}$ be the compositum of all symmetric extensions of $\mathbb{Q}$, i.e., the finite Galois extensions with Galois group isomorphic to S_n for some positive integer n, and let $\mathbb{Z}_{\mathrm{symm}}$ be the ring of integers inside $\mathbb{Q}_{\mathrm{symm}}$. Then, Th($\mathbb{Z}_{\mathrm{symm}}$) is primitive recursively decidable.

2010 *Mathematics Subject Classification*. 12E30.

Introduction Let $\mathcal{O}$ be a Dedekind domain with a trivial Jacobson radical and with a global field of quotients K. Let K_{symm} be the compositum of all symmetric extensions of K, i.e., finite Galois extensions with symmetric Galois groups, let $K_{\mathrm{symm,ins}}$ be the maximal purely inseparable extension of K_{symm}, and let $\mathcal{O}_{\mathrm{symm,ins}}$ be the integral closure of $\mathcal{O}$ in $K_{\mathrm{symm,ins}}$. Denote the language of rings extended with a constant symbol for each element of $\mathcal{O}$ by $\mathcal{L}$(ring, $\mathcal{O}$).

With these notations, our main result, Theorem 4.3, states that the elementary theory of the ring $\mathcal{O}_{\mathrm{symm,ins}}$ in the language $\mathcal{L}$(ring, $\mathcal{O}$) is primitive recursively decidable if $\mathcal{O}$ is an effective computability domain (Definition 1.3). The latter condition holds in particular for $\mathcal{O} = \mathcal{O}_0$, where $\mathcal{O}_0 = \mathbb{Z}$ or $\mathcal{O}_0 = \mathbb{F}_p[t]$, and also for $\mathcal{O} = S_0^{-1}\mathcal{O}_0$, where S_0 is a presented multiplicative subset of $\mathcal{O}_0$ (Definition 1.3) and either $S_0 = \mathcal{O}_0 \setminus \{0\}$ (in which case $\mathcal{O} = K$) or S_0 is relatively prime to infinitely many irreducible elements of $\mathcal{O}_0$.

The primitive recursive decidability of $\mathcal{O}_{\mathrm{symm,ins}}$ relies among others on the fact that K_{symm} is pseudo algebraically closed (PAC) over its ring of integers $\mathcal{O}_{\mathrm{symm}}$ (Definition 2.1) and on the isomorphism of the absolute Galois group Gal(K_{symm}) of K_{symm} to $\hat{F}_\omega$ (Remark 2.4). That K_{symm} is PAC over $\mathcal{O}_{\mathrm{symm}}$ follows from a series of three papers of the authors, the first two with Wulf-Dieter Geyer, [**4**], [**5**], and [**9**]. The first paper applies Konrad Neumann's theorem on the "symmetric stabilization of function fields over K" [**12**]. The second one relies on a work of Moret-Bailly on Skolem problems [**11**].

The property of K_{symm} of being PAC over $\mathcal{O}_{\mathrm{symm}}$ implies that $\mathcal{O}_{\mathrm{symm}}$ satisfies "Rumely's local-global principle" [**5**, Prop. 13.4]. That principle has stimulated numerous developments in model theory, especially decidability results for those rings (see the survey paper of L. Darnière [**1**]). The first result, due to v.d. Dries [**2**], extends $\mathcal{L}$(ring, $\mathbb{Z}$) with "radical

relations" to a language $\mathcal{L}_{\mathrm{rad}}(\mathbb{Z})$ and establishes a recursive elimination of quantifiers procedure for the ring of all algebraic integers $\tilde{\mathbb{Z}}$ in that language. In particular, $\tilde{\mathbb{Z}}$ is decidable. In order to apply Rumely's local-global principle, one has to decompose algebraic sets defined over an integral domain R which contains K into irreducible varieties, and to do it uniformly with respect to all homomorphisms of R into an algebraic closure $\tilde{K}$ of K. For this purpose, v.d. Dries applies a compactness argument of model theory, so his elimination of quantifiers is not primitive recursive.

The work [**13**] replaces v.d. Dries compactness argument by an application of the Bertini–Noether theorem and establishes a primitive recursive elimination of quantifiers procedure for the integral closure $\tilde{\mathcal{O}}$ of $\mathcal{O}$ in $\tilde{K}$ in the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$. In particular, $\tilde{\mathcal{O}}$ is primitive recursively decidable. The elimination procedure works over each ring of integers $\mathcal{O}_M$ of a perfect algebraic extension M of K which is *Frobenius over* $\mathcal{O}_M$. This means that M is PAC over $\mathcal{O}_M$ and $\mathrm{Gal}(M)$ has the *embedding property* (Remark 2.4). In order for the elimination procedure to be primitive recursive, the set $\mathrm{Im}(\mathrm{Gal}(M))$ of all finite quotients of $\mathrm{Gal}(M)$ should be primitive recursive. Using the assumption that M is Frobenius over $\mathcal{O}_M$, [**13**] generalizes the primitive recursive procedure via Galois stratification [**3**, Section 30] to a primitive recursive procedure of radical Galois stratification. The latter allows us to eliminate quantifiers from formulas of the language $\mathcal{L}_{\mathrm{rad}}(\mathcal{O})$.

The assumption that $\mathcal{O}$ is an effective computability domain is needed in order to have a primitive recursive procedure to factor ideals in the ring of integers of a global field into products of prime ideals [**13**, Appendix A]. Another auxiliary tool that our elimination procedure applies is a local elimination procedure. More precisely, it uses elimination of quantifiers for the theory of valuation domains which are not fields but with algebraically closed quotient field in the language of rings with a binary relation symbol for divisibility. [**13**, Appendix B] is an elaboration of Weispfenning's primitive recursive procedure [**14**] for that theory.

Lemma 3.1 of this work states that $K_{\mathrm{symm,ins}}$ is Frobenius over $\mathcal{O}_{\mathrm{symm,ins}}$ and the set $\mathrm{Im}(\mathrm{Gal}(K_{\mathrm{symm,ins}}))$ is primitive recursive. This allows us to apply [**13**, Corollary 3.29] to the field $K_{\mathrm{symm,ins}}$. By [**6**, Lemma 8.1], the set $\mathrm{Root}(K_{\mathrm{symm,ins}})$ of monic polynomials in $K[X]$ that have roots in $K_{\mathrm{symm,ins}}$ is primitive recursive. Following an argument that appears in [**10**, Lemma 3.3], we conclude that $\mathrm{Th}(\mathcal{O}_{\mathrm{symm,ins}})$ is primitive recursive.

Note that $\mathrm{Th}(\mathcal{O}_{\mathrm{symm,ins}})$ being decidable (as opposed to primitive recursively decidable) is a new result, since it depends on the recent results that $\mathrm{Th}(K_{\mathrm{symm,ins}})$ is decidable [**6**, Theorem 8.5] and that K_{symm} satisfies Rumely's local-global principle [**9**, Theorem 4.4]. Using these results, among others, one can use other techniques (see [**1**]) than the primitive recursive one we used in this paper [**13**, Corollary 3.29] to prove that $\mathrm{Th}(\mathcal{O}_{\mathrm{symm,ins}})$ is decidable.

The authors are indebted to the anonymous referee for his helpful comments.

1. Effective computability domain. The Jacobson radical of a commutative ring with a unit is the intersection of all maximal ideals of the ring. The Jacobson radical of a field is defined to be zero.

We use the following data throughout this work.

DATA 1.1. We use the terminology of [**3**, p. 404, Definition 19.1.1 and the discussion that follows] and consider a presented Dedekind domain $\mathcal{O}$ with zero Jacobson radical. Then, we present its quotient field K, as usual, as the field of equivalent classes of pairs (a, b) with $a, b \in \mathcal{O}$ and $b \neq 0$ with the usual equivalent relation. In this way, $\mathcal{O}$ turns out

to be a primitive recursive subset of K, so, in the above terminology, $\mathcal{O}$ is presented in K. Note, for example, that this does not mean that $\mathbb{Z}$ is a primitive recursive subset of $\mathbb{Q}$ in the usual language of rings, which is still a known open question.

Then, the algebraic closure $\tilde{K}$ of K is a presented field with elimination theory [3, p. 413, Lemma 19.4.1]. Also, the integral closure $\tilde{\mathcal{O}}$ of $\mathcal{O}$ in $\tilde{K}$ is presented in $\tilde{K}$ because for each $x \in \tilde{K}$, we can compute $f(X) = \mathrm{irr}(x, K)$ and check if all its coefficients belong to $\mathcal{O}$; if so, then $x \in \tilde{\mathcal{O}}$, otherwise $x \notin \tilde{\mathcal{O}}$.

DEFINITION 1.2. [13, Definition 1.3]. A commutative domain R is an *Euclidean ring* if there exists a function

$$\delta : R \setminus \{0\} \to \mathbb{N}$$

which satisfies that for each $a, b \in R \setminus \{0\}$, $\delta(ab) = \delta(a)\delta(b)$ and there exist $c, r \in R$ such that $a = bc + r$ and $\delta(r) < \delta(b)$ or $r = 0$. We also define $\delta(0) = 0$.

If in addition R satisfies that for each $n \in \mathbb{N}$, the set $\{a \in R \mid \delta(a) \leq n\}$ is finite, then R is an *Euclidean ring of finite type*.

For example, $\mathbb{Z}$ with $\delta(a) = |a|$ and $\mathbb{F}_p[t]$ with $\delta(g(t)) = c^{\deg(g)}$, where $2 \leq c \in \mathbb{N}$ is a fixed constant, are Euclidean rings of finite type.

A Euclidean ring is in particular a principal ideal domain, hence a unique factorization domain.

A Euclidean ring of finite type R is *presented* if it satisfies the following conditions:

(a) R is a presented ring [3, p. 404, Definition 19.1.1].
(b) For each $n \in \mathbb{N}$, the finite set $\{a \in R \mid \delta(a) \leq n\}$ is given explicitly.
(c) The set of the irreducible elements of R is a primitive recursive subset of R which is given explicitly. Also, each element of R can be written effectively as a product of irreducible elements of R (up to an invertible element of R).
(d) The function δ is presented, and we can effectively perform division with a remainder as above.
In particular, we can effectively find, using Euclid's algorithm, a greatest common divisor of two elements in R.

Note that the Euclidean rings $\mathbb{Z}$ and $\mathbb{F}_p[t]$ are presented.

DEFINITION 1.3. [13, Definition 1.4]. We say that the ring $\mathcal{O}$ is an *effective computability domain* if $\mathcal{O}$ is presented in K and $\mathcal{O} = S_0^{-1}\mathcal{O}_0$, where $\mathcal{O}_0$ is a presented Euclidean domain of finite type and S_0 is a presented multiplicative subset of $\mathcal{O}_0$ by a set of generators that consists of explicitly given irreducible elements of $\mathcal{O}_0$. Thus, we can effectively perform calculations in $\mathcal{O}$.

Note that for $S_0 = \mathcal{O}_0 \setminus \{0\}$, we get $\mathcal{O} = K$. Also, the Jacobson radical of $\mathcal{O}$ is zero if and only if $\mathcal{O} = K$ or S_0 is disjoint from an infinite subset of irreducible elements of $\mathcal{O}_0$.

2. Frobenius fields over subrings.

Recall that a field M is *pseudo algebraically closed* (it PAC) if every absolutely integral variety V defined over M has an M-rational point. The field M may have a stronger property with respect to a subset:

DEFINITION 2.1. [8, Definition 1.1]. Let R be a subset of a field M. We say that M is *PAC over* R if for every absolutely integral variety V of dimension $r \geq 0$ and for each dominating separable rational map $\varphi : V \to \mathbb{A}^r$ over M (i.e., the corresponding function fields extension is finite separable) there exists $\mathbf{a} \in V(M)$ such that $\varphi(\mathbf{a}) \in R^r$.

Note that if S is a subring of M which contains R, then M is also PAC over S.

As in the case of PAC fields, it suffices to check the condition of Definition 2.1 only for plane curves:

REMARK 2.2. [8, Lemma 1.3]. Let R be a subring of a field M. Then, the following condition is necessary and sufficient for M to be PAC over R:

For each absolutely irreducible polynomial $f \in M[T, X]$ such that $\frac{\partial f}{\partial X} \neq 0$ and for each $0 \neq g \in M[T]$, there exists $(a, b) \in R \times M$ such that $f(a, b) = 0$ and $g(a) \neq 0$. □

LEMMA 2.3. *[8, Corollary 2.5]. Let M be a PAC field over a subring R with quotient field M_0. Let N_0 be an algebraic extension of M_0 and let S be the integral closure of R in N_0. Then $N = N_0M$ is PAC over S.*

REMARK 2.4. For a profinite group G, we set $\mathrm{Im}(G)$ to be the set of all finite quotients of G. We say that G has the *embedding property* if for every epimorphism $\alpha : B \to A$ with $B \in \mathrm{Im}(G)$ and every epimorphism $\varphi : G \to A$ there exists an epimorphism $\gamma : G \to B$ such that $\alpha \circ \gamma = \varphi$ [3, p. 564, Definition 24.1.2]. Finally, we write $\hat{F}_\omega$ for the free profinite group with countably many generators and note that by [3, p. 568, Lemma 24.3.3], $\hat{F}_\omega$ has the embedding property. □

DEFINITION 2.5. [13, Definition 3.1]. Let R be a subring of a field M. We say that M is a *Frobenius field over R* if M is PAC over R and the absolute Galois group $\mathrm{Gal}(M)$ of M has the embedding property.

Note that if M is algebraically closed, then M is Frobenius over each subring. More examples can be found in [9, 13]: Let e be a positive integer. Then, for all $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$, but a set of Haar measure 0 of $\mathrm{Gal}(K)^e$, the fixed field $K_{\mathrm{sep}}(\boldsymbol{\sigma}) = \{x \in K_{\mathrm{sep}} \mid \sigma_i(x) = x, i = 1, \ldots, e\}$ is Frobenius over $\mathcal{O}$ and the Galois closure, $K_{\mathrm{sep}}[\boldsymbol{\sigma}]$, of K inside $K_{\mathrm{sep}}(\boldsymbol{\sigma})$ is Frobenius over the integral closure of $\mathcal{O}$ inside $K_{\mathrm{sep}}[\boldsymbol{\sigma}]$.

3. Compositum of symmetric extensions. Let F be a field. A *symmetric extension* of F is a finite Galois extension of F with Galois group isomorphic to S_n for some positive integer n. Let F_{symm} be the compositum of all symmetric extensions of F. We denote the maximal purely inseparable extension of F by F_{ins}.

A field F is *Hilbertian* if each separable Hilbert set of F is nonempty [3, Section 12.1, p. 219]. A major theorem in field arithmetic states that if F is a countable PAC Hilbertian field, then $\mathrm{Gal}(F) \cong \hat{F}_\omega$ [7, Section 5.10].

Let $\mathcal{O}_{\mathrm{symm,ins}}$ be the integral closure of $\mathcal{O}$ in $K_{\mathrm{symm,ins}}$.

LEMMA 3.1. *$K_{\mathrm{symm,ins}}$ is Frobenius over $\mathcal{O}_{\mathrm{symm,ins}}$ and the set $\mathrm{Im}(\mathrm{Gal}(K_{\mathrm{symm,ins}}))$ is primitive recursive.*

Proof. By [9, Corollary 2.5], K_{symm} is PAC over the integral closure $\mathcal{O}_{\mathrm{symm}}$ of $\mathcal{O}$ in K_{symm}. Hence, by Lemma 2.3, $K_{\mathrm{symm,ins}}$ is PAC over $\mathcal{O}_{\mathrm{symm,ins}}$.

By [3, p. 396, Theorem 18.10.4], K_{symm} is PAC and Hilbertian. Since K is global, K is countable. By [7, p. 89, Theorem 5.10.2(c)], $\mathrm{Gal}(K_{\mathrm{symm}}) \cong \hat{F}_\omega$. Since $K_{\mathrm{symm,ins}}/K_{\mathrm{symm}}$ is a purely inseparable extension, we also have $\mathrm{Gal}(K_{\mathrm{symm,ins}}) \cong \hat{F}_\omega$. By Remark 2.4, $\mathrm{Gal}(K_{\mathrm{symm,ins}})$ has the embedding property. Since the set $\mathrm{Im}(\hat{F}_\omega)$ consists of all finite groups, it is primitive recursive.

Hence, by Definition 2.5, $K_{\mathrm{symm,ins}}$ is Frobenius over $\mathcal{O}_{\mathrm{symm,ins}}$. □

For an algebraic extension M of K, we let $\mathrm{Root}(M/K)$ be the set of monic polynomials in $K[X]$ with roots in M. By [**6**, Lemma 8.1]:

LEMMA 3.2. *The set* $\mathrm{Root}(K_{\mathrm{symm,ins}}/K)$ *is primitive recursive.*

4. Primitive recursive decidability. Denote the language of rings extended with constant symbol for each element of $\mathcal{O}$ by $\mathcal{L}(\mathrm{ring}, \mathcal{O})$. If R is a ring extension of $\mathcal{O}$, we write $\mathrm{Th}(R)$ for the set of all first order sentences in $\mathcal{L}(\mathrm{ring}, \mathcal{O})$ that are true in R.

For an algebraic extension M of K, we denote by $\mathcal{O}_M$ the integral closure of $\mathcal{O}$ in M. The following lemma is [**13**, Corollary 3.29].

LEMMA 4.1. *Let* $\mathcal{H}$ *be a family of finite groups that contains the trivial group and let* θ *be a sentence in the language* $\mathcal{L}(\mathrm{ring}, \mathcal{O})$. *Then, there exists a finite Galois extension* L *of* K, *and there exists a conjugacy domain* Con *of* $\mathrm{Gal}(L/K)$ *with groups that belong to* $\mathcal{H}$ *such that the following statement holds:*

For every perfect algebraic extension M *of* K *which is Frobenius over* $\mathcal{O}_M$ *and with* $\mathrm{Im}(\mathrm{Gal}(M)) = \mathcal{H}$, *we have*

$$\mathcal{O}_M \models \theta \Leftrightarrow \mathrm{Gal}(L/L \cap M) \in \mathrm{Con}.$$

Moreover, if $\mathcal{O}$ *is an effective computability domain,* $\mathcal{H}$ *is primitive recursive, and* θ *is presented, then we can effectively construct* L *and* Con.

The following Lemma is an adjustment of [**10**, Lemma 3.3].

LEMMA 4.2. *Suppose that* $\mathcal{O}$ *is an effective computability domain and let* M *be an algebraic extension of* K. *Suppose that* M *is perfect and Frobenius over* $\mathcal{O}_M$, $\mathrm{Im}(\mathrm{Gal}(M))$ *is primitive recursive, and* $\mathrm{Root}(M/K)$ *is primitive recursive. Then* $\mathrm{Th}(\mathcal{O}_M)$ *is primitive recursively decidable.*

Proof. Let θ be an effectively given sentence of $\mathcal{L}(\mathrm{ring}, \mathcal{O})$ and let $\mathcal{H} = \mathrm{Im}(\mathrm{Gal}(M))$. By Lemma 4.1, we can effectively construct a finite Galois extension L of K and a conjugacy domain Con of $\mathrm{Gal}(L/K)$ which consists of groups that belong to $\mathcal{H}$ such that $\mathcal{O}_M \models \theta$ if and only if $\mathrm{Gal}(L/L \cap M) \in \mathrm{Con}$.

We effectively compute $z_1, \ldots, z_n$ in L such that $K(z_1), \ldots, K(z_n)$ are all of the subfields of L that contain K. Since $\mathrm{Root}(M/K)$ is primitive recursive, we can effectively check for each $1 \leq i \leq n$ whether the polynomial $\mathrm{irr}(z_i, K)$ has a root in M, that is whether $K(z_i)$ has a K-embedding into M. Doing that, we effectively find $1 \leq j \leq n$ such that $K(z_j)$ has a K-embedding into M, but no proper extension of $K(z_j)$ in L has a K-embedding into M. Thus, $K(z_j)$ is K-conjugate to $L \cap M$. Finally, we effectively check whether $\mathrm{Gal}(L/K(z_j))$ belongs to Con, hence whether $\mathrm{Gal}(L/L \cap M)$ belongs to Con in order to primitive recursively decide whether $\mathcal{O}_M \models \theta$. □

With this, we reach our main result.

THEOREM 4.3. *Suppose that the ring* $\mathcal{O}$ *introduced in Data 1.1 is an effective computability domain. Then, the theory* $\mathrm{Th}(\mathcal{O}_{\mathrm{symm,ins}})$ *is primitive recursive.*

Proof. By Lemma 3.1, $K_{\mathrm{symm,ins}}$ is Frobenius over $\mathcal{O}_{\mathrm{symm,ins}}$ and $\mathrm{Im}(\mathrm{Gal}(K_{\mathrm{symm,ins}}))$ is primitive recursive. By Lemma 3.2, the set $\mathrm{Root}(K_{\mathrm{symm,ins}}/K)$ is primitive recursive. Hence, by Lemma 4.2, $\mathrm{Th}(\mathcal{O}_{\mathrm{symm,ins}})$ is primitive recursive. □

REFERENCES

1. L. Darnière, Decidability and local-global principles, in *Hilbert's tenth problem: relations with arithmetic and algebraic geometry* (Denef, J., Lipshitz, L., Pheidas, T. and Geel, J. V., Editors), Contemporary Mathematics, vol. 270 (AMS, Providence, 2000), 145–167.

2. L. van den Dries, Elimination theory for the ring of algebraic integers, *J. Reine Angew. Math.* **388** (1988), 189–205.

3. M. Fried and M. Jarden, *Field Arithmetic*, 3rd edition, Ergebnisse der Mathematik, vol. **11** (Springer, Heidelberg, 2008).

4. W.-D. Geyer, M. Jarden and A. Razon, On stabilizers of algebraic function fields of one variable, *Adv. Geom.* **17**(2) (2017), 131–174.

5. W.-D. Geyer, M. Jarden and A. Razon, Strong approximation theorem for absolutely integral varieties over P$\mathcal{S}$C Galois extensions of global fields, *N.Y. J. Math.* **23** (2017), 1447–1529.

6. W.-D. Geyer, M. Jarden and A. Razon, Composita of symmetric extensions of $\mathbb{Q}$, *Münster J. Math.* **12** (2019), 139–161.

7. M. Jarden, *Algebraic Patching*, Springer Monographs in Mathematics (Springer, Heidelberg, 2011).

8. M. Jarden and A. Razon, Pseudo algebraically closed fields over rings, *Isr. J. Math.* **86** (1994), 25–59.

9. M. Jarden and A. Razon, Strong approximation theorem for absolutely integral varieties over the compositum of all symmetric extensions of a global field, *Glasgow Math. J.* **61** (2018), 373–380.

10. M. Jarden and A. Shlapentokh, Decidable algebraic fields, *J. Symbolic Logic* **82** (2017), 474–488.

11. L. Moret-Bailly, Groupes de Picard et problémes de Skolem II, *Annales Scientiques de l'Ecole Normale Superieure* **22**(4) (1989), 181–194.

12. K. Neumann, Every finitely generated regular field extension has a stable transcendence base, *Isr. J. Math.* **104** (1998), 221–260.

13. A. Razon, Primitive recursive decidability for large rings of algebraic integers, *Albanian J. Math.* **13**(1) (2019), 3–93.

14. V. Weispfenning, Quantifier elimination and decision procedure for valued fields, in *Models and Sets*, LNM, vol. 1103 (Springer Verlag, Heidelberg, 1984), 419–472.