The Diophantine problem in the classical matrix groups

Alexei G. Myasnikov[*], Mahmood Sohrabi[†]

1 Introduction

In this paper we study the Diophantine problem in the classical matrix groups $GL_n(R), SL_n(R), T_n(R), UT_n(R)$, $n \geq 3$, over associative unitary rings R. We show that if $G_n(R)$ is one of these groups then the Diophantine problem in $G_n(R)$ is polynomial time equivalent (more precisely, Karp equivalent) to the Diophantine problem in R. Here for $SL_n(R)$ we assume that R is commutative. Similar results hold for $PGL_n(R)$ and $PSL_n(R)$, provided R has no zero divisors (for $PGL_n(R)$ the ring R is not assumed to be commutative).

Recall that the Diophantine problem (also called the Hilbert's tenth problem or the generalized Hilbert's tenth problem) in a countable algebraic structure $\mathcal{A}$, denoted $\mathcal{D}(\mathcal{A})$, asks whether there exists an algorithm that, given a finite system S of equations in finitely many variables and coefficients in $\mathcal{A}$, determines if S has a solution in $\mathcal{A}$ or not. In particular, if R is a countable ring then $\mathcal{D}(R)$ asks whether the question if a finite system of polynomial equations with coefficients in R has a solution in R is decidable or not. It is tacitly assumed that the ring R comes with a fixed enumeration, i.e., a function $\nu : \mathbb{N} \to R$, which enables one to enumerate all polynomials in the ring of all non-commutative polynomials $R\langle x_1, x_2, \ldots\rangle$ (in countably many variables $x_1, x_2, \ldots$), as well as all finite systems of polynomial equations $p(x_1, \ldots, x_n) = 0$, where $p(x_1, \ldots, x_n) \in R\langle x_1, x_2, \ldots\rangle$, so one can provide them as inputs to a decision algorithm. If the ring R is commutative then by tradition only commutative polynomials from $R[x_1, x_2, \ldots]$ are considered. The original version of this problem was posed by Hilbert for the ring of integers $\mathbb{Z}$. This was solved in the negative in 1970 by Matiyasevich [54] building on the work of Davis, Putnam, and Robinson [17]. Subsequently, the Diophantine problem has been studied in a wide variety of commutative rings R, where it was shown to be undecidable by reducing $\mathcal{D}(\mathbb{Z})$ to $\mathcal{D}(R)$. By definition the Diophantine problem in a structure $\mathcal{A}$ *reduces* to

[*] Address: Stevens Institute of Technology, Department of Mathematical Sciences, Hoboken, NJ 07087, USA. Email: amiasnik@stevens.edu. Supported by NSF Award 1953784

[†] Address: Stevens Institute of Technology, Department of Mathematical Sciences, Hoboken, NJ 07087, USA. Email: msohrab1@stevens.edu

the Diophantine problem in a structure $\mathcal{B}$, symbolically $\mathcal{D}(\mathcal{A}) \leq \mathcal{D}(\mathcal{B})$, if there is an algorithm that for a given finite system of equations S with coefficients in $\mathcal{A}$ constructs a system of equations S^* with coefficients in $\mathcal{B}$ such that S has a solution in $\mathcal{A}$ if and only if S^* has a solution in $\mathcal{B}$. So if $\mathcal{D}(\mathbb{Z}) \leq \mathcal{D}(R)$ then $\mathcal{D}(R)$ is undecidable. If the reducing algorithm is polynomial-time then the reduction is termed polynomial-time (or Karp reduction). Thus, the results above that the Diophantine problems in $G_n(R)$ and R are polynomial time equivalent mean, precisely, that $\mathcal{D}(G_n(R))$ and $\mathcal{D}(R)$ reduce to each other in polynomial time. In particular they are either both decidable or both undecidable. A lot of research has been done on equations in commutative rings. Nevertheless, the Diophantine problem is still open in $\mathbb{Q}$ and fields F which are finite algebraic extensions of $\mathbb{Q}$. Much more is known on the Diophantine problem in the rings of algebraic integers O of the fields F. Namely, it was shown that $\mathcal{D}(\mathbb{Z})$ reduces to $\mathcal{D}(O)$ for some algebraic number fields O, hence in such O the Diophantine problem $\mathcal{D}(O)$ is undecidable. We refer to [63, 62, 78] for further information on the Diophantine problem in different rings and fields of number-theoretic flavor. There are long-standing conjectures (see, for example, [18, 62]) which state that the Diophantine problems in $\mathbb{Q}, F$, and O, as above, are all undecidable. The following result is important for our paper. If a commutative unitary ring R is infinite and finitely generated then, in the case of a positive characteristic, $\mathcal{D}(R)$ is undecidable, and in the case of characteristic zero, $\mathcal{D}(O)$ polynomial-time reduces to $\mathcal{D}(R)$ for some ring of algebraic integers O (Kirsten Eisentraeger's PhD thesis (Theorem 7.1), which is available on her website, see also [36]).

In the class of non-commutative associative unitary rings it was shown recently by Kharlampovich and Myasnikov in [43] that the Diophantine problem is undecidable in free associative algebras over fields and in the group algebras of a wide variety of torsion-free groups, including toral relatively hyperbolic groups, right angled Artin groups, commutative transitive groups, and the fundamental groups of various graphs of groups. For non-associative rings it was proved that the Diophantine problem is undecidable in free Lie algebras of rank at least three with coefficients in an arbitrary integral domain [42]. A general approach to the Diophantine problem in non-commutative rings (via reductions to the commutative ones) was developed in [35].

In another direction, coming from model theory, it was shown that the first-order theory of some classical fields is decidable: Tarski proved it for for complex numbers $\mathbb{C}$ and reals $\mathbb{R}$ [79], and Ershov, Ax and Kochen for p-adic numbers $\mathbb{Q}_p$ and $\mathbb{Z}_p$ [28, 1, 2]. The statement that a given finite system of equations has a solution in R can be represented by a very particular existential formula (a positive-primitive formula) with coefficients in R, so the Diophantine problem seems to be a part of the first-order theory of R, but the coefficients are getting involved, and this complicates the whole picture. In fact, involvement of constants makes Diophantine problems rather different from the classical model-theoretic problems of elementary equivalence and decidability of first order theories in the standard languages of groups or rings. We will say more on this later, specifically for the classical matrix groups.

Similar to the Diophantine problem in rings if a structure $\mathcal{A}$ is countable or finite then we assume that it comes equipped with an enumeration $\nu : \mathbb{N} \to \mathcal{A}$, which enables one to enumerate all terms in the language of $\mathcal{A}$ with constants in $\mathcal{A}$, hence all equations (which in this case are represented by equalities of two terms), as well as all finite systems of equations over $\mathcal{A}$. On the other hand, if $\mathcal{A}$ is uncountable then, by definition, one has to consider only equations with constants from a fixed arbitrary countable (or finite) subset C of $\mathcal{A}$. We denote this form of the Diophantine problem by $\mathcal{D}_C(\mathcal{A})$. This modification allows one to consider Diophantine problems over arbitrary structures in a more precise and also a more uniform way. As we will see below it may happen that the Diophantine problem $\mathcal{D}_C(\mathcal{A})$ is decidable for one subset $C \subseteq \mathcal{A}$ and undecidable for another one, even in countable structures $\mathcal{A}$. It is easy to see that for a countable (or finite) subset C of $\mathcal{A}$ the Diophantine problems $\mathcal{D}_C(\mathcal{A})$ and $\mathcal{D}_{\langle C\rangle}(\mathcal{A})$ reduce to each other, where $\langle C\rangle$ is the substructure generated by C in $\mathcal{A}$ (see Section 3). Furthermore, if $\mathcal{D}_C(\mathcal{A})$ is decidable then $\langle C\rangle$ is computable (recursive, constructible) in the sense of Malcev [52] and Rabin [65]. However, the converse is not necessary true. In Section 7 we study decidability of the Diophantine problem for the classical uncountable rings $\mathbb{C}, \mathbb{R}, \mathbb{Q}_p, \mathbb{Z}_p$ with respect to the choice of the constants C. We note that $\mathcal{D}_C(\mathbb{C})$ is decidable if and only if the subfield $\langle C\rangle$ is computable, while in $\mathbb{R}$, $\mathbb{Q}_p$ and $\mathbb{Z}_p$ decidability of the Diophantine problem depends on the subset C, and is closely related to computable reals and computable p-adics.

Research on systems of equations and their decidability in groups has a very long history, it goes back to 1912 to the pioneering works of Dehn on the word and conjugacy problems in finitely presented groups. Recall that an equation in a group G is an expression of the type $w(x_1, \ldots, x_n, g_1, \ldots, g_m) = 1$, where w is a group word in variables $x_1, \ldots, x_n$ and constants $g_1, \ldots, g_m \in G$. Currently, there are two main approaches to the Diophantine problems in groups. In the first approach one given a fixed group G tries to find a commutative unitary ring A such that the Diophantine problem in A algorithmically reduces to the Diophantine problem in G. In this case if $D(A)$ is undecidable then $D(G)$ is also undecidable. The first principle result in this vein is due to Romankov, who showed that the Diophantine problem is undecidable in any non-abelian free nilpotent group N of nilpotency class at least 9 (he proved that $\mathcal{D}(\mathbb{Z}) \leq \mathcal{D}(N)$ even one considers only single equations in the group N) [75]. Recently, Duchin, Liang and Shapiro showed in [26] that $\mathcal{D}(\mathbb{Z}) \leq \mathcal{D}(N)$ for any nonabelian free nilpotent group N, hence $\mathcal{D}(N)$ is undecidable. A far-reaching generalizations of these were obtained by Garreta, Myasnikov and Ovchinnikov in [34] where they proved that for any finitely generated non-virtually abelian nilpotent group G there exists a ring of algebraic integers O (depending on G) interpretable by equations in G, hence $\mathcal{D}(O)$ is Karp reducible to $\mathcal{D}(G)$. Furthermore, in [33] they gave a general sufficient condition for the ring O to be isomorphic to $\mathbb{Z}$, so in this case the Diophantine problem in G is undecidable. Based on this, they proved that a random nilpotent group G (given by a random presentation in the variety $\mathcal{N}_c$ of nilpotent groups of class at most c, for any $c \geq 2$) has $O \simeq \mathbb{Z}$, hence the undecidable Diophantine problem. These results on nilpotent groups allow numerous applications to the Diophantine problems in non-nilpotent groups H either via suitable Diophantine nilpotent subgroups of H or via suitable Diophantine nilpotent quotients of H [34]. For example, this technique allows one to show that the Diophantine problem in any finitely generated free solvable non-abelian group is undecidable.

This line of results changes drastically in the second approach, where one tries to show that the Diophantine problem in a given group G is decidable by reducing it to the Diophantine problem in a non-abelian free group F or a free monoid M (see, for example, Rips and Sela [69], Damani and Guirardel [16], Diekert and Muschol [24], Casals-Ruiz and Kazachkov [13, 12], and Diekert and Lohrey [23]). We refer to [41] for further results in this area. The principal results here are due to Makanin [48, 49] and Razborov [66, 67] who showed that the Diophantine problems $\mathcal{D}(M)$ and $\mathcal{D}(F)$ are decidable and, in the case of the free group F, further provided a description of the solution sets to arbitrary finite systems of equations in terms of Makanin-Razborov's diagrams. Another description of solutions sets in F in terms of NTQ systems (also termed ω-residually free towers) was obtained in [40]. NTQ systems give an effective approach to algebraic geometry and model theory of free groups. Recently, an entirely different method of solving equations in free groups, free monoids, and hyperbolic groups was developed in a series of papers [22, 37, 38, 14, 15].

In his now classical paper [51] Malcev studied elementary equivalence of matrix groups $G_n(F)$ where $G_n \in \{GL_n, SL_n, PGL_n, PSL_n\}$, $n \geq 3$, and F is a field. Namely, he showed that $G_n(F) \equiv G_m(L)$ if and only if $n = m$ and $F \equiv L$. His proof was based on two principal results. The first one states that for any integer $k \geq 3$ and G_n as above there is a group sentence $\Phi_{k,G}$ such that for any n, and a field F, $\Phi_{k,G}$ holds in $G_n(F)$ if and only if $k = n$. The second one is that F and $G_n(F)$ are mutually interpretable in each other. More precisely, $G_n(F)$ is absolutely interpretable in F (i.e., no use of parameters), while F is interpretable in $G_n(F)$ uniformly with respect to some definable subset of tuples of parameters. This implies that the theories $Th(F)$ and $Th(G_n(F))$ are reducible to each other in polynomial time, hence $Th(G_n(F))$ is decidable if and only if $Th(F)$ is decidable. Later Beidar and Michalev introduced another general approach to elementary equivalence of classical matrix groups [4]. Their proof was based on Keisler-Shelah theorem (two structures are elementarily equivalent if and only if their ultrapowers over non-principal ultrafilters are isomorphic) and the description of the abstract isomorphisms of the groups of the type $G_n(F)$. Bunina extended their results to unitary linear and Chevalley groups [5, 6, 7, 8, 9]. We reefer to recent book [10] for a comprehensive description of these and some other results in this area. Note that in all the results above the first-order theories include only the standard constants from the languages of groups and rings. The model theory of the group $UT_n(R)$, where $n \geq 3$, and R is an arbitrary unitary associative ring, was studied in detail by Belegradek (see [3]). Here he used heavily that the ring R is interpretable (with parameters) in $UT_n(R)$. The authors studied model theory of groups

$SL_n(O)$,$GL_n(O)$, and $T_n(O)$ for fields and rings of algebraic integers in [57, 58]. Their method exploits the mutual interpretability (and also bi-interpretability) of the group and the ring. In a similar manner Avni, A. Lubotsky, and C. Meiri studied the first order rigidity of non-uniform higher rank arithmetic groups [45]. Recently, Segal and Tent showed that for Chevalley groups $G(R)$ of rank at least 2 over a ring R if $G(R)$ has finite elementary width then $G(R)$ and R are bi-interpretable. Though related, all the model-theoretic results above do not shed much light on the Diophantine problem in the corresponding groups. Because to relate the Diophantine problems in $G_n(R)$ or $G(R)$ and R one needs to have their mutual interpretability by equations, not by arbitrary first-order formulas. This is precisely what we do in this paper. Recall that a subset (in particular a subgroup) H of a group G is Diophantine in G if it is definable in G by a formula of the type $\Phi(x) = \exists y_1 \ldots \exists y_n (\wedge_{i=1}^{k} w_i(x, y_1, \ldots, y_n) = 1$, where $w_i(x, y_1, \ldots, y_n)$ is a group word on $x, y_1, \ldots, y_n$. Such formulas are called Diophantine (in number theory) or positive-primitive (in model theory). Following [34], we say that a structure $\mathcal{A}$ is *e-interpretable* (or *interpretable by equations*, or *Diophantine interpretable*) in a structure $\mathcal{B}$ if $\mathcal{A}$ is interpretable (see Section 3) in $\mathcal{B}$ by Diophantine formulas. The main point of this definition is that if $\mathcal{A}$ is e-interpretable in $\mathcal{B}$ then the Diophantine problem in $\mathcal{A}$ reduces in polynomial time (Karp reduces) to the Diophantine problem in $\mathcal{B}$. On the one hand, it is harder to get e-interpretability than just interpretability, since in the latter you can use arbitrary formulas not only the Diophantine ones, but on the other hand, to study first-order equivalence of structures one does not usually use the constants in the language, while in the Diophantine problems the constants are allowed.

A subgroup $G \leq GL_n(R)$ is termed *large* if it contains the subgroup $E_n(R)$ generated in $GL_n(R)$ by all transvections $t_{ij}(\alpha)$, $i \neq j$, and $\alpha \in R$. In particular, the subgroups $SL_n(R)$ (when R is commutative) and $E_n(R)$ are large. Introducing large subgroups of $GL_n(R)$ allows one to unify similar arguments, otherwise used separately for each of the groups $GL_n(R)$, $SL_n(R)$ and $E_n(R)$. This also emphasize the fact that our method, unlike the one used in Malcev's paper [51], is based solely on transvections and nilpotent subgroups. Below by T_{ij} we denote the one-parametric subgroup $\{t_{ij}(\alpha) \mid \alpha \in R\}$.

In Section 4 we study Diophantine subgroups of large subgroups G of $GL_n(R)$, in particular, we prove the following key technical result.

Theorem 4.1 *Let G be a large subgroup of $GL_n(R)$, $n \geq 3$. Then for any $1 \leq k \neq m \leq n$ the one-parametric subgroup T_{km} is Diophantine in G (defined with constants from the set $\{t_{ij}(1) \mid 1 \leq i \neq j \leq n\}$).*

As a consequence it is not hard to see that the nilpotent subgroup $UT_n(R)$ is also Diophantine in G. Similar results hold for the large subgroups of $PGL_n(R)$ (these are the images of the large subgroups of $GL_n(R)$ under the canonical projection), provided that the ring R has no zero divisors (see Section 4.3). In particular, such results hold for $PSL_n(R)$, assuming in this case that the ring R is also commutative.

A similar approach works for the groups $T_n(R)$ and $UT_n(R)$, $n \geq 3$, in fact for any large subgroups of $T_n(R)$. Here we call a subgroup G of $T_n(R)$ *large* if it contains $UT_n(R)$. The following result is reminiscent of Theorem 4.1. However, since $T_n(R)$ has only transvections of the type t_{ij} with $i < j$ the argument is a little bit more involved and the result is slightly weaker than in $GL_n(R)$. Though it is sufficient for all our purposes. Below by R_G we denote the set (in fact, a subgroup) of all scalar matrices from $GL_n(R)$ that belong to G.

Theorem 5.1 *Let G be a large subgroup of $T_n(R), n \geq 3$. Then the following hold:*

1) for every $1 \leq i, j \leq n$ with $j - i \geq 2$ the subgroup T_{ij} is Diophantine in G;

2) for every $1 \leq i < n$ the subgroup $R_G T_{i,i+1} T_{1n}$ is Diophantine in G.

Note that in the case of $G = UT_n(R)$ our argument follows considerations in [3].

Now, using Diophantiness of the subgroups T_{ij} in Theorem 4.1 and the subgroups T_{ij} and $R_G T_{i,i+1} T_{1n}$ in Theorem 5.1, and Malcev's ideas from [50] one can interpret the ring R in the large subgroups G of $GL_n(R)$ and $T_n(R)$, as well as the large subgroups of $PGL_n(R)$, provided the ring R has no zero divisors (see Theorem 6.1). We do it in Section 6 and summarize in the following corollary.

Corollary 6.2 *For any $n \geq 3$, the ring R is e-interpretable in each of groups $GL_n(R)$, $SL_n(R)$ (assuming that in this case R is commutative), $E_n(R)$, $T_n(R)$, and $UT_n(R)$. If in addition R has no zero divisors, then R is e-interpretable in $PGL_n(R)$ and $PSL_n(R)$ (as before, R is also commutative in this case).*

Corollary 6.2 shows that the Diophantine problem in R is polynomial time reducible to the Diophantine problem for each of the groups mentioned there. To show the converse (with exception for $E_n(R)$) we need the following result (see Section 6), which, we believe, is known in folklore.

Proposition 6.4 *The groups $GL_n(R)$, $T_n(R)$, and $UT_n(R)$, are all e-interpretable in R. If the ring R is commutative then the groups $PGL_n(R)$, $SL_n(R)$, and $PSL_n(R)$ are all e-interpretable in R.*

Combining Corollary 6.2 and Proposition 6.4 one gets that the Diophantine problem in all the classical matrix groups mentioned above is polynomial time equivalent to the Diophantine problem in R (with appropriate restrictions on the ring R). A few comments on the restrictions on the ring R we put in our results. For $SL_n(R)$ we assume that R is commutative only for convenience of the definition, one can extend the results in this case for non-commutative division rings (skew-fields) R by showing that in this case R is still e-interpretable in $SL_n(R)$ when $n \geq 3$. However, to show that $SL_n(R)$ is e-interpretable in a skew-field R we need to have the commutant of the multiplicative group R^* to be Diophantine in R^*. The requirement on R to have no zero divisors in the case of $PGL_n(R)$ and $PSL_n(R)$ seems to come only from our argument in the proof. We do not know whether this requirement is really necessary or not to have R e-interpretable in large subgroups of $PGL_n(R)$.

Finally, in Section 7 we study in detail the Diophantine problems in the classical matrix groups over the fields $\mathbb{Q}$, algebraic number fields, $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}_p$, as well as the rings $\mathbb{Z}$, $\mathbb{Z}_p$, and the rings of algebraic integers $\mathcal{O}$. We start with the Diophantine problems in the rings $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}_p$, and $\mathbb{Z}_p$ themselves. Despite the fact that the first-order theories of these rings are well-studied, in particular, proved to be decidable (see, for example [53, 64]) the corresponding Diophantine problems with various sets of coefficients were not as well investigated. To this end we describe (and sometimes prove) the related results even though we believe that some of them are known in folklore.

Notation: By $G_n(R)$ we denote any of the classical linear groups $GL_n(R)$, $SL_n(R)$, $T_n(R)$, $UT_n(R)$, $PGL_n(R)$, $PSL_n(R)$ over a ring R.

We start with the following two results, which clarify the situation when $R = \mathbb{Z}$ or R is an algebraically closed field.

Theorem 7.1 *Let $n \geq 3$. Then the Diophantine problem in $G_n(\mathbb{Z})$ is Karp equivalent to the Diophantine problem in $\mathbb{Z}$, in particular, it is undecidable.*

Proposition 7.3

Let R be an algebraically closed field. Then the following hold:

1) *If A is a computable subfield of R then the first-order theory $Th_A(R)$ of R with constants from A in the language is decidable. In particular, $\mathcal{D}_A(R)$ is decidable.*

2) *Let C be a countable or finite subset of $G_n(R)$ such that the ring $\langle C \rangle$ generated by C is computable. Then the Diophantine problem in $G_n(R)$ with constants from C is decidable.*

In Section 7.3 we consider the Diophantine problems in the field $\mathbb{R}$ of reals and in the classical matrix groups over $\mathbb{R}$.

Let A be a countable (or finite) subset of $\mathbb{R}$. In this section we discuss first when the Diophantine problem in $\mathbb{R}$ with constants from A is decidable and then apply these results to the Diophantine problems in classical matrix groups over $\mathbb{R}$. Observe first, that by Lemma 3.3 if $\mathcal{D}_A(\mathbb{R})$ is decidable then the subfield $F(A)$ generated by A in $\mathbb{R}$ is computable. However, the converse is not true. The following result clarifies the situation.

Proposition 7.3 *Let A be a finite or countable subset of $\mathbb{R}$. Then the Diophantine problem in $\mathbb{R}$ with coefficients in A is decidable if and only if the ordered subfield $F(A)$, generated by A, is computable. Furthermore, in this case the whole first-order theory $Th_A(\mathbb{R})$ is decidable.*

Recall that a real $a \in \mathbb{R}$ is *computable* if its standard decimal expansion $a = a_0.a_1a_2\ldots$ is computable, i.e., the integer function $n \to a_n$ is computable. In other words, a is computable if and only if one can effectively approximate it by rationals with any precision. The set of all computable reals $\mathbb{R}^c$ forms a real closed subfield of $\mathbb{R}$, in particular $\mathbb{R}^c$ is first-order equivalent to $\mathbb{R}$.

In the following Proposition we collect some facts about computable ordered subfields of $\mathbb{R}$. Statements 1) and 2) were proved in [44], 3) was proven in [46] (see also [29] (Theorem 4, Ch.6, section 3), and 4) is known in folklore. We are grateful to Andrey Morozov for helping us with computable ordered fields.

Proposition 7.4 *The following holds:*

1) *Every ordered computable subfield of $\mathbb{R}$ is contained in $\mathbb{R}^c$.*

2) *The ordered subfield $\mathbb{R}^c \leq \mathbb{R}$ with the induced order from $\mathbb{R}$ is not computable.*

3) *If F is a computable ordered field, then its real closure is also computable. In particular, if F is a computable subfield of $\mathbb{R}$ then the algebraic closure $\bar{F}$ of F in $\mathbb{R}$ is a computable ordered field.*

4) *If $a_1, \ldots, a_m$ are computable reals then the ordered subfield $\mathbb{Q}(a_1, \ldots, a_m) \leq \mathbb{R}$ with the induced order from $\mathbb{R}$ is computable.*

Now we can provide an example mentioned above. Namely, if $a \in \mathbb{R}$ is not a computable real, then $F = \mathbb{Q}(a)$ is a computable field, but $\mathcal{D}_{\{a\}}(\mathbb{R})$ is undecidable.

Summarizing the discussion above we get the following result.

Corollary 7.5 *The following holds:*

- *The Diophantine problem in $\mathbb{R}$ with coefficients in $\mathbb{R}^c$ is undecidable;*
- *The Diophantine problem in $\mathbb{R}$ with coefficients in any finite subset of $\mathbb{R}^c$ is decidable;*
- *The Diophantine problem in $\mathbb{R}$ with coefficients in $\{a\}$, where a is not computable, is undecidable.*

Now we turn to the Diophantine problem in a classical matrix group over $\mathbb{R}$.

We say that a matrix $A \in GL_n(\mathbb{R})$ is *computable* if all entries in A are computable real numbers. Hence the computable matrices in $SL_n(\mathbb{R})$ are precisely the matrices from $SL_n(\mathbb{R}^c)$.

Theorem 7.7. *Let $n \geq 3$ and*

$$G_n(\mathbb{R}) \in \{GL_n(\mathbb{R}), SL_n(\mathbb{R}), T_n(\mathbb{R}), UT_n(\mathbb{R}), PGL_n(\mathbb{R}), PSL_n(\mathbb{R})\}.$$

If F is a computable ordered subfield of $\mathbb{R}$ then the first-order theory $Th(G_n(\mathbb{R}))$ of the matrix group $G_n(\mathbb{R})$ with constants from $G_n(F)$ is decidable (here $G_n(F)$ is the set of all matrices from $G_n(\mathbb{R})$ with entries from F). In particular, the Diophantine problem for equations with coefficients from $G_n(F)$ is decidable in $G_n(\mathbb{R})$.

The following result complements the theorem above (here by t_{ij} we denote the transvection $t_{ij}(1)$).

Theorem 7.8. *Let G be a large subgroup of $GL_n(\mathbb{R})$, where $n \geq 3$. If a matrix $A \in SL_n(\mathbb{R})$ is not computable then the Diophantine problem in G with coefficients in $\{t_{ij} \mid i, j = 1, \ldots, n\} \cup \{A\}$ is undecidable.*

The following result is instructive, it shows a big difference between finitely generated and countable structures with respect to the Diophantine problems even for rather nice rings and groups.

Theorem 7.9. *The following holds:*

1) *The Diophantine problem in the computable real-closed field $\mathbb{R}^c$ with coefficients in $\mathbb{R}^c$ is undecidable, but for any finitely generated subfield F of $\mathbb{R}^c$ the Diophantine problem in $\mathbb{R}^c$ with coefficients in F is decidable.*

2) *The Diophantine problem in the computable matrix group $G_n(\mathbb{R}^c)$ is undecidable, but for any finitely generated subgroup C of $G_n(\mathbb{R}^c)$ the Diophantine problem in $G_n(\mathbb{R}^c)$ with coefficients in C is decidable.*

In Section 7.4 we study the Diophantine problems in rings $\mathbb{Z}_p$ and $\mathbb{Q}_p$ and classical matrix groups over them.

Similarly to computable reals, one can define computable p-adic numbers for every fixed prime p. Recall, that every p-adic number $a \in \mathbb{Q}_p$ has a unique presentation in the form $a = p^m \xi$, where $m \in \mathbb{Z}$ and ξ is a unit in the ring $\mathbb{Z}_p$. In its turn, the unit ξ is uniquely determined by a sequence of natural numbers $\{\xi(i)\}_{i \in \mathbb{N}}$, where

$$0 \leq \xi(i) < p^{i+1}, \ \xi(i+1) = \xi(i)(\bmod p^{i+1}), \ (i \in \mathbb{N}).$$

The p-adic number $a = p^m \xi$ is computable if the sequence $i \to \xi(i)$ is computable. In this case the sequence $\{\xi(i)\}_{i \in \mathbb{N}}$ gives an effective p-adic approximation of ξ. It is known (see, for example [55]), that the set $\mathbb{Q}_p^c$ of all computable p-adic numbers forms a subfield of $\mathbb{Q}_p$, such that $\mathbb{Q}_p \equiv \mathbb{Q}_p^c$. Observe also that the ring $\mathbb{Z}_p$ is Diophantine in $\mathbb{Q}_p$. More precisely, if $p \neq 2$, then $\mathbb{Z}_p$ is defined in $\mathbb{Q}_p$ by formula $\exists y(1 + px^2 = y^2)$, while if $p = 2$ then $\mathbb{Z}_p$ is defined by the formula $\exists y(1 + 2x^3 = y^3)$.

The following result was proved in [55].

Theorem 7.10. *The following holds:*

1) *$Th(\mathbb{Z}_p, a_1, \ldots, a_n)$ is decidable if and only if each of $a_1, \ldots, a_n$ is a computable p-adic number.*

2) *$Th(\mathbb{Q}_p, a_1, \ldots, a_n)$ is decidable if and only if each of $a_1, \ldots, a_n$ is a computable p-adic number.*

We need a slightly more precise version of the results above in the case when the theory is undecidable.

Theorem 7.11. *The following holds:*

1) *If a p-adic integer a is not computable then equations with constants from $\mathbb{Q} \cup \{a\}$ are undecidable in $\mathbb{Z}_p$.*

2) *If a p-adic number $a \in \mathbb{Q}_p$ is not computable then equations with constants from $\mathbb{Q} \cup \{a\}$ are undecidable in $\mathbb{Q}_p$.*

We say that a matrix $A \in GL_n(\mathbb{Q}_p)$ is *computable* if all entries in A are computable p-adic numbers, i.e., $A \in GL_n(\mathbb{Q}_p^c)$. Hence the computable matrices in $SL_n(\mathbb{Q}_p)$ are precisely the matrices from $SL_n(\mathbb{Q}_p^c)$.

Theorem 7.12.

Let $n \geq 3$. The following holds:

1) *Let*

$$G_n(\mathbb{Q}_p) \in \{GL_n(\mathbb{Q}_p), SL_n(\mathbb{Q}_p), T_n(\mathbb{Q})_p, UT_n(\mathbb{Q}_p), PGL_n(\mathbb{Q}_p), PSL_n(\mathbb{Q}_p)\}.$$

   If $A_1, \ldots, A_m$ are computable matrices from $G_n(\mathbb{Q}_p)$ then the first-order theory of $G_n(\mathbb{Q}_p)$ with constants $A_1, \ldots, A_m$ is decidable. In particular, the Diophantine problem for equations with coefficients $A_1, \ldots, A_m$ is decidable in $G_n(\mathbb{Q}_p)$.

2) *Let*

$$G_n(\mathbb{Z}_p) \in \{GL_n(\mathbb{Z}_p), SL_n(\mathbb{Z}_p), T_n(\mathbb{Z}_p), UT_n(\mathbb{Z}_p), PGL_n(\mathbb{Z}_p), PSL_n(\mathbb{Z}_p)\}.$$

   If $A_1, \ldots, A_m$ are computable matrices from $G_n(\mathbb{Z}_p)$ then the first-order theory of $G_n(\mathbb{Z}_p)$ with constants $A_1, \ldots, A_m$ is decidable. In particular, the Diophantine problem for equations with coefficients $A_1, \ldots, A_m$ is decidable in $G_n(\mathbb{Z}_p)$.

In the following result t_{ij} denotes the transvection $t_{ij}(1)$.

Theorem 7.13 *If a matrix $A \in SL_n(\mathbb{Z}_p)$ ($A \in SL_n(\mathbb{Q}_p)$) is not computable then Diophantine problem for equations with coefficients in $\{t_{ij} \mid i, j = 1, \ldots, n\} \cup \{A\}$ is undecidable in $SL_n(\mathbb{Z}_p)$ ($SL_n(\mathbb{Q}_p)$).*

2 Preliminaries

In this section we fix some notation and recall technical results that are used throughout the paper.

For a group G and $x, y \in G$ we denote by x^y the conjugate $y^{-1}xy$ of x by y, and by $[x, y]$ the commutator $x^{-1}y^{-1}xy$. For a subset $A \subseteq G$ by $C_G(A)$ we denote the centralizer $\{x \in G \mid \forall a \in A \ ([x, a] = 1)\}$, in particular, $Z(G) = \{x \in G \mid \forall y \in G \ ([x, y] = 1)\}$ is the center of G. For subsets $X, Y \subseteq G$ by $[X, Y]$ we denote the subgroup of G generated by all commutators $[x, y]$, where $x \in X, y \in Y$. Then $[G, G]$ is the derived subgroup G' of G (the commutant of G). The lower central series of G is defined as $G = \gamma_1(G) \geq \gamma_2(G) \geq \ldots$, where $\gamma_{i+1}(G) = [G, \gamma_i(G)]$.

In the rest of the paper by R we denote an arbitrary associative ring with identity 1. By $R^\times$ we denote the multiplicative group of invertible (unit) elements of R and by R^+ the additive group of R.

Now we define the groups we study in this paper and list some of their properties that we use often.

2.1 $GL_n(R)$

Fix $n \in \mathbb{N}$. By $GL_n(R)$ we denote the group of all invertible $n \times n$ matrices over an associative unitary ring R.

Let e_{ij} be an $n \times n$ matrix where (i, j)-entry is 1 and every other entry is 0. For $1 \leq i \neq j \leq n$ the matrix $t_{ij}(\alpha) = I_n + \alpha e_{ij}$, where $\alpha \in R$ and I_n is the $n \times n$ identity matrix, is called a *transvection*. Sometimes we denote the transvection $t_{ij}(1)$ simply by t_{ij}. Put $\mathcal{T}_n = \{t_{ij} \mid 1 \leq i \neq j \leq n\}$.

Transvections $t_{ij}(\alpha), t_{kl}(\beta)$, for $\alpha, \beta \in R$, satisfy the following well-known (Steinberg) relations:

1) $t_{ij}(\alpha)t_{ij}(\beta) = t_{ij}(\alpha + \beta)$.
2) $[t_{ik}(\alpha), t_{kl}(\beta)] = t_{il}(\alpha\beta)$, for $i \neq l$.
3) $[t_{ik}(\alpha), t_{jl}(\beta)] = 1$ for $i \neq l, j \neq k$.

Observe, that 2) implies that $[t_{ij}(\alpha), t_{ki}(\beta)] = t_{kj}(-\alpha\beta)$, for $j \neq k$.

Let $diag(\alpha_1, \ldots, \alpha_n)$ be the $n \times n$ diagonal matrix with (i, i)-entry $\alpha_i \in R^\times$. Then $diag(\alpha_1, \ldots, \alpha_n) \in GL_n(R)$ and the set of all such matrices forms a subgroup $D_n(R)$ of $GL_n(R)$. Note that for any $\alpha_1, \ldots, \alpha_n \in R^\times$, $\beta \in R$ the following holds:

$$diag(\alpha_1, \ldots, \alpha_n)^{-1} t_{ij}(\beta) diag(\alpha_1, \ldots, \alpha_n) = t_{ij}(\alpha_i^{-1}\beta\alpha_j). \tag{1}$$

In particular,

$$[t_{ij}(\beta), diag(\alpha_1, \ldots, \alpha_n)] = t_{ij}(\alpha_i^{-1}\beta\alpha_j - \beta). \tag{2}$$

By $d(\alpha)$ we denote the scalar matrix $diag(\alpha, \ldots, \alpha) = \alpha I_n$, where $\alpha \in R^\times$. The set of all scalar matrices forms a subgroup $R^\times I_n \leq D_n(R)$ which is isomorphic to $R^\times$. It follows from (2) that the subgroup $Z_n(R)$ of $R^\times I_n$, which consists of all scalar matrices $d(\alpha)$, where α is in the center of the group $R^\times$, forms the center of the groups $R^\times I_n$, $D_n(R)$, as well as the group $GL_n(R)$.

Now consider the following diagonal matrices for $\alpha \in R^\times$:

$$d_i(\alpha) \overset{\text{def}}{=} diag(1, \ldots, \underbrace{\alpha}_{i'\text{th}}, \ldots, 1).$$

It is known (see, for example [39]) that if R is a field then there are natural numbers r and s, which depend only on n, such that every element $g \in GL_n(R)$ can be presented as a product of the type

$$g = x_1 \ldots x_r d_n(\beta) y_1 \ldots y_s \tag{3}$$

where x_i, y_j are transvections and $\beta \in R^\times$.

2.2 $SL_n(R)$ and $E_n(R)$

Denote by $E_n(R)$ the subgroup of $GL_n(R)$ generated by all transvections, i.e., $E_n(R) = \langle t_{ij}(\alpha) \mid \alpha \in R, 1 \leq i \neq j \leq n\rangle$.

Definition 2.1. *We say that a subgroup $G \leq GL_n(R)$ is* large *if G contains $E_n(R)$.*

Throughout the paper we assume $n \geq 3$.

If the ring R is commutative then, as usual, the group $SL_n(R)$ consists of all matrices from $GL_n(R)$ with determinant 1. One can define $SL_n(R)$ for arbitrary division rings (using the Dieudonne determinant), but we do not consider such groups here. In every case we mention a group $SL_n(R)$ we assume that R is commutative. Clearly, $E_n(R)$ is a subgroup of $SL_n(R)$, so $SL_n(R)$ is a large subgroup of $GL_n(R)$. If R is a field or Euclidean domain then $SL_n(R) = E_n(R)$, but in general, this is not the case. For fields R one has

$$[GL_n(R), GL_n(R)] = SL_n(R).$$

Now (3) implies that

$$GL_n(R) \simeq SL_n(R) \rtimes d_n(R^\times) \simeq GL_n(R)' \rtimes R^\times.$$

Note also that in this case

$$[SL_n(R), SL_n(R)] = SL_n(R).$$

Following [11] we say that $SL_n(R)$ has *bounded elementary generation* if there is a natural number w such that every element of $SL_n(R)$ is a product of at most w transvections. Order all pairs of indices $(i,j), i,j = 1,\ldots,n$ into a sequence σ in some arbitrary but fixed way, say $\sigma = (1,1),\ldots,(n,n)$. Repeat this sequence consequently w times, obtaining a new sequence $\sigma^* = \sigma,\sigma,\ldots,\sigma = (i_1,j_1),\ldots,(i_m,j_m)$, where $m = wn^2$. Then every element $g \in SL_n(R)$ can be decomposed into a product

$$g = t_{i_1j_1}(\alpha_1)\ldots t_{i_mj_m}(\alpha_m)$$

for some $\alpha_1,\ldots,\alpha_m \in R$ (note that we allow here elements $\alpha_i = 0$), which is uniform in the order of transvections.

For $1 \leq i \neq j \leq n$ denote by T_{ij} the one-parametric subgroup $\{t_{ij}(\alpha) \mid \alpha \in R\}$. Then the bounded elementary generation of $SL_n(R)$ is equivalent to the statement that there is sequence of pairs $(i_1,j_1),\ldots,(i_m,j_m)$, where $1 \leq i_k \neq j_k \leq n$ such that

$$SL_n(R) = T_{i_1j_1}\ldots T_{i_mj_m}.$$

If R is a field then formula (3) implies that $SL_n(R)$ has bounded elementary generation. A much harder argument shows that $SL_n(\mathcal{O})$ over a ring of algebraic integers $\mathcal{O}$ has bounded elementary generation [11]. However, this is not the case even for arbitrary domains. Indeed, it was shown in [81, 21] that if F is a field of infinite transcendence degree over its prime subfield (for example: $F = \mathbb{C}$) then for every number c there is a matrix in the group $SL_n(F[x])$ which cannot be written as a product of c commutators.

2.3 Unitriangular groups $UT_n(R)$

The transvections $t_{ij}(\alpha)$, where $1 \leq i < j \leq n$, $\alpha \in R$, generate the subgroup $UT_n(R)$ of all (upper) unitriangular matrices in $GL_n(R)$.

For $m = 1,\ldots,n$ denote by $UT^m(n,R)$ the subgroup of $UT_n(R)$ consisting of all matrices with $m-1$ zero diagonals above the main one. Then

$$UT_n(R) = UT_n^1(R) > UT_n^2(R) > \ldots > UT_n^n(R) = 1. \quad (4)$$

Furthermore, for any positive $r,s \in \mathbb{N}$ one has

$$[UT_n^r(R), UT_n^s(R)] = UT_n^{r+s}(R).$$

This implies that the series (4) is the lower central series of $UT_n(R)$, in particular, $\gamma_k(UT_n(R)) = UT_n^k(R)$. Direct computations show that any element $g \in UT_n^m(R)$ can be uniquely written as a product of the following type:

$$g = t_{n-m,n}(\alpha_{n-m})t_{n-m-1,n-1}(\alpha_{n-m-1})\ldots t_{1,1+m}(\alpha_1)h,$$

where $\alpha_i \in R$ and $h \in UT_n^{m+1}(R)$. Therefore,

$$UT_n^m(R) = T_{n-m,n}T_{n-m-1,n-1}\ldots T_{1,1+m}UT_n^{m+1}(R) \quad (5)$$

This implies that $UT_n(R)$ is a finite product of one parametric subgroups T_{ij}.

2.4 Triangular groups $T_n(R)$

Recall, that $T_n(R)$ consists of all upper triangular matrices $x = (x_{ij})$ over R with units on the main diagonal, i.e., $x_{ij} = 0$ for $i > j$, $x_{ij} \in R$ for $i < j$, and $x_{ii} \in R^\times$ for $1 \leq i \leq n$. Clearly, $UT_n(R) \leq T_n(R)$.

Note that any matrix $x \in T_n(R)$ can be represented as a product $x = d_x u_x$, where $d_x = diag(x_{11}, \ldots, x_{nn})$, and $u_x \in UT_n(R)$, where $u_x = (y_{ij})$, with $y_{ij} = x_{ii}^{-1} x_{ij}$ for $i < j$. Therefore, $T_n(R) = D_n(R)UT_n(R)$ and $D_n(R) \cap UT_n(R) = 1$. Furthermore, $UT_n(R)$ is a normal subgroup in $T_n(R)$, see (1), hence

$$T_n(R) \simeq UT_n(R) \rtimes D_n(R).$$

Definition 2.2. *We call $G \leq T_n(R)$ a large subgroup of $T_n(R)$ if G contains $UT_n(R)$.*

Obviously, $UT_n(R)$ is a large subgroup of $T_n(R)$, but it is not a large subgroup of $GL_n(R)$.

2.5 Groups $PGL_n(R)$ and $PSL_n(R)$

The projective general and projective special linear groups $PGL_n(R)$ and $PSL_n(R)$ are defined as quotients $PGL_n(R) = GL_n(R)/Z(GL_n(R))$ and $PSL_n(R) = SL_n(R)/Z(SL_n(R))$ of the groups by their centers. Note that $Z(GL_n(R))$ is the subgroup $Z_n(R)$ of all the scalar matrices $d(\alpha)$, where α belongs to the center of the group $R^\times$. Respectively, $Z(SL_n(R)) = Z_n(R) \cap SL_n(R)$.

Definition 2.3. *Let $\phi : GL_n(R) \to PGL_n(R)$ be the canonical homomorphism. We call a subgroup G of $PGL_n(R)$* large *if it contains $\phi(E_n(R))$.*

3 The Diophantine problem

3.1 Equations, constants and computable structures

Recall, that the *Diophantine problem* $\mathcal{D}(\mathcal{A})$ in an algebraic structure $\mathcal{A}$ is the task to determine whether or not a given finite system of equations with constants in $\mathcal{A}$ has a solution in $\mathcal{A}$. $\mathcal{D}(\mathcal{A})$ is *decidable* if there is an algorithm that given a finite system S of equations with constants in $\mathcal{A}$ decides whether or not S has a solution in $\mathcal{A}$. Here, the structure $\mathcal{A}$ is assumed to be countable, moreover, supposedly it comes equipped with a fixed enumeration $\mathcal{A} = \{a_1, a_2, \ldots\}$, which is given by a surjective function $\nu : \mathbb{N} \to \mathcal{A}$ (the function is not necessary injective). One can use the function ν for enumeration of all finite systems of equations with coefficients in $\mathcal{A}$ in countably many variables $x_1, x_2, \ldots$, and then provide them as inputs to a decision algorithm in the Diophantine problem $\mathcal{D}(\mathcal{A})$. The first question to address here is how much decidability of $\mathcal{D}(\mathcal{A})$

depends on the choice of the enumeration $\nu : \mathbb{N} \to \mathcal{A}$. Decidability of $\mathcal{D}(\mathcal{A})$ does depend on the enumeration ν, so for some ν, $\mathcal{D}(\mathcal{A})$ is decidable, and for others it is not. For example, every non-trivial finite or countable group has an infinite countable presentation with undecidable word problem, so the Diophantine problem in the group with respect to enumerations related to such infinite presentations is undecidable. However, researchers are usually interested only in "natural" enumerations ν, which come from finite descriptions of the elements of $\mathcal{A}$ that reflect the nature of the structure $\mathcal{A}$. For instance, if $\mathcal{A}$ is a finitely generated group then one may describe elements of $\mathcal{A}$ by finite words in a fixed finite set of generators, and use known effective enumerations of words, while if $\mathcal{A}$ is, say, a group $GL_n(R)$ over a ring R, then elements of $GL_n(R)$ can be described by n^2-tuples of elements from R, so one can use enumerations of R to enumerate elements of $GL_n(R)$. Here, and in all other places, by an effective enumeration of words (or polynomials, or any other formulas of finite signature) we understand such an enumeration $\mu : n \to w_n$ of words in a given finite or countable alphabet that for any number $n \in \mathbb{N}$ one can compute the word w_n and for any word w in the given alphabet one can compute a number n such that $w = w_n$. If $\mathcal{A}$ is a finitely generated associative unitary ring R then elements of $\mathcal{A}$ can be presented as non-commutative polynomials with integer coefficients in finitely many variables (which can be also viewed as elements of a free associative unitary ring of finite rank), and then effectively enumerate such polynomials. Similarly, for commutative rings R the usual commutative polynomials can be used. There are two ways to make the formulation of the Diophantine problem a bit more precise, either explicitly fix the enumeration ν of $\mathcal{A}$ in the Diophantine problem (denote it by $\mathcal{D}_\nu(\mathcal{A})$), or to term that $\mathcal{D}(\mathcal{A})$ is decidable if *there exists* an enumeration ν of $\mathcal{A}$ such that $\mathcal{D}_\nu(\mathcal{A})$ is decidable. To study which enumerations are "reasonable" in the discourse of Diophantine problems we need to digress to the theory of computable algebra, or computable model theory, that stem from pioneering works of Rabin [65] and Malcev [52] (for details see a book [29] and a more recent survey [31]).

Recall that a structure $\mathcal{A}$ of finite signature is *computable* with respect to an enumeration $\nu : \mathbb{N} \to \mathcal{A}$ if all the basic operations and predicates (including the equality) on $\mathcal{A}$ are computable with respect to the enumeration ν. In particular, a group G is computable with respect to ν if there are two computable functions $f(x, y)$ and $h(x, y)$ such that for any $i, j \in \mathbb{N}$ the following holds: $\nu(i) \cdot \nu(j) = \nu(f(i, j))$ and $\nu(i) = \nu(j) \iff h(i, j) = 1$. Similarly, a countable ring R is computable with respect to enumeration $\nu : \mathbb{N} \to R$ if in addition to the conditions above there is a computable function $g(x, y)$ such that $\nu(i) + \nu(j) = \nu(g(i, j))$.

The following observation shows the connection between decidability of Diophantine problems and computable structures.

Lemma 3.1. *Let $\mathcal{A}$ be a countable structure given with an enumeration ν : $\mathbb{N} \to \mathcal{A}$. If the Diophantine problem $\mathcal{D}_\nu(\mathcal{A})$ is decidable then the structure $\mathcal{A}$ is computable with respect to ν.*

Proof. We give a sketch of the proof in the case of groups. The general case is quite similar and we leave to the reader. Let $A = \{a_1, a_2, \ldots\}$, where $a_i = \nu(i), i \in \mathbb{N}$. Assuming that the $\mathcal{D}_\nu(A)$ is decidable we need to show that A is computable, i.e., the following sets are computable

$$\{(i,j) \mid a_i = a_j, i, j \in \mathbb{N}\},$$

$$\{(i,j,k) \mid a_i \cdot a_j = a_k, i, j, k \in \mathbb{N}\}.$$

These sets are defined by equations in A, so they are, indeed, computable. □

Lemma 3.1 shows that that the only interesting enumerations of $\mathcal{A}$ with respect to the Diophantine problem are those that make $\mathcal{A}$ computable, they are called *constructivizations* of $\mathcal{A}$. The question whether a given countable structure $\mathcal{A}$ has a constructivization is a fundamental one in computable model theory, so there are a lot of results in this direction (see [29, 31, 30]) that can be used here.

Let μ and ν be two enumerations of $\mathcal{A}$. By definition μ *reduces* to ν (symbolically $\mu \preceq \nu$) if there is a computable function $f(x)$ such that $\mu = \nu \circ f$. μ and ν are termed *equivalent* (symbolically $\mu \sim \nu$) if $\nu \preceq \nu$ and $\nu \preceq \mu$.

Lemma 3.2. *[29] Let $\mathcal{A}$ be a finitely generated structure that have at least one constructivization. Then all constructivizations of $\mathcal{A}$ are equivalent to each other.*

It follows that a finitely generated structure $\mathcal{A}$ has a constructivization if and only if the word problem in $\mathcal{A}$ with respect to some (any) finite generating set is decidable. In this case, any other constructivization is equivalent to the one that comes as described above from any fixed finite set of generators. This is why for finitely generated structures the enumerations usually are not mentioned explicitly.

If $\mathcal{A}$ is uncountable then, as we mentioned in Introduction, one has to consider only equations with constants from a fixed countable (or finite) subset C of $\mathcal{A}$ which comes equipped with a enumeration $\nu : \mathbb{N} \to C$. This form of the Diophantine problem is denoted by $\mathcal{D}_C(\mathcal{A})$. It will be convenient to consider instead of the set C the substructure $\langle C \rangle$ generated by C in $\mathcal{A}$. In this case one needs to consider enumerations of $\langle C \rangle$ that are "compatible" with the given enumeration of C. To this end we introduce the following notion from computable model theory (see [29]). Let S be a set with an enumeration ν and $\phi : S \to S^*$ an embedding of sets. We say that an enumeration $\nu^* : \mathbb{N} \to S^*$ *extends* the enumeration ν if there exists a computable function $f : \mathbb{N} \to \mathbb{N}$ such that $\phi \circ \nu = \nu^* \circ f$. It is easy to construct an enumeration of $\langle C \rangle$ that extends a given enumeration of the generating set C (see [29], Ch. 6, Section 1, Theorem 1). In the case of the subset C of $\mathcal{A}$ we will always, if not said otherwise, consider enumerations ν^* of $\langle C \rangle$ that extend a given enumeration of C. Furthermore, we will always assume that for a given $n \in \mathbb{N}$ one can compute the term t of the language of the structure $\mathcal{A}$ with constants from C which represents the element $\nu^*(n)$ in the structure $\langle C\rangle$. And conversely, for every such a term T one can compute a number $n \in \mathbb{N}$ such that $\nu^*(n) = t$. We call such enumerations ν^* *effective*. To construct an effective enumeration of $\langle C\rangle$ in the case when $\mathcal{A}$ is a group one needs only effectively enumerate all words in the alphabet $C^{\pm 1}$, while in the case when $\mathcal{A}$ is a commutative unitary ring one needs to enumerate all polynomials from $\mathbb{Z}[C]$.

The following is useful.

Lemma 3.3. *Let $\mathcal{A}$ be a structure, C a finite or countable subset of $\mathcal{A}$ equipped with an enumeration ν, and $\langle C\rangle$ the substructure generated by C in $\mathcal{A}$ with an effective enumeration that extends ν. Then the following hold:*

1) *The Diophantine problems $\mathcal{D}_C(\mathcal{A})$ and $\mathcal{D}_{\langle C\rangle}(\mathcal{A})$ are equivalent (reduce to each other).*

2) *If $\mathcal{D}_C(\mathcal{A})$ is decidable then $\langle C\rangle$ is computable with respect to any enumeration of $\langle C\rangle$ that extends the enumeration ν of the generating set C.*

Proof. To prove 1) assume first that $\mathcal{D}_C(\mathcal{A})$ is decidable. Since ν^* is an effective enumeration that extends the enumeration ν one can for every $n \in \mathbb{N}$ compute a term t that represents the element $\nu^*(n)$ via generators from C. Therefore, given a finite system of equations $S(X)$ with coefficients in $\langle C\rangle$ one can "rewrite" every coefficient a in $S(X)$ as a term t_a that represents a via generators in C and adjust the system $S(X)$ accordingly. The system S^* obtained this way has only coefficients in C and it has precisely the same set of solutions in $\mathcal{A}$ as the system S. This reduces $\mathcal{D}_{\langle C\rangle}(\mathcal{A})$ to $\mathcal{D}_C(\mathcal{A})$. Conversely, to reduce $\mathcal{D}_C(\mathcal{A})$ to $\mathcal{D}_{\langle C\rangle}(\mathcal{A})$ one can do the following. First note, that since ν^* extends ν there is a computable function $f : \mathbb{N} \to \mathbb{N}$ such that, for every $n \in \mathbb{N}$, $f(n)$ gives the "number" of the element $\nu(n)$ in the enumeration ν^*. This allows one to algorithmically rewrite a system T with coefficients in C into an equivalent system T^* with coefficients in $\langle C\rangle$. This reduces $\mathcal{D}_C(\mathcal{A})$ to $\mathcal{D}_{\langle C\rangle}(\mathcal{A})$.

The proof of 2) is straightforward and we omit it. □

From now on we will always assume, without loss of generality, that coefficients in the Diophantine problem is taken from a countable substructure $\langle C\rangle$ rather then from the set C.

3.2 Diophantine sets and e-interpretability

To prove that $\mathcal{D}(\mathcal{A})$ reduces to $\mathcal{D}(\mathcal{M})$ for some structures $\mathcal{A}$ and $\mathcal{M}$ it suffices to show that $\mathcal{A}$ is interpretable by equations (or *e-interpretable*) in $\mathcal{M}$.

The notion of e-interpretability was introduced in [34, 33, 35]. Here we remind this notion and state some basic facts we use in the sequel.

In what follows we often use non-cursive boldface letters to denote tuples of elements: e.g. $\mathbf{a} = (a_1, \ldots, a_n)$. Furthermore, we always assume that equations may contain constants from the algebraic structure in which they are considered.

Definition 3.4. *A subset $D \subset M^m$ is called* Diophantine*, or* definable by systems of equations *in $\mathcal{M}$, or* e-definable *in $\mathcal{M}$, if there exists a finite system of equations, say $\Sigma_D(x_1, \ldots, x_m, y_1, \ldots, y_k)$, in the language of $\mathcal{M}$ such that for any tuple $\mathbf{a} \in M^m$, one has that $\mathbf{a} \in D$ if and only if the system $\Sigma_D(\mathbf{a}, \mathbf{y})$ on variables $\mathbf{y}$ has a solution in $\mathcal{M}$. In this case Σ_D is said to* e-define *D in $\mathcal{M}$.*

Remark 3.5. Observe that, in the notation above, if $D \subset M^m$ is e-definable then it is definable in $\mathcal{M}$ by the formula $\exists \mathbf{y} \Sigma_D(\mathbf{x}, \mathbf{y})$. Such formulas are called *positive primitive*, or pp-formulas. Hence, e-definable subsets are sometimes called pp-definable. On the other hand, in number theory such sets are usually referred to as Diophantine ones. And yet, in algebraic geometry they can be described as projections of algebraic sets.

Definition 3.6. *An algebraic structure $\mathcal{A} = (A; f, \ldots, r, \ldots, c, \ldots)$ is called* e-interpretable *in another algebraic structure $\mathcal{M}$ if there exists $n \in \mathbb{N}$, a subset $D \subseteq \mathcal{M}^n$ and an onto map (called the* interpreting *map) $\phi : D \twoheadrightarrow \mathcal{A}$, such that:*

1. *D is e-definable in $\mathcal{M}$.*
2. *For every function $f = f(y_1, \ldots, y_k)$ in the language of $\mathcal{A}$, the preimage by ϕ of the graph of f, i.e. the set $\{(\bar{x}_1, \ldots, \bar{x}_k, \bar{x}_{k+1}) \in D^{k+1} \mid \phi(\bar{x}_{k+1}) = f(\phi(\bar{x}_1), \ldots, \phi(\bar{x}_k))\}$, where for each $1 \leq i \leq k+1$, $\bar{x}_i = (x_{i1}, \ldots, x_{in})$, is e-definable in $\mathcal{M}$.*
3. *For every relation r in the language of $\mathcal{A}$, and also for the equality relation $=$ in $\mathcal{A}$, the preimage by ϕ of the graph of r is e-definable in $\mathcal{M}$.*

Let $\mathcal{A}$ is e-interpretable in $\mathcal{M}$ as in Definition 3.6 above. This interpretation is completely determined by the map ϕ and a tuple Γ of the Diophantine formulas that define the set D from 1), the functions f from 2), and the relations r from 3). By $P_\Gamma \subseteq \mathcal{M}$ we denote the finite set of constants (parameters) that occur in formulas from Γ. E-interpretability is a variation of the classical notion of the first-order interpretability, where instead of arbitrary first-order formulas finite systems of equations are used as the interpreting formulas. Note that in number theory there are notions of Diophantine definition and Diophantine generation, introduced by Shlapentokh [78], which are specifically designed for studying the Hilbert's tenth problem in number fields and play a part similar to e-interpretability.

The following is a fundamental property of e-interpretability. Intuitively it states that if $\mathcal{A}$ is e-interpretable in $\mathcal{M}$ by formulas Γ and an interpreting map $\phi : D \twoheadrightarrow \mathcal{A}$, then any system of equations in $\mathcal{A}$ can be effectively "encoded" by an equivalent system of equations in $\mathcal{M}$. To explain we need the following notation. Let C be a finite or countable subset of $\mathcal{A}$ equipped with an enumeration $\nu : \mathbb{N} \to C$. For every $c_i = \nu(i) \in C$ fix an arbitrary tuple $d_i \in \phi^{-1}(c_i)$. Denote by D_R the set of all elements in $\mathcal{M}$ that occur as components in tuples d_i from R. Denote by C_Γ the set $D_R \cup P_\Gamma$. We say that enumeration $\nu^* : \mathbb{N} \to C_\Gamma$ is *compatible* with the enumeration ν (with respect to the set of representatives

R) if there is an algorithm that for every $i \in N$ computes the ν^*-numbers of the components of the tuple d_i. For example, one can enumerate first all elements in P_Γ and then for $i = 1, 2, \ldots$ enumerate in the natural order all the components of $d_1, d_2, \ldots$.

Lemma 3.7. *[34] Let $\mathcal{A}$ be e-interpretable in $\mathcal{M}$ by a set of formulas Γ with an interpreting map $\phi : D \twoheadrightarrow \mathcal{A}$ (in the notation of the Definition 3.6). Let C be a finite or countable subset of $\mathcal{A}$ equipped with an enumeration ν. Then there is a polynomial time algorithm that for every finite system of equations $S(\mathbf{x})$ in $\mathcal{A}$ with coefficients in C constructs a finite system of equations $S^*(\mathbf{y}, \mathbf{z})$ in $\mathcal{M}$ with coefficients in C_Γ (given via a compatible enumeration $\nu^* : \mathbb{N} \to C_\Gamma$), such that if $(\mathbf{b}, \mathbf{c})$ is a solution to $S^*(\mathbf{y}, \mathbf{z})$ in $\mathcal{M}$, then $\mathbf{b} \in D$ and $\phi(\mathbf{b})$ is a solution to $S(\mathbf{x})$ in $\mathcal{A}$. Moreover, any solution $\mathbf{a}$ to $S(\mathbf{x})$ in $\mathcal{A}$ arises in this way, i.e. $\mathbf{a} = \phi(\mathbf{b})$ for some solution $(\mathbf{b}, \mathbf{c})$ to $S^*(\mathbf{y}, \mathbf{z})$ in $\mathcal{M}$.*

Now we state two key consequences of Lemma 3.7.

Corollary 3.8. *Let $\mathcal{A}$ be e-interpretable in $\mathcal{M}$ by a set of formulas Γ with with an interpreting map $\phi : D \twoheadrightarrow \mathcal{A}$ (in the notation of the Definition 3.6). Let C be a finite or countable subset of $\mathcal{A}$ equipped with an enumeration ν. Then the Diophantine problem in $\mathcal{A}$ with coefficients in C is reducible in polynomial time (Karp reducible) to the Diophantine problem in $\mathcal{M}$ with coefficients in C_Γ with respect to any compatible with ν enumeration ν^*. Consequently, if $\mathcal{D}_C(\mathcal{A})$ is undecidable, then $\mathcal{D}_{C_\Gamma}(\mathcal{M})$ (relative to ν^*) is undecidable as well.*

Corollary 3.9. *e-interpetability is a transitive relation, i.e., if $\mathcal{A}_1$ is e-intepretable in $\mathcal{A}_2$, and $\mathcal{A}_2$ is e-interpretable in $\mathcal{A}_3$, then $\mathcal{A}_1$ is e-interpretable in $\mathcal{A}_3$.*

4 Diophantine structure in large subgroups of $GL_n(R)$ and $PGL_n(R)$

In this section we show that many important subgroups of the the classical matrix groups of R are Diophantine. We freely use notation from Preliminaries.

4.1 One-parametric subgroups T_{ij} are Diophantine in large subgroups of $GL_n(R)$

We start with the following key result.

Theorem 4.1. *Let G be a large subgroup of $GL_n(R)$, $n \geq 3$. Then for any $1 \leq k \neq m \leq n$ the subgroup T_{km} is Diophantine in G (defined with constants from $\{t_{ij}\}$).*

Proof. Let $x = (x_{st}) \in G$ and assume that $xt_{ij} = t_{ij}x$. without loss of generality we can assume $i < j$, then

$$\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1i} & \cdots & x_{1j} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2i} & \cdots & x_{2j} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{i1}+x_{j1} & x_{i2}+x_{j2} & \cdots & x_{ii}+x_{ji} & \cdots & x_{ij}+x_{jj} & \cdots & x_{in}+x_{jn} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ x_{j1} & x_{j2} & \cdots & x_{ji} & \cdots & x_{jj} & \cdots & x_{jn} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{ni} & \cdots & x_{nj} & \cdots & x_{nn} \end{pmatrix} = t_{ij}x =$$

$$xt_{ij} = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1i} & \cdots & x_{1i}+x_{1j} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2i} & \cdots & x_{2i}+x_{2j} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{i1} & x_{i2} & \cdots & x_{ii} & \cdots & x_{ii}+x_{ij} & \cdots & x_{in} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ x_{j1} & x_{j2} & \cdots & x_{ji} & \cdots & x_{ji}+x_{jj} & \cdots & x_{jn} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{ni} & \cdots & x_{ni}+x_{nj} & \cdots & x_{nn} \end{pmatrix}$$

Comparing row i and column j of the two matrices we observe that every non-diagonal entry of the i'th column and j'th row of x has to be zero, and $x_{ii} = x_{jj}$, that is,

$$x \in C_G(t_{ij}) \Leftrightarrow \begin{cases} x_{ii} = x_{jj} & \\ x_{st} = 0 & \text{if } s \neq t, \text{ and } s = j \text{ or } t = i \end{cases} \tag{6}$$

Hence for a fixed $k \neq m$ every t_{ij} where $i \neq m$ and $j \neq k$ belongs to $C_G(t_{km})$. Put $S_{km} = \{t_{ij} | i \neq m, j \neq k\}$.

Consider the following centralizer in G:

$$C_G(S_{km}) = \bigcap_{1 \leq i \neq m, j \neq k \leq n} C_G(t_{ij}) \tag{7}$$

Now assume $x \in C_G(S_{km})$ and consider x_{ij}, where $i \neq j$, and $(i,j) \neq (k,m)$. If $i \neq k$ and $j \neq m$, then $t_{ji} \in S_{km}$ and $x_{ij} = 0$ by (6). Assume $i = k$, but $j \neq m$. Then $t_{jm} \in S_{km}$. Again, by (6), $x_{ij} = 0$. The remaining case is similar. Therefore,

$$x \in C_G(S_{km}) \Rightarrow \begin{cases} x_{ij} = 0 & \text{if } i \neq j \text{ and } (i,j) \neq (k,m) \\ x_{ii} = x_{jj} & \text{for all } 1 \leq i,j \leq n \end{cases}$$

Note that if $x \in C_G(S_{km})$ and $x_{11} = \alpha, x_{km} = \beta$ then $x = d(\alpha)t_{km}(\alpha^{-1}\beta)$, so the scalar matrix $d(\alpha)$ belongs to G. It follows that $C_G(S_{km}) = R_G T_{km}$, where $R_G = R_n^\times \cap G$ is the subgroup of all scalar matrices from $R^\times$ that belong to G.

Observe, that any scalar matrix in G commutes with every transvection of the type $t_{ij}, i \neq j$. Hence

$$T_{km} = [C_G(S_{kj}), t_{jm}]$$

for any $j \neq k, m$. The subgroup $C_G(S_{kj})$ is Diophantine as the centralizer of finite set of transvections, therefore, the set T_{km} is also Diophantine.

□

Corollary 4.2. *Let $G = GL_n(R)$, $n \geq 3$. Then for any $1 \leq k \neq m \leq n$ the subgroup T_{km} is Diophantine in G (with constants $t_{ij}, 1 \leq i \neq j \leq n$).*

Corollary 4.3. *Let R be a commutative ring and $G = SL_n(R)$, $n \geq 3$. Then for any $1 \leq k \neq m \leq n$ the subgroup T_{km} is Diophantine in G (with constants $t_{ij}, 1 \leq i \neq j \leq n$).*

4.2 $UT_n(R)$ and $T_n(R)$ are Diophantine in large subgroups of $GL_n(R)$

We start with a simple lemma, which is used often in the paper.

Lemma 4.4. *Let $A_1, \ldots, A_k$ be Diophantine subsets of a group H. Then their product $A = A_1 \ldots A_k$ is also Diophantine in H.*

Proof. It suffices to note that $x \in H$ belongs to A if and only if the following condition holds:

$$\exists y_1 \ldots \exists y_k (a = y_1 \ldots y_k \wedge (\bigwedge_{i=1}^{k} (y_i \in A_i))$$

Since the sets A_i are Diophantine in H the condition above also describes a Diophantine subset of H. □

Proposition 4.5. *Let G be a large subgroup of $GL_n(R)$, $n \geq 3$. Then for every $1 \leq m \leq n-1$ the subgroup $UT_n^m(R)$ is Diophantine in G. In particular, $UT_n(R)$ is Diophantine in G.*

Proof. Fix $1 \leq m \leq n-1$, and let $UT_n^n(R) = \{1\}$. By (5) one has that

$$UT_n^m(R) = T_{n-m,n} T_{n-m-1,n-1} \ldots T_{1,1+m} UT_n^{m+1}(R)$$

Set

$$P_m = T_{n-m,n} T_{n-m-1,n-1} \ldots T_{1,1+m}$$

Then

$$UT_n^m(R) = P_m P_{m+1} \ldots P_{n-1} \tag{8}$$

This implies that each subgroup $UT_n^m(R)$ is a particular finite product of one parametric subgroups T_{ij}. By Lemma 4.1 every subgroup T_{ij} is Diophantine in G. Now the result follows from Lemma 4.4. □

Lemma 4.6. *Let G be a large subgroup of $GL_n(R)$, $n \geq 3$. Then the set R_G of all scalar matrices from G is Diophantine in G.*

Proof. Observe, that R_G is precisely the centralizer of the set of all transvections $\{t_{ij} \mid 1 \leq i \neq j \leq n\}$. Hence R_G is Diophantine in G. □

Proposition 4.7. *Let G be a large subgroup of $GL_n(R)$, $n \geq 3$. If R^+ does not have elements of order 2, then the following hold:*

1) *$G \cap D_n(R)$ is Diophantine in G.*

2) *$G \cap T_n(R)$ is Diophantine in G.*

Proof. To show 1) for any $1 \leq k \neq m \leq n$ let $d_{km} = d_k(-1)d_m(-1)$, i.e. $d_{km} = diag(\beta_1, \ldots, \beta_n)$, where $\beta_k = -1, \beta_m = -1$, and $\beta_i = 1$ if $i \neq k, m$. Note that for $x = (x_{ij}) \in GL_n(R)$ one has

$$xd_{km} = d_{km}x \iff \bigwedge_{i \neq m,k} \big[(-x_{im} = x_{im}) \wedge (-x_{mi} = x_{mi}) \wedge (-x_{ik} = x_{ik}) \wedge (-x_{ki} = x_{ki})\big]$$

Since R^+ does not have elements of order 2, as k ranges over all possible choices, the right-hand side of the relevant equivalences produce that $x_{mi} = x_{im} = 0$ for any $i \neq m$. Hence the system of equations

$$\bigwedge_{1 \leq i \neq j \leq n} xd_{ij} = d_{ij}x$$

defines $D_n(R)$ in G.

To prove 2) note first that the group $UT_n(R)$ is normal in $T_n(R)$. Hence $G \cap T_n(R) = (G \cap D_n(R))UT_n(R)$ is a product of two Diophantine subgroups of G (by the statement 1) above and Proposition 4.5). Therefore, by Lemma 4.4 $T_n(R)$ is Diophantine in G. □

4.3 Diophantine subgroups in $PGL_n(R)$ and $PSL_n(R)$

Let $\phi : GL_n(R) \to PGL_n(R)$ be the canonical epimorphism. The image of subgroup H of $GL_n(R)$ under ϕ will be denoted by H^ϕ. We call a subgroup G of $PGL_n(R)$ *large* if it contains $\phi(E_n(R))$, i.e., if $G = H^\phi$ for some large subgroup H of $GL_n(R)$. We note that for $1 \leq i \neq j \leq n$, $ker(\phi) \cap T_{ij} = \{I_n\}$, so indeed $T_{ij}^\phi \cong T_{ij}$.

Proposition 4.8. *Let G be a large subgroup of $PGL_n(R)$, where $n \geq 3$ and R has no zero-divisors. Then for any $1 \leq i \neq j \leq n$, the subgroup T_{ij}^ϕ is Diophantine in G.*

Proof. Let $H = \phi^{-1}(G)$, then H is a large subgroup of $GL_n(R)$. Consider the set $S_{km} = \{t_{ij} | i \neq m, j \neq k\}$, introduced in proof of Theorem 4.1 in H, and let $S^{\phi}_{km} = \{t^{\phi}_{ij} | i \neq m, j \neq k\}$. We see that for $y \in G$ and $x \in H$ with $\phi(x) = y$, $yt^{\phi}_{ij} = t^{\phi}_{ij}y$ if and only if there is $z \in R_H$, such that $t_{ij}x = xt_{ij}z$, for $x = (x_{st}) \in H$. Without loss of generality we can assume $i < j$. Then

$$\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1i} & \cdots & x_{1j} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2i} & \cdots & x_{2j} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{i1}+x_{j1} & x_{i2}+x_{j2} & \cdots & x_{ii}+x_{ji} & \cdots & x_{ij}+x_{jj} & \cdots & x_{in}+x_{jn} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ x_{j1} & x_{j2} & \cdots & x_{ji} & \cdots & x_{jj} & \cdots & x_{jn} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{ni} & \cdots & x_{nj} & \cdots & x_{nn} \end{pmatrix} = t_{ij}x =$$

$$xt_{ij}z = \begin{pmatrix} \alpha x_{11} & \alpha x_{12} & \cdots & \alpha x_{1i} & \cdots & \alpha(x_{1i}+x_{1j}) & \cdots & \alpha x_{1n} \\ \alpha x_{21} & \alpha x_{22} & \cdots & \alpha x_{2i} & \cdots & \alpha(x_{2i}+x_{2j}) & \cdots & \alpha x_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha x_{i1} & \alpha x_{i2} & \cdots & \alpha x_{ii} & \cdots & \alpha(x_{ii}+x_{ij}) & \cdots & \alpha x_{in} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \alpha x_{j1} & \alpha x_{j2} & \cdots & \alpha x_{ji} & \cdots & \alpha(x_{ji}+x_{jj}) & \cdots & \alpha x_{jn} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha x_{n1} & \alpha x_{n2} & \cdots & \alpha x_{ni} & \cdots & \alpha(x_{ni}+x_{nj}) & \cdots & \alpha x_{nn} \end{pmatrix}$$

where $z = \alpha I, \alpha \in R$. Consider the column i of both of the matrices, and compare the same non-diagonal (s, i)-entry, $s \neq i$, in the i-th column in the both matrices. Then $x_{si} = \alpha x_{si}$. Hence, either $x_{si} = 0$, or $\alpha = 1$ since R has no zero-divisors. Suppose $\alpha \neq 1$. Then $x_{si} = 0$ for all $s \neq i$. Now comparing the diagonal entries in the i's columns one has $x_{ii} + x_{ji} = \alpha x_{ii}$. Since $x_{ji} = 0$ it follows that $x_{ii} = \alpha x_{ii}$, so $x_{ii} = 0$. This means that the whole i's column in x consists of zeros, which contradicts the condition that $x \in GL_n(R)$ is an invertible matrix. Hence $\alpha = 1$. This shows that the equality $t_{ij}x = xt_{ij}z$ above becomes the equality $t_{ij}x = xt_{ij}$. Now, following the argument in Theorem 4.1, one has

$$[C_G(S^{\phi}_{kj}), t^{\phi}_{jm}] = [T_{kj}R_H, t_{jm}]^{\phi} = T^{\phi}_{km},$$

which indeed proves that T^{ϕ}_{km} is Diophantine in G.

□

Corollary 4.9. *If G is a large subgroup of $PGL_n(R)$, where R has no zero-divisors, $UT^{\phi}_n(R)$ is Diophantine in G.*

Proof. This is a direct corollary of Lemma 4.4 and Proposition 4.8. □

Corollary 4.10. *$G = PGL_n(R)$ or $G = PSL_n(R)$ is which case we assume R is commutative. If R does not have any zero-divisors, and R^+ has no elements of order 2, then the following hold:*

1. *$G \cap D_n^\phi(R)$ is Diophantine in G*
2. *$G \cap T_n^\phi(R)$ is Diophantine in G.*

Proof. Similar to the proof of Proposition 4.7, let $d_{ij} = d_i d_j$. Note that $d_{ij}^\phi \neq 1$. Let $G_1 = C_G(\{d_{ij}^\phi | 1 \leq i \neq j \leq n\}$, and $H_1 = C_H(\{d_{ij} | 1 \leq i \neq j \leq n\} = H \cap D_n(R)$. Let $y \in G_1$ and $\phi(x) = y$, $x \in H$. Now if $yd_{km}^\phi = d_{km}^\phi y$, then there exists $z = \alpha I \in R_H$ such that

$$\bigwedge_{i \neq k,m} \left[(-x_{im} = \alpha x_{im}) \wedge (-x_{mi} = \alpha x_{mi}) \wedge (-x_{ik} = \alpha x_{ik}) \wedge (-x_{ki} = \alpha x_{ki})\right],$$

and also $-x_{kk} = -\alpha x_{kk}$, and $-x_{mm} = -\alpha x_{mm}$. So $(1 - \alpha)x_{kk} = 0$. Since R has no zero divisors, either $\alpha = 1$ or $x_{kk} = 0$. Given what we want to prove we need to introduce a set of positive existential sentences that prevent the latter case. Without loss of generality we can assume $k = 1$. Recall that the T_{ij}^ϕ are Diophantine in G. So consider the positive existential sentences

$$\exists \bar{u}(\bigwedge_{1 \leq i \neq j \leq n} ((yd_{ij}^\phi = d_{ij}^\phi y) \wedge (yt_{ij}^\phi y^{-1} = u_{ij}) \wedge (u_{ij} \in T_{ij}^\phi)).$$

This means that x has to satisfy $xt_{1m} = t_{1m}(\beta_m)xz_m$ for some $\beta_m \in R$ and $z_m = \alpha_m I \in R_H$. Note that $\beta_m \neq 0$. Now we argue by contradiction that $x_{11} \neq 0$. So assume $x_{11} = 0$ and for each $m \neq 1$ apply the corresponding equation to x. A straightforward matrix calculation and comparing the $(1,1)$-entries of the resulting matrices on the two sides of the equation we get $0 = \beta_m \alpha_m x_{m1}$. Hence, for all m, $x_{m1} = 0$. That is, the first column of x consists entirely of zeros, making x non-invertible, which is impossible. This shows that $\alpha = 1$, which makes the rest similar to the proof of Proposition 4.7. □

5 Diophantine structure in large subgroups of $T_n(R)$

The following result is reminiscent of Theorem 4.1 on Diophantiness of one-parametric subgroups T_{ij} in large subgroups of $GL_n(R)$. However, since $T_n(R)$ has only transvections of the type $t_{ij}(\alpha)$ with $i < j$, the argument is a little bit more involved and the result is slightly weaker than in $GL_n(R)$. Though it is sufficient for all our purposes. Note that in the case of $G = UT_n(R)$ our argument follows considerations in [3].

Theorem 5.1. *Let G be a large subgroup of $T_n(R), n \geq 3$. Then the following hold:*

1) for every $1 \leq i, j \leq n$ with $j - i \geq 2$ the subgroup T_{ij} is Diophantine in G;

2) for every $1 \leq i < n$ the subgroup $R_G T_{i,i+1} T_{1n}$ is Diophantine in G.

Proof. We recall that for $x = (x_{ij}) \in G$

$$x \in C_G(t_{km}) \Leftrightarrow \begin{cases} x_{kk} = x_{mm} & \\ x_{ij} = 0 & \text{if } i \neq j, \text{ and either } j = k \text{ or } i = m \end{cases}$$

This implies that for $1 \leq k < m \leq n$ the centralizer of the set

$$S_{km} = \{t_{km}, t_{1i}, t_{jn} \mid i \neq 1, k; j \neq m, n\}$$

in G consists precisely of matrices $x = (x_{ij})$ with $x_{ij} = 0$ if $i < j$ and $(i, j) \notin \{(k, m), (1, m), (k, n), (1, n)\}$ and $x_{11} = \ldots = x_{nn}$. This set is Diophantine in G, we denote it by C_{km}.

It is convenient in calculations to represent an element $x = (x_{ij}) \in C_{km}$ as the following product, depending on k, m, and n. If $1 < k < m < n$ then

$$x = d(\sigma) t_{1m}(\sigma^{-1}\alpha) t_{km}(\sigma^{-1}\beta) t_{kn}(\sigma^{-1}\gamma) t_{1n}(\sigma^{-1}\delta),$$

where $x_{11} = \sigma, x_{1m} = \alpha, x_{km} = \beta, x_{kn} = \gamma$, and $x_{1n} = \delta$. If $1 = k < m < n$, then in the notation above

$$x = d(\sigma) t_{1m}(\sigma^{-1}\alpha) t_{1n}(\sigma^{-1}\delta).$$

If $1 < k < m = n$ then

$$x = d(\sigma) t_{kn}(\sigma^{-1}\gamma) t_{1n}(\sigma^{-1}\delta),$$

and in the case $1 = k, m = n$

$$x = d(\sigma) t_{1n}(\sigma^{-1}\delta).$$

The scalar matrix $d(\sigma)$ above belongs to G, since G contains x and $UT_n(R)$. Also note that C_{km} contains the whole subgroup R_G of all scalar matrices in G, since $[R_G, t_{ij}] = 1$ for any transvection t_{ij}. The argument above shows that

$$C_{km} = R_G T_{1m} T_{km} T_{kn} T_{1n}.$$

In particular, for any $j > 1$ and any $i < n$

$$C_{1j} = R_G T_{1j} T_{1n}, \quad C_{in} = R_G T_{in} T_{1n}. \tag{9}$$

It follows then that for $j > 2$

$$T_{1j} = [C_{1,j-1}, t_{j-1,j}],$$

hence it is Diophantine in G, because the set $C_{1,j-1}$ is. Similarly, for $i < n-1$ one has

$$T_{i,n} = [t_{i,i+1}, C_{i+1,n}],$$

hence it is also Diophantine in G.

Suppose now that $1 < i < j < n$, $j - i \geq 2$. Note that the set $[C_{i,j-1}, t_{j-1,j}]$ consists of all matrices $x = (x_{st}) \in G$ such that $x_{st} = 0$ for all $s < t$, provided $(s,t) \notin \{(1,j),(i,j)\}$. Clearly, this set is Diophantine. Similarly, the set $[t_{i,i+1}, C_{i+1,j}]$ is Diophantine and consists of matrices $X = (x_{st}) \in G$ such that $x_{st} = 0$, provided $s < t$ and $(s,t) \notin \{(i,j),(i,n)\}$. Therefore,

$$T_{ij} = [C_{i,j-1}, t_{j-1,j}] \cap [t_{i,i+1}, C_{i+1,j}],$$

so it is Diophantine as the intersection of two Diophantine sets. This proves 1).

To show 2), note, first, that (9) implies $R_G T_{12} T_{1n} = C_{12}$ and $R_G T_{n-1,n} T_{1n} = C_{n-1,n}$, so these sets are Diophantine in G.

Fix $1 < i < n-1$. Let $x = (x_{st}) \in C_{i,i+1}$. Then $[x, t_{i+1,i+2}] = t_{1,i+2}(\alpha) t_{i,i+2}(\beta)$, where $\sigma^{-1} x_{1,i+1} = \alpha$ and $\sigma^{-1} x_{i,i+1} = \beta$, where $\sigma = x_{11}$. Hence $x_{1,i+1} = 0$ if and only if

$$[x, t_{i+1,i+2}] = t_{i,i+2}(\beta) \in T_{i,i+2}.$$

This condition is Diophantine, since the set $T_{i,i+2}$ is Diophantine as shown in 1). Similarly, for such matrix x one has $x_{in} = 0$ if and only if $[t_{i-1,i}, x] \in T_{i-1,i+1}$. This condition is again Diophantine in G. The intersection of these conditions is Diophantine as well, and it describes the subgroup $R_G T_{i,i+1} T_{1n}$ in G. This proves 2).

□

Corollary 5.2. *Let $G = T_n(R)$, $n \geq 3$. Then the following hold:*

1) for every $1 \leq i, j \leq n$ with $j - i \geq 2$ the subgroup T_{ij} is Diophantine in G;

2) for every $1 \leq i < n$ the subgroup $R_G T_{i,i+1} T_{1n}$ is Diophantine in G.

Corollary 5.3. *Let $G = UT_n(R)$, $n \geq 3$. Then the following hold:*

1) for every $1 \leq i, j \leq n$ with $j - i \geq 2$ the subgroup T_{ij} is Diophantine in G;

2) for every $1 \leq i < n$ the subgroup $T_{i,i+1} T_{1n}$ is Diophantine in G.

Proposition 5.4. *Let G be a large subgroup of $T_n(R), n \geq 3$. Then:*

1) The subgroup R_G is e-interpretable in G.

2) The subgroup $R_G UT_n(R)$ is Diophantine in G.

Proof. To see 1) observe that $R_GT_{1n} = R_GT_{12}T_{1n} \cap R_GT_{23}T_{1n}$, so it is Diophantine as an intersection of two Diophantine subgroups of G (by Theorem 5.1). The subgroup T_{1n} is also Diophantine in G. Hence the quotient $R_GT_{1n}/T_{1n} \simeq R_G$ is e-interpretable in G.

The argument for 2) is similar to the one in Proposition 4.5. Indeed, from (8) $UT(n, R) = P_1 \ldots P_{n-1}$, where $P_m = T_{n-m,n}T_{n-m-1,n-1} \ldots T_{1,1+m}$.

By Theorem 5.1 and Lemma 4.4 all products $P_2, \ldots, P_{n-1}$ are Diophantine in G. Consider a product

$$P_1' = (R_GT_{n-1,n}T_{1n})(R_GT_{n-2,n-1}T_{1n}) \ldots (R_GT_{1,2}T_{1n}) = R_GP_1T_{1n}$$

By Theorem 5.1 and Lemma 4.4 P_1' is Diophantine in G. Hence

$$R_GUT_n(R) = P_1'P_2 \ldots P_{n-1}$$

is also Diophantine in G. Now 3) comes from 1) and 2), since R_G is a normal Diophantine subgroup of $R_GUT_n(R)$ and $UT_n(R) \simeq R_GUT_n(R)/R_G$. □

6 The Diophantine problem in classical linear groups

Theorem 6.1. *Let G be a large subgroup of $GL_n(R)$, $PGL_n(R)$ (assuming that R has no zero divisors in this case), or $T_n(R)$, $n \geq 3$. Then the ring R is e-interpretable in G.*

Proof. There are three cases to consider.

Case 1. G is a large subgroup of $GL_n(R)$. By Theorem 4.1 the subgroups T_{12}, T_{2n} and T_{1n} are Diophantine in G.

We e-interpret R on T_{1n} turning it into a ring $\langle T_{1n}; \oplus, \otimes\rangle$ as follows.

For $x, y \in T_{1n}$ define

$$x \oplus y = x \cdot y \tag{10}$$

Note that if $x = t_{1n}(\alpha), y = t_{1n}(\beta)$ then $x \cdot y = t_{1n}(\alpha + \beta)$, which corresponds to the addition in R.

To define $x \otimes y$ for given $x, y \in T_{1n}$ we need some notation. Let $x_1, y_1 \in G$ be such that

$$x_1 \in T_{12} \text{ and } [x_1, t_{2n}] = x, \quad y_1 \in T_{2n} \text{ and } [t_{12}, y_1] = y. \tag{11}$$

Note that such x_1, y_1 always exist and unique, for if $x = t_{1n}(\alpha), y = t_{1n}(\beta)$ then $x_1 = t_{12}(\alpha), y_1 = t_{2n}(\beta)$. Now define

$$x \otimes y = [x_1, y_1].$$

Observe, that in this case

$$[x_1, y_1] = [t_{12}(\alpha), t_{2n}(\beta)] = t_{1n}(\alpha\beta), \tag{12}$$

so $\otimes$ corresponds to the multiplication in R. To finish the proof we need two claims.

Claim 1. The map $\alpha \to t_{1n}(\alpha)$ gives rise to a ring isomorphism $R \to \langle T_{1n}; \oplus, \otimes\rangle$.

This is clear from the argument above.

Claim 2. The ring $\langle T_{1n}; \oplus, \otimes\rangle$ is e-interpretable in G.

To see this, observe first that, as was mentioned above, T_{1n} is Diophantine in G. The addition $\oplus$ defined in (10) is clearly Diophantine in G. Since the subgroups T_{12} and T_{2n} are Diophantine in G the conditions (11) are Diophantine in G, as well as the condition (12). This shows that the multiplication $\otimes$ is also Diophantine in G. This proves the case 1.

Case 2. Let G be a large subgroup of $PGL_n(R)$. The proof is similar to the one in Case 1. Only instead of Theorem 4.1 one uses Proposition 4.8.

Case 3. Let G be a large subgroup of $T_n(R)$. To prove that R is e-interpretable in G we adjust the argument above by making a few changes. Namely, we replace the subgroup T_{12} by the Diophantine subgroup $T'_{12} = R_G T_{12} T_{1n}$ if $n > 3$. If $n = 3$, then we also replace $T_{2n} = T_{23}$ with $T'_{23} = R_G T_{23} T_{13}$. In both cases the argument works word by word except for in these cases the elements $x_1 \in T'_{12}$ and $y_1 \in T'_{23}$ if $n = 3$, are not unique. However, this does not matter, since any such x_1 and y_1 give the same commutator $[x_1, y_1]$.

This proves the theorem. □

Corollary 6.2. *The ring R is e-interpretable in groups $GL_n(R)$, $SL_n(R)$ (assuming that in this case R is commutative), $E_n(R)$, $T_n(R)$, and $UT_n(R)$, where $n \geq 3$. If in addition R has no zero divisors then R is e-interpretable in $PGL_n(R)$ and $PSL_n(R)$ (as before, R is also commutative in this case).*

Remark 6.3. If $n \geq 3$, the ring R is e-interpretable in groups $GL_n(R)$, $PGL_n(R)$, $E_n(R)$ on each of the one parametric subgroups T_{ij}. The same holds for $T_n(R)$ and $UT_n(R)$, if $j - i \geq 2$. If in addition R is commutative then it is e-interpretable in $SL_n(R)$ and $PSL_n(R)$ on each of the one parametric subgroups T_{ij}.

Now we prove the converse of Theorem 6.1 (with exception for $E_n(R)$). The result, we believe, is known in folklore.

Proposition 6.4. *The groups $GL_n(R)$, $T_n(R)$, and $UT_n(R)$, are all e-interpretable in R. If R is commutative then the groups $PGL_n(R)$, $SL_n(R)$, and $PSL_n(R)$ are all e-interpretable in R.*

Proof. We represent an $n \times n$ matrix $x = (x_{ij})$ with entries in R by an n^2-tuple $\bar{x}$ over R, where

$$\bar{x} = (x_{11}, \ldots, x_{1n}, x_{21}, \ldots, x_{n1}, \ldots, x_{nn}).$$

The matrix multiplication $\odot$ on tuples from R^{n^2} is defined by

$$\bar{x} \odot \bar{y} = \bar{z} \Longleftrightarrow \bigwedge_{i,j=1}^{n} z_{ij} = P_{ij}(\bar{x}, \bar{y}),$$

where $P_{ij}(\bar{x}, \bar{y})$ is integer polynomial $\Sigma_{s=1}^{n} x_{is} y_{sj}$. The multiplication $\odot$ is clearly Diophantine. To finish the description of the interpretations of the groups $GL_n(R)$, $SL_n(R)$, $T_n(R)$, and $UT_n(R)$ in R it suffices to define the corresponding subsets of R^{n^2} by Diophantine formulas. We do it case by case.

The case of $GL_n(R)$. A matrix $x = (x_{ij})$ belongs to $GL_n(R)$ if it is invertible, i.e., there exists a matrix $y = (y_{ij})$ such that $xy = I_n$. In the language of the tuples $\bar{x}$ and $\bar{y}$ this is expressed as

$$\exists \bar{y} (\bar{x} \odot \bar{y}) = \bar{I}_n.$$

This condition is Diophantine, so $GL_n(R)$ is e-interpretable in R.

The case of $SL_n(R)$. In this case R is a commutative ring. Recall that the determinant of an $n \times n$-matrix (x_{ij}) with entries in a commutative ring R can be computed as the value of some fixed polynomial $Det_n(\bar{x})$ on the tuple $\bar{x}$. Hence the matrix $x = (x_{ij})$ belongs to $SL_n(R)$ if and only if $Det_n(\bar{x}) = 1$. This is a Diophantine equation in R.

The case of $PGL_n(R)$ and $PSL_n(R)$. Observe that if the ring R is commutative then the subgroup of all scalar matrices in $GL_n(R)$ and $SL_n(R)$ is Diophantine as the centralizer of the finite set of all transvections t_{ij}. Hence the factor groups $PGL_n(R)$ and $PSL_n(R)$ are e-interpretable, correspondingly, in the groups $GL_n(R)$ and $SL_n(R)$. Now the result follows from the previous two cases by transitivity of e-interpretability.

The case of $T_n(R)$. By definition $x = (x_{ij}) \in T_n(R)$ if and only if $x_{ij} = 0$ for all $i < j$ and there exists y in R such that $x_{11} \ldots x_{nn} y = 1$. All these conditions are Diophantine, so $T_n(R)$ is e-interpretable in R.

The case of $UT_n(R)$ is similar to the one above. This proves the proposition.

□

Now we can prove the main result of the paper.

Theorem 6.5. *Let $n \geq 3$. The Diophantine problem in each of the groups $GL_n(R)$, $SL_n(R)$ (assuming that in this case R is commutative), $T_n(R)$, and $UT_n(R)$, as well as in the groups $PGL_n(R)$ and $PSL_n(R)$ (in this case we additionally assume that the ring R has no zero divisors) is Karp equivalent to the Diophantine problem in R. In particular, the Diophantine problem in all these groups is decidable if and only if it is decidable in R.*

Proof. The result follows from Corollary 6.2, Proposition 6.4, and properties of the e-interpretability from Corollary 3.8. □

We are not able to show that $E_n(R)$ is e-interpretable in R for any associative ring R. However, the following holds.

Theorem 6.6. *If $E_n(R)$ has bounded elementary generation then $E_n(R)$ is e-interpretable in R. In this case the Diophantine problem in $E_n(R)$ is Karp equivalent to the Diophantine problem in R.*

Corollary 6.7. *If $n \geq 3$ and $E_n(R)$ has bounded elementary generation then the Diophantine problem in $E_n(R)$ is Karp equivalent to the Diophantine problem in R.*

For arbitrary associative ring R we have the following consequence of Corollary 6.2.

Proposition 6.8. *If the Diophantine problem is undecidable in a ring R then it is also undecidable in the group $E_n(R)$ for any $n \geq 3$.*

7 Diophantine problem in matrix groups over classical rings and fields

In this section we discuss Diophantine problem in the classical matrix groups over classical rings and fields.

As before by $G_n(R)$ we denote any of the classical linear groups $GL_n(R)$, $SL_n(R)$, $T_n(R)$, $UT_n(R)$, $PGL_n(R)$, $PSL_n(R)$ over a ring R (in the case of $SL_n(R), PGL_n(R)$ and $PSL_n(R)$ the ring R is assumed to be commutative). In fact, except for Lemma 7.1, all our rings R in this section will be either integral domains or fields.

In general, we consider the Diophantine problems of the type $\mathcal{D}_C(G_n(R))$, where C is a countable subset of $G_n(R)$ equipped with an enumeration $\nu : \mathbb{N} \to C$. Denote by $C_R \subseteq R$ the set of all elements of R that occur in matrices from C. Note that in the case of $PGL_n(R)$ or $PSL_n(R)$ we assume that elements from C (which are cosets of the center of $GL_n(R)$ or $SL_n(R)$) are given by some fixed representatives, i.e., matrices over R. The enumeration ν gives rise to an enumeration $\mu : \mathbb{N} \to C_R$, here to construct μ it suffices to enumerate matrices in C with respect to ν, for each matrix $\nu(n)$ enumerate its entries in some fixed order, and combine all these into an enumeration μ.

Lemma 7.1. *Let $G_n(R)$ be a classical matrix group over a ring R and C a countable subset of $G_n(R)$ equipped with an enumeration $\nu : \mathbb{N} \to C$. Then $\mathcal{D}_C(G_n(R))$ reduces to $\mathcal{D}_{C_R}(R)$.*

Proof. By Proposition 6.4, $G_n(R)$ is e-interpretable in R. Via this interpretation every finite system S of equations in $G_n(R)$ with coefficients in C can be reduced to a finite system S^* over R with coefficients in C_R, such that the map $S \to S^*$ gives the required reduction. □

This gives decidability of $\mathcal{D}_C(G_n(R))$, provided the Diophantine problem $\mathcal{D}_{C_R}(R)$ is decidable. Proving undecidability of $\mathcal{D}_C(G_n(R))$ might be more involved (see Theorem 7.8 below).

7.1 R is a ring of algebraic integers or a number field

By a *number field F* we mean a finite algebraic extension of $\mathbb{Q}$. The *ring of integers $\mathcal{O}$ of a number field F* is the subring of F consisting of all roots of monic polynomials with integer coefficients.

It is a classical result that the Diophantine problem in $\mathbb{Z}$ is undecidable [54]. Together with Theorem 6.5 this gives the following result.

Theorem 7.2. *Let $n \geq 3$. Then the Diophantine problem in the matrix groups $G_n(\mathbb{Z})$ is Karp equivalent to the Diophantine problem in $\mathbb{Z}$, in particular, it is undecidable.*

The following is one of the major conjectures in number theory.

Conjecture 1. The Diophantine problem in $\mathbb{Q}$, as well as in any number field F, or any ring of algebraic integers $\mathcal{O}$, is undecidable.

For $\mathbb{Q}$ and any its finite extension F the conjecture above is wide open. However, for the rings of algebraic integers $\mathcal{O}_F$ of the fields F there are results where the undecidability of the Diophantine problem is confirmed. Namely, it is known that $\mathbb{Z}$ is Diophantine in $\mathcal{O}_F$ if $[F : \mathbb{Q}] = 2$ or F is totally real [19, 20], or $[F : \mathbb{Q}] > 3$ and F has exactly two nonreal embeddings into the field of complex numbers [60], or F is an abelian number field [77]. We refer to two surveys and a book [62, 63, 78] for details on this matter.

If Conjecture 1 holds then the following conjecture also holds.

Conjecture 2. Let $n \geq 3$ and $R \in \{\mathbb{Q}, F, \mathcal{O}\}$, where F is a number field and $\mathcal{O}$ is a ring of algebraic integers. Then the Diophantine problem in the matrix groups $G_n(R)$ is undecidable.

7.2 R is an algebraically closed field

The following result is surely known in folklore, but we could not find a proper reference, so we give a sketch of a proof.

Proposition 7.3. *Let R be an algebraically closed field. Then the following hold:*

1) *If A is a computable subfield of R then the first-order theory $Th_A(R)$ of R with constants from A in the language is decidable. In particular, $\mathcal{D}_A(R)$ is decidable.*

2) Let C be a countable or finite subset of $G_n(R)$ such that the ring R_C is computable. Then the Diophantine problem in $G_n(R)$ with constants from C is decidable.

Proof. Let $\nu : \mathbb{N} \to A$ be an enumeration of A which makes A computable. Let $\bar{A}$ be the algebraic closure of A in R, i.e., the smallest algebraically closed subfield of R containing A. The enumeration ν extends to an enumeration of $\mu : \mathbb{N} \to \bar{A}$ which makes $\bar{A}$ computable [30]. Since the first-order theory of algebraically closed fields of a given characteristic admits elimination of quantifiers the whole theory $Th_A(\bar{A})$ reduces to the quantifier-free statements about $\bar{A}$, which is decidable since $\bar{A}$ is computable. Moreover, $\bar{A}$ is an elementary submodel of R, so $Th_A(\bar{A}) = Th_A(R)$. Hence $Th_A(R)$ is decidable, as claimed.

2) follows from Lemma 7.1 and 1). □

Now we turn to the case of classical fields with decidable first-order theory, such as $\mathbb{C}, \mathbb{R}$ and $\mathbb{Q}_p$, for arbitrary prime p. We also pay a special attention to the ring of p-adic integers $\mathbb{Z}_p$, because of its relations with pro-p completions of groups.

7.3 R is the field of reals

Let $R = \mathbb{R}$ be the field of real numbers and A a countable (or finite) subset of $\mathbb{R}$. In this section we discuss first when the Diophantine problem in $\mathbb{R}$ with constants from A (denoted by $D_A(\mathbb{R})$) is decidable and then apply these results to the Diophantine problems in classical matrix groups over $\mathbb{R}$.

Observe first, that by Lemma 3.3 if $D_A(\mathbb{R})$ is decidable then the subfield $F(A)$ generated by A in $\mathbb{R}$ is computable. However, the converse is not true. For example, as we mention below, if $a \in \mathbb{R}$ is not a computable real, then $F = \mathbb{Q}(a)$ is a computable field, but $\mathcal{D}_{\{a\}}(\mathbb{R})$ is undecidable. The following result clarifies the situation.

Proposition 7.4. *Let A be a finite or countable subset of $\mathbb{R}$. Then the Diophantine problem in $\mathbb{R}$ with coefficients in A is decidable if and only if the ordered subfield $F(A)$ is computable. Furthermore, in this case the whole first-order theory $Th_A(\mathbb{R})$ is decidable.*

Proof. Suppose A is a finite or countable subset of $\mathbb{R}$ with decidable $\mathcal{D}_A(\mathbb{R})$. By Lemma 3.3 the subfield $F(A)$ generated by A in $\mathbb{R}$ is computable. So it is suffices to show that the ordering $\leq$ induced from $\mathbb{R}$ on $F(A)$ is computable. Note, that $a \leq b$ in $\mathbb{R}$ if and only if the equation $b - a = y^2$ has a solution for y. Hence if $\mathcal{D}_A(\mathbb{R})$ is decidable then $\leq$ is computable on $F(A)$.

Let's prove the converse. Suppose $F(A)$ is computable ordered field. An equation $E(x_1, \ldots, x_n, a_1, \ldots, a_m) = 0$ in variables $x_1, \ldots, x_n$ and coefficients in $a_1, \ldots, a_m \in A$, has a solution in $\mathbb{R}$ if and only if the formula $\Phi(a_1, \ldots, a_m) =$

$\exists x_1 \ldots \exists x_n (E(x_1, \ldots, x_n, a_1, \ldots, a_m) = 0)$ is true in $\mathbb{R}$. Since $\mathbb{R}$ admits quantifier elimination in the language of ordered rings the formula $\Phi(y_1, \ldots, y_m)$ in free variables $y_1, \ldots, y_m$ is equivalent in $\mathbb{R}$ to a quantifier-free formula $\Psi(y_1, \ldots, y_m)$, therefore, $\Phi(a_1, \ldots, a_m)$ holds in $\mathbb{R}$ if and only if $\Psi(a_1, \ldots, a_m)$ holds in $\mathbb{R}$. The latter is algorithmically decidable since the ordered subfield $F(A)$ is computable.

Now we prove the last statement of the proposition. Let $\Phi(a_1, \ldots, a_n)$ be a sentence with coefficients from $F(A)$. Via quantifier elimination for real closed ordered fields we can assume that $\Phi(a_1, \ldots, a_n)$ is quantifier-free. But then whether it is true or not in $\mathbb{R}$ can be checked algorithmically since the field $F(A)$ is computable. This shows that $Th_A(\mathbb{R})$ is decidable. □

Recall that a real $a \in \mathbb{R}$ is *computable* if its standard decimal expansion $a = a_0.a_1a_2\ldots$ is computable, i.e., the integer function $n \to a_n$ is computable. In other words, a is computable if and only if one can effectively approximate it by rationals with any precision. The set of all computable reals $\mathbb{R}^c$ forms a real closed subfield of $\mathbb{R}$, in particular $\mathbb{R}^c$ is first-order equivalent to $\mathbb{R}$.

In the following Proposition we collect some facts about computable ordered subfields of $\mathbb{R}$. Statements 1) and 2) were proved in [44], 3) was proved in [46] (see also [29] (Theorem 4, Ch.6, section 3), and 4) is known in folklore. We are grateful to Andrey Morozov for helping us with computable ordered fields.

Proposition 7.5. *The following holds:*

1) *Every ordered computable subfield of $\mathbb{R}$ is contained in $\mathbb{R}^c$.*

2) *The ordered subfield $\mathbb{R}^c \leq \mathbb{R}$ with the induced order from $\mathbb{R}$ is not computable.*

3) *If F is a computable ordered field, then its real closure is also computable. In particular, if F is a computable subfield of $\mathbb{R}$ then the algebraic closure $\bar{F}$ of F in $\mathbb{R}$ is a computable ordered field.*

4) *If $a_1, \ldots, a_m$ are computable reals then the ordered subfield $\mathbb{Q}(a_1, \ldots, a_m) \leq \mathbb{R}$ with the induced order from $\mathbb{R}$ is computable.*

Proof. 1) and 2) were proved in [44]. Theorem 4 from section 3, chapter 6, of [29] states that if F_0 is an algebraic extension of a computable field F then a constructivization of F extends to a constructivization of F_0 if and only if the set of polynomials $f \in F[x]$ that have a root in F_0 is computably enumerable. In our case all polynomials $f \in F[x]$ that have a root in $\mathbb{R}$ have also a root in F. It suffices to show that the set of polynomials $f \in F[x]$ having a root in $\mathbb{R}$ is computably enumerable. For each $n \in \mathbb{N}$ consider a polynomial $h(x, z_0, \ldots, z_n) = z_n x^n + z_{n-1}x^{n-1} + \ldots + z_0$ and a formula $\Phi_n(z_0, \ldots, z_n) = \exists x h(x, \bar{z}) = 0$. By construction for any $a_0, \ldots, a_n \in \mathbb{R}$ the formula $\Phi_n(a_0, \ldots, a_n)$ holds in $\mathbb{R}$ if and only if the polynomial $a_n x^n + \ldots + a_0$ has a root in $\mathbb{R}$. Since $\mathbb{R}$ admits elimination of quantifiers (with $\leq$ in the language) for every n one can find a quantifier-free formula $\Phi'_n(z_0, \ldots, z_n)$ such that $\Phi'_n(a_0, \ldots, a_n)$ holds in $\mathbb{R}$ if and only if the polynomial $a_n x^n + \ldots + a_0$ has a root in $\mathbb{R}$. Now, if $a_0, \ldots, a_n$ are in F, since F is computable, one can algorithmically check whether or not $\Phi'_n(a_0, \ldots, a_n)$ holds in $\mathbb{R}$. Hence to computably enumerate all polynomials $f \in F[x]$ that have a root in $\mathbb{R}$ one can enumerate all polynomials $f_1, f_2, \ldots,$ in $F[x]$ and check, one-by-one, if f_i has a root in $\mathbb{R}$. This finishes 3).

To prove 4) consider a finite extension $\mathbb{Q}(t_1, \ldots, t_m, \alpha_1, \ldots, \alpha_k)$ of the field $\mathbb{Q}$. We can assume that $L = \mathbb{Q}(t_1, \ldots, t_m)$ is a pure transcendental extension, and $F = L(\alpha_1, \ldots, \alpha_k)$ is algebraic. It is easy to see that the field L is computable (see, for example, [29, 30]). We show, first, that the restriction of the ordering $\leq$ from $\mathbb{R}$ onto L is computable in L. Note, that viewing the field L as the field of rational functions in $t_1, \ldots, t_n$ with coefficients in $\mathbb{Q}$, it suffices to show that for any polynomial $f(\bar{x}) = f(x_1, \ldots, x_m)$ with rational coefficients one can algorithmically verify whether $f(\bar{t}) > 0$ or $f(\bar{t}) < 0$ (here $f(\bar{t}) = f(t_1, \ldots, t_m)$. Observe, that $f(\bar{t}) \neq 0$. The elements $t_1, \ldots, t_m$ are computable, so for every $s = 1, \ldots, m$ there are computable sequences of rationals $\{a_i^{(s)}\}_{i \in \mathbb{N}}$ and $\{b_i^{(s)}\}_{i \in \mathbb{N}}$, such that $\{a_i^{(s)}\}_{i \in \mathbb{N}}$ increases and converges to t_s and $\{b_i^{(s)}\}_{i \in \mathbb{N}}$ decreases and converges to t_s. Since $f(\bar{t}) \neq 0$ then in some small neighbourhood of the point $\bar{t} \in \mathbb{R}^m$ the polynomial $f(x_1, \ldots, x_m)$ is either strictly positive, or it is strictly negative. For $i \in \mathbb{N}$ consider a formula

$$\Phi_i = \exists y_1 \ldots \exists y_m \left(\bigwedge_{j=1}^{m} (a_i^{(j)} \leq y_j \leq b_i^{(j)}) \bigwedge (f(y_1, \ldots, y_m) = 0) \right).$$

Since the theory $Th(\mathbb{R})$ is decidable, one can algorithmically decide for every $i \in \mathbb{N}$ whether or not Φ_i holds in $\mathbb{R}$. Since $f(\bar{x})$ does not have zeros in some small neighborhood of $\bar{t}$ the formula Φ_i is not true in $\mathbb{R}$ for some i, which can be found. It follows that $f(\bar{x})$ is either positive or negative on the neighbourhood

$$U_i = \prod_{j=1}^{m} [a_i^{(j)}, b_i^{(j)}]$$

Hence, computing the value $f(a_i^{(1)}, \ldots, a_i^{(m)})$ one can find out if $f(\bar{t}) > 0$ or $f(\bar{t}) < 0$, as required.

Now, consider the algebraic extension $F = L(\alpha_1, \ldots, \alpha_k)$. We discuss only the case of $k = 1$, the general case can be argued similarly. Let $f = a_n x^n + \ldots + a_0$ be the minimal polynomial of $\alpha = \alpha_1$ over L, here $a_i = \frac{P_i(\bar{t})}{Q_i(\bar{t})}$ are rational functions in $t_1, \ldots, t_m$ with rational coefficients. It is easy to see that F is computable, one needs only to check that the ordering $\leq$ is computable on F. Take an arbitray element $b \in F$. We may assume that $b \neq 0$ and that it can be (algorithmically) presented as a non-trivial linear combination

$$b = \frac{P_0(\bar{t})}{Q_0(\bar{t})} \cdot 1 + \ldots + \frac{P_{n-1}(\bar{t})}{Q_{n-1}(\bar{t})} \alpha^{n-1}$$

of the basis $1, \ldots, \alpha^{n-1}$ of F over L. To check if $b > 0$ or $b < 0$ one can consider a rational function

$$h(\bar{x}, y) = \frac{P_0(\bar{x})}{Q_0(\bar{x})} \cdot 1 + \ldots + \frac{P_{n-1}(\bar{x})}{Q_{n-1}(\bar{x})} y^{n-1}$$

Notice that $h(\bar{t}, \alpha) \neq 0$. Hence in a small neighbourhood of $(\bar{t}, \alpha)$ the function $h(\bar{x}, y)$ is either strictly positive or strictly negative. The reals $t_1, \ldots, t_m, \alpha$ are computable so we can repeat the argument above to show that one can verify if $b > 0$ or $b < 0$. This proves 4).

□

Summarizing the discussion above we get the following result.

Corollary 7.6. *The following holds:*

- *The Diophantine problem in $\mathbb{R}$ with coefficients in $\mathbb{R}^c$ is undecidable;*
- *The Diophantine problem in $\mathbb{R}$ with coefficients in any finite subset of $\mathbb{R}^c$ is decidable;*
- *The Diophantine problem in $\mathbb{R}$ with coefficients in $\{a\}$, where a is not computable, is undecidable.*

Now we turn to the Diophantine problem in the classical matrix group over $\mathbb{R}$.

We say that a matrix $A \in GL_n(\mathbb{R})$ is *computable* if all entries in A are computable real numbers. Hence the computable matrices in $SL_n(\mathbb{R})$ are precisely the matrices from $SL_n(\mathbb{R}^c)$.

Theorem 7.7. *Let $n \geq 3$ and*

$$G_n(\mathbb{R}) \in \{GL_n(\mathbb{R}), SL_n(\mathbb{R}), T_n(\mathbb{R}), UT_n(\mathbb{R}), PGL_n(\mathbb{R}), PSL_n(\mathbb{R})\}.$$

If F is a computable ordered subfield of $\mathbb{R}$ then the first-order theory $Th(G_n(\mathbb{R}))$ with constants from $G_n(F)$ is decidable (here $G_n(F)$ is the set of all matrices from $G_n(\mathbb{R})$ with entries from F). In particular, the Diophantine problem for equations with coefficients from $G_n(F)$ is decidable in $G_n(\mathbb{R})$.

Proof. By Proposition 7.4 the theory $Th_F(\mathbb{R})$ is decidable. Since the group $G_n(\mathbb{R})$ is interpretable in the field $\mathbb{R}$ with no use of parameters (Theorem 6.4) the first-order theory of $G_n(\mathbb{R})$ with constants from $G_n(F)$ is decidable, as claimed. □

The following result complements the theorem above.

Theorem 7.8. *Let G be a large subgroup of $GL_n(\mathbb{R})$, where $n \geq 3$. If a matrix $A \in SL_n(\mathbb{R})$ is not computable then the Diophantine problem in G with coefficients in $\{t_{ij}\} \cup \{A\}$ is undecidable.*

Proof. Let G and $A \in SL_n(\mathbb{R})$ be as in the statement of the theorem. Assume that there exists an algorithm to decide whether a given finite systems of equations with coefficients in $\{t_{ij}\} \cup \{A\}$ has a solution in G. We show that in this case the matrix A is computable. The group $SL_n(\mathbb{R})$ is generated by transvections. Consider an arbitrary decomposition of A as a product of transvections:

$$A = t_{i_1 j_1}(\alpha_1) \dots t_{i_m j_m}(\alpha_m). \tag{13}$$

Consider the set S of all decompositions $A = t_{i_1 j_1}(\beta_1) \dots t_{i_m j_m}(\beta_m)$ with the fixed sequence of pairs of indexes $(i_1, j_1), \dots, (i_m, j_m)$ and fixed signs of the reals β_k, i.e., $sign(\beta_k) = sign(\alpha_k)$, $k = 1, \dots, m$. To simplify notation put $x_k(\beta) = t_{i_k j_k}(\beta)$. Now we show that there is a particular decomposition

$$A = x_1(\beta_1) \dots x_m(\beta_m),$$

where all reals $\beta_1, \dots, \beta_m$ are computable. For every $n \in \mathbb{N}$ define rational numbers $r_{1,n}, \dots, r_{m,n}$ by induction on n. Let $r_{k,0}$ be the integral part of the real number $|\alpha_k|$, where α_k, $k = 1, \dots, m$, are from (13). Suppose $r_{k,n-1}$, $k = 1, \dots, m$, are already defined. Let $(y_{1,n}, \dots, y_{m,n})$ be the smallest in the left-lexicographical order tuple of integers such that:

1) $0 \leq y_{k,n} \leq 9, \quad k = 1, \dots, m,$

2) there are reals $\gamma_{1,n}, \dots, \gamma_{m,n}$ such that $A = x_1(\gamma_{1,n}) \dots x_m(\gamma_{m,n})$,

3) $sign(\gamma_{k,n}) = sign(\alpha_k)$, $k = 1, \dots, m$, and

4) $0 \leq |\gamma_{k,n}| - (r_{k,n-1} + \frac{y_{k,n}}{10^n}) < \frac{1}{10^n}, \quad k = 1, \dots, m.$

Note that such a tuple $(y_{1,n}, \dots, y_{m,n})$ exists. Put $r_{k,n} = r_{k,n-1} + \frac{y_{k,n}}{10^n}$. Observe, that for every k the sequence $\{r_{k,n}\}_{n \in \mathbb{N}}$ is a Cauchy sequence, hence it converges to some real number β_k. Since $0 \leq |\gamma_{k,n}| - r_{k,n} < \frac{1}{10^n}$, the sequence $\{|\gamma_{k,n}|\}_{n \in \mathbb{N}}$ also converges to β_k, $k = 1, \dots, m$. Therefore, $\{\gamma_{k,n}\}_{n \in \mathbb{N}}$ converges to $\varepsilon_k \beta_k$, where $\varepsilon_k = sign(\alpha_k)$, $k = 1, \dots, m$.

Since $A = x_1(\gamma_{1,n}) \dots x_m(\gamma_{m,n})$ then there exist polynomials P_{ij} with integer coefficients such that for any $n \in \mathbb{N}$ the entry a_{ij} of A is equal to $P_{ij}(\gamma_{1,n}, \dots, \gamma_{m,n})$. It follows that for every i, j

$$a_{ij} = \lim_{n \to \infty} P_{ij}(\gamma_{1,n}, \dots, \gamma_{m,n}) = P_{ij}(\varepsilon_1 \beta_1, \dots, \varepsilon_m \beta_m).$$

Hence every entry a_{ij} is computable provided, the reals $\beta_1, \dots, \beta_m$ are computable. To prove that the real β_k is computable it suffices to show that the sequence of numbers $\{y_{k,n}\}_{n \in \mathbb{N}}$ is computable. We prove first that every condition 1)-4) can be described in the group G by Diophantine formulas. Indeed, 2) is Diophantine because the one-parametric subgroups T_{ij} are definable by Diophantine formulas with constants from $\{t_{ij}\}$ for each i, j. Note that the field $\mathbb{R}$ is e-interpretable in G by Theorem 6.1 and Remark 6.3 on every one-parametric subgroup T_{ij}. The predicate $x \leq y$ in $\mathbb{R}$ is Diophantine since it is equivalent to the condition $\exists z(y - x = z^2)$. Therefore, all the conditions 1), 3), 4) can also be described by Diophantine formulas. By our assumption there is an algorithm to decide whether a given finite system of equations with coefficients in $\{t_{ij}\} \cup \{A\}$ has a solution in G. This shows that for $n = 1, 2, \dots$ one can compute $y_{1,n}, \dots, y_{m,n}$. Hence the reals $\beta_1, \dots, \beta_m$ as well as the matrix A are computable. This proves the theorem.

□

Theorem 7.9. *The following holds:*

1) *The Diophantine problem in the computable real-closed field $\mathbb{R}^c$ with coefficients in $\mathbb{R}^c$ is undecidable, but for any finitely generated subfield F of $\mathbb{R}^c$ the Diophantine problem in $\mathbb{R}^c$ with coefficients in F is decidable.*

2) *The Diophantine problem in the computable matrix group $G_n(\mathbb{R}^c)$ is undecidable, provided $n \geq 3$. However, for any finitely generated subgroup C of $G_n(\mathbb{R}^c)$ the Diophantine problem in $G_n(\mathbb{R}^c)$ with coefficients in C is decidable.*

Proof. The ordered field $\mathbb{R}^c$ is not computable by Proposition 7.5. Hence by Proposition 7.4 the Diophantine problem in $\mathbb{R}^c$ with coefficients in $\mathbb{R}^c$ is undecidable. If F is a finitely generated subfield of $\mathbb{R}^c$ then by Proposition 7.5 it is a computable ordered field. Hence, by Proposition 7.4 the Diophantine problem in $\mathbb{R}^c$ with coefficients in $\mathbb{R}^c$ is decidable. This proves 1).

2) Follows from 1), Theorem 7.7 and the main Theorem 6.5.

□

7.4 Rings of p-adics: $\mathbb{Z}_p$ and $\mathbb{Q}_p$

Similarly, one can define computable p-adic numbers for every fixed prime p. Recall, that every p-adic number $a \in \mathbb{Q}_p$ has a unique presentation in the form $a = p^m\xi$, where $m \in \mathbb{Z}$ and ξ is a unit in the ring $\mathbb{Z}_p$. In its turn, the unit ξ is uniquely determined by a sequence of natural numbers $\{\xi(i)\}_{i \in \mathbb{N}}$, where

$$0 \leq \xi(i) < p^{i+1},\ \xi(i+1) = \xi(i)(\bmod p^{i+1}),\ (i \in \mathbb{N}).$$

The p-adic number $a = p^m\xi$ is computable if the sequence $i \to \xi(i)$ is computable. In this case the sequence $\{\xi(i)\}_{i \in \mathbb{N}}$ gives an effective p-adic approximation of ξ. It is known (see, for example [55]), that the set $\mathbb{Q}_p^c$ of all computable p-adic numbers forms a subfield of $\mathbb{Q}_p$, such that $\mathbb{Q}_p \equiv \mathbb{Q}_p^c$. Observe also that the ring $\mathbb{Z}_p$ is Diophantine in $\mathbb{Q}_p$. More precisely, if $p \neq 2$, then $\mathbb{Z}_p$ is defined in $\mathbb{Q}_p$ by formula $\exists y(1 + px^2 = y^2)$, while if $p = 2$ then $\mathbb{Z}_p$ is defined by the formula $\exists y(1 + 2x^3 = y^3)$ (see [29]).

Theorem 7.10. *[55] The following holds:*

1) $Th(\mathbb{Z}_p, a_1, \ldots, a_n)$ is decidable if and only if each of $a_1, \ldots, a_n$ is a computable p-adic number.

2) $Th(\mathbb{Q}_p, a_1, \ldots, a_n)$ is decidable if and only if each of $a_1, \ldots, a_n$ is a computable p-adic number.

We need a slightly more precise version of the results above in the case when the theory is undecidable.

Theorem 7.11. *The following holds:*

1) If a p-adic integer a is not computable then equations with constants from $\mathbb{Q} \cup \{a\}$ are undecidable in $\mathbb{Z}_p$.

2) If a p-adic number $a \in \mathbb{Q}_p$ is not computable then equations with constants from $\mathbb{Q} \cup \{a\}$ are undecidable in $\mathbb{Q}_p$.

Proof. For 1) we represent $a \in \mathbb{Q}_p$ in the form $a = p^m \xi$, where $m \in \mathbb{Z}$ and ξ is a unit in $\mathbb{Z}_p$. Note that $\mathbb{Z}_p$ is Diophantine in $\mathbb{Q}_p$, hence the argument from 1) could be adjusted in this case as well. □

We say that a matrix $A \in GL_n(\mathbb{Q}_p)$ is *computable* if all entries in A are computable p-adic numbers, i.e., $A \in GL_n(\mathbb{Q}_p^c)$. Hence the computable matrices in $SL_n(\mathbb{Q}_p)$ are precisely the matrices from $SL_n(\mathbb{Q}_p^c)$.

Theorem 7.12. *Let $n \geq 3$. The following holds:*

1) Let

$$G_n(\mathbb{Q}_p) \in \{GL_n(\mathbb{Q}_p), SL_n(\mathbb{Q}_p), T_n(\mathbb{Q})_p, UT_n(\mathbb{Q}_p), PGL_n(\mathbb{Q}_p), PSL_n(\mathbb{Q}_p)\}.$$

If $A_1, \ldots, A_m$ are computable matrices from $G_n(\mathbb{Q}_p)$ then the first-order theory of $G_n(\mathbb{Q}_p)$ with constants $A_1, \ldots, A_m$ is decidable. In particular, the Diophantine problem for equations with coefficients $A_1, \ldots, A_m$ is decidable in $G_n(\mathbb{Q}_p)$.

2) Let

$$G_n(\mathbb{Z}_p) \in \{GL_n(\mathbb{Z}_p), SL_n(\mathbb{Z}_p), T_n(\mathbb{Z})_p, UT_n(\mathbb{Z}_p), PGL_n(\mathbb{Z}_p), PSL_n(\mathbb{Z}_p)\}.$$

If $A_1, \ldots, A_m$ are computable matrices from $G_n(\mathbb{Z}_p)$ then the first-order theory of $G_n(\mathbb{Z}_p)$ with constants $A_1, \ldots, A_m$ is decidable. In particular, the Diophantine problem for equations with coefficients $A_1, \ldots, A_m$ is decidable in $G_n(\mathbb{Z}_p)$.

Proof. It follows from Theorem 7.10 and Proposition 6.3. □

Theorem 7.13. *If a matrix $A \in SL_n(\mathbb{Z}_p)$ ($A \in SL_n(\mathbb{Q}_p)$) is not computable then Diophantine problem for equations with coefficients in $\{t_{ij}\} \cup \{A\}$ is undecidable in $SL_n(\mathbb{Z}_p)$ ($SL_n(\mathbb{Q}_p)$).*

Proof. Follows from Theorem 7.11 in a fashion similar to Theorem 7.8. □

References

[1] J. Ax, S. Kochen, Diophantine problems over local fields. I, II, Amer. J. Math. 1965, 87, 605-648.

[2] J. Ax, S. Kochen, Diophantine problems over local fields. III, Amer. J. Math. 1966, 83, 437-456.

[3] O. V. Belegradek, The model theory of unitriangular groups, Ann. Pure App. Logic, 68 (1994) 225-261.

[4] C. Beidar, A. Michalev, On Malcev's theorem on elementary equivalence of linear groups, Contemporary mathematics, 1992, V. 131, P. 29-35.

[5] E. Bunina, Elementary equivalence of unitary linear groups over fields. Fund and Applied Math, 1998, v. 4, 4, p. 1265-1278.

[6] E. Bunina, Elementary equivalence of unitary linear groups over rings and skew fields. Uspehi mat nauk, 1998, v 53, 2, p. 137-138.

[7] E. Bunina, Elementary equivalence of Chevalley groups, Uspehi Mat. Nauk, 2001, v.56, 1, p.157-158.

[8] E. Bunina, Elementary equivalence of Chevalley groups over local rings, Mat. Sbornik, 2010, v. 201, 3, p.101-120.

[9] E. I. Bunina, "Isomorphisms and elementary equivalence of Chevalley groups over commutative rings", Sb. Math., 210, 8 (2019), p. 1067–1091.

[10] E. Bunina, A. Mikhalev, A. Pinus, Elementary equivalence and close to it logical equivalences of classical and universal algebras.

[11] D. Carter, G. Keller Bounded Elementary Generation of $SL_n(\mathcal{O})$, American Journal of Mathematics Vol. 105, No. 3, 1983, pp. 673-687.

[12] M. Casals-Ruiz, I. Kazachkov, On systems of equations over free products of groups, Journal of Algebra, 333, 1, 2011, 368 - 426.

[13] M. Casals-Ruiz, I. Kazachkov, On Systems of Equations Over Free Partially Commutative Groups, Memoirs of the American Mathematical Society, 2011, American Mathematical Society.

[14] L. Ciobanu, V. Diekert and M. Elder, Solution sets for equations over free groups are EDT0L languages, International Journal of Algebra and Computation, 2016, Vol. 26, No. 05, pp. 843-886.

[15] L. Ciobanu, M. Elder, The complexity of solution sets to equations in hyperbolic groups, arXiv:2001.09591 [math.GR].

[16] F. Dahmani, V. Guirardel, Foliations for solving equations in groups: free, virtually free, and hyperbolic groups, Journal of Topology, 3,2, 2016, 343-404.

[17] M. Davis, H. Putnam, J. Robinson, The Decision Problem for Exponential Diophantine Equations, Annals of Mathematics, 3, 74,1961, 425–436.

[18] J. Denef, L. Lipshitz, Diophantine Sets over Some Rings of Algebraic Integers, Journal of the London Mathematical Society, s2-18, 3, 1978, 385–391.

[19] J. Denef, Hilbert's Tenth Problem for quadratic rings, Proc. Amer. Math. Soc. 48, 1975, 214–220.

[20] J. Denef, Diophantine sets of algebraic integers, II, Trans. Amer. Math. Soc. 257, 1980, 227–236.

[21] R. Dennis, K. Vaserstein, On a Question of M. Newman on the Number of Commutators, Journal of Algebra Volume 118, Issue 1, October 1988, Pages 150-161.

[22] V. Diekert, A. Jeż, W. Plandowski. Finding all solutions of equations in free groups and monoids with involution. Inf. Comput., 2016, 251, 263–286.

[23] V. Diekert, M.Lohrey, Word equations over graph products, International Journal of Algebra and Computation, 18, 3, (2008), 493-533.

[24] V. Diekert, A. Muscholl, Solvability of equations in graph groups is decidable, International Journal of Algebra and Computation, 16, 6, 2006, 1047-1069.

[25] D. L. Dubrovsky, Some subfields of $\mathbb{Q}_p$ and their non-Standard analogies, Can. J. Math. 1974. V. 26, No 2. P. 473—491.

[26] M. Duchin, H. Liang, M. Shapiro, Equations in nilpotent groups, Proc. Amer. Math. Soc., 2015, 143, 11, 4723-4731.

[27] P. C. Eklof, and R. F. Fischer, The elementary theory of abelian groups, Ann. Math. Logic, 4(2) (1972) 115-171.

[28] Y. Ershov, On elementary theories of local fields, Algebra i Logika, Sem 4, (1965), 2, 5-30.

[29] Y. Ershov, Decidability problems and constructible models, Moscow, Nauka, 1980.

[30] Y. Ershov, Algorithmic problems of the theory of fields (positive aspects), Handbook of Mathematical Logic, 3, 268–353, Nauka, Moscow, 1982.

[31] Y. Ershov and S. S. Goncharov, Constructive models. Siberian School of Algebra and Logic. Consultants Bureau, New York, 2000.

[32] N. Garcia-Fritz, H. Pasten, Towards Hilbert's Tenth Problem for rings of integers through Iwasawa theory and Heegner points, arXiv e-prints, 2019, arXiv:1909.01434.

[33] A. Garreta, A. Miasnikov, D. Ovchinnikov, *Full rank presentations and nilpotent groups: structure, Diophantine problem, and genericity*, Journal of Algebra, Volume 556, 15 August 2020, Pages 1-34.

[34] A. Garreta, A. Miasnikov, D. Ovchinnikov, Diophantine problems in solvable groups, Bulletin of Mathematical Sciences, Vol. 10, No. 1 (2020), 27 pages. DOI: 10.1142/S1664360720500058

[35] A. Garreta, A. Miasnikov, D. Ovchinnikov, Diophantine problems in rings and algebras: undecidability and reductions to rings of algebraic integers, arXiv:1805.02573 [math.RA]

[36] A. Garreta, A. Miasnikov, D. Ovchinnikov, Diophantine problems in commutative rings, arXiv:2012.09787 [math.NT].

[37] A. Jeż, Recompression: a simple and powerful technique for word equations, Journal of the ACM, 63(1):4:1–4:51, Mar 2016. ISSN 0004-5411/2015. doi: 10.1145/2743014. URL http://dx.doi.org/10.1145/2743014.

[38] A. Jeż, Word equations in linear space, arXiv:1702.00736 [cs.FL]

[39] M. Kargapolov, Yu. Merzljakov, Fundamentals of the Theory of Groups, Graduate Texts in Mathematics, 1979, Springer.

[40] O. Kharlampovich and A. Myasnikov, *Irreducible affine varieties over a free group. II: Systems in triangular quasi-quadratic form and description of residually free groups.* J. of Algebra, v. 200, no. 2, 517–570, 1998. MR 2000b:20032b

[41] O. Kharlampovich, A. Myasnikov, "Model theory and algebraic geometry in groups, non-standard actions and algorithmic problems", Proceedings of the Intern. Congress of Mathematicians 2014, Seoul, v. 2, invited lectures, 223-244.

[42] O. Kharlampovich and A. G. Miasnikov, Undecidability of Equations in Free Lie Algebras, Transactions of the American Mathematical Society, 2017, 08,

[43] O. Kharlampovich, A. Myasnikov, Equations in Algebras, International Journal of Algebra and Computation, 28, 8, 2018, 1517-1533.

[44] A. Lachlan and E. Madison, Computable Fields and Arithmetically Definable Ordered Fields, Proceedings of the American Mathematical Society, Vol. 24, No. 4 (Apr., 1970), pp.803-807

[45] N. Avni, A. Lubotsky, and C. Meiri, First order rigidity of non-uniform higher rank arithmetic groups, Inventiones mathematicae,2019, v. 217, p. 219–240.

[46] E. Madison, A note on computable real numbers, The Journal of Symbolic Logic, Volume 35, Number 2, June 1970, p.239-241.

[47] G. S. Makanin, Equations in a free group, Mathematics of the USSR-Izvestiya, 21, 3, 1983, 483.

[48] G. S. Makanin. *Equations in a free group* (Russian). Izv. Akad. Nauk SSSR, Ser. Mat., 46:1199–1273, 1982. transl. in Math. USSR Izv., V. 21, 1983; MR 84m:20040.

[49] G. S. Makanin. *Decidability of the universal and positive theories of a free group* Izv. Akad. Nauk SSSR, Ser. Mat., 48(1):735–749, 1985. transl. in Math. USSR Izv., V. 25, 1985; MR 86c:03009.

[50] A. I. Malcev, On a correspondence between rings and groups, Amer. Math. Soc. Transl., 1960, 45, 2, 221-231.

[51] A. Malcev, On elementary properties of linear groups, Problems of mathematics and mechanics, Novosibirsk, 1961, 110-132.

[52] A. Malcev, Constructive algebras I, Yspehi, Mat. Nayk, 1961, 3, p.3-60.

[53] D. Marker, Model theory: An introduction, Springer, Graduate Texts in Mathematics, 217, 2010.

[54] Y. Matijasevič. The Diophantineness of enumerable sets.Doklady AkademiiNauk SSSR, 191:279–282, 1970.

[55] A. Myasnikov and V. Remeslennikov, Recursive p-adic numbers and elementary theories of finitely generated pro-p groups, 1988 American Mathematical Society, Mathematics of the USSR-Izvestiya, Volume 30, Number 3.

[56] A. G. Myasnikov and M. Sohrabi, Elementary coordinatization of finitely generated nilpotent groups, arXiv:1311.1391

[57] A. G. Myasnikov and M. Sohrabi, On groups elementarily equivalent to a group of triangular matrices $T_n(R)$, arXiv:1609.09802

[58] A. G. Myasnikov, M. Sohrabi, Bi-interpretability with $\mathbb{Z}$ and models of the complete elementary theories of $SL(n, O)$, $T(n, O)$ and $GL(n, O)$, $n \geq 3$, arXiv:2004.03585

[59] F. Oger, G. Sabbagh, Quasi finitely axiomatizable nilpotent groups, J. Group Theory, 9 (2006) 95-106.

[60] T. Pheidas, Hilbert's Tenth Problem for a class of rings of algebraic integers, Proc. Amer. Math. Soc. 104, 1988, 611–620.

[61] T. Pheidas, Hilbert's Tenth Problem for fields of rational functions over finite fields, Inventiones mathematicae, 1991, 103,1, 1-8.

[62] T. Pheidas, K. Zahidi, Undecidability of existential theories of rings and fields: A survey, Contemporary Mathematics, 270, 2000, 49-106.

[63] B. Poonen, Hilbert's Tenth Problem over rings of number-theoretic interest, Notes for Arizona Winter School on "Number theory and logic",2003.

[64] A. Prestel, P. Roquette, Formally p-adic fields, Lec. Notes in Math., 1050, Springer-Verlag, 1984.

[65] M. Rabin, Computable algebra, general theory and theory of computable fields, Trans Amer. Math. Soc., 1960, 95, 2, p.341-360.

[66] A. Razborov. *On systems of equations in a free group.* Math. USSR, Izvestiya, 25(1), , 1985, 115-162.

[67] A. Razborov. *On systems of equations in a free group.* PhD thesis, Steklov Math. Institute, Moscow, 1987.

[68] H. G. Rice, Recursive real number, Proc Amer. Math. Soc. 1954. V. 5. P. 784—791.

[69] E. Rips, Z. Sela, Canonical representatives and equations in hyperbolic groups, Inventiones mathematicae, 1995, 120, 1, 489–51.

[70] J. Robinson, The undecidability of algebraic rings and fields, Proc. Amer. Math. Soc. 10 (1959) 950-957.

[71] N. S. Romanovskii, On the elementary theory of an almost polycyclic group, Math. USSR Sbornik, 39(2) (1981) 125-132.

[72] V. A. Romankov, Width of subgroups in solvable groups, Algebra and Logic 21 (1982), 41-49.

[73] V. Romankov, Universal theory of nilpotent groups, Mat. Zametki, 25, 1979, 4, 487–495.

[74] V. Romankov, Equations in free metabelian groups, Siberian Mathematical Journal, 1979, 1, 20, 469-471.

[75] V. Romankov, Unsolvability of the endomorphic reducibility problem in free nilpotent groups and in free rings, Algebra and Logic, 1977, 1,16, 4, 310–320.

[76] D. Segal, Polycyclic Groups, Cambridge University Press, 1983.

[77] H. N. Shapiro, A. Shlapentokh, Diophantine relationships between algebraic number fields, Communications on Pure and Applied Mathematics, 42,8, 1989, 1113–1122.

[78] A. Shlapentokh, Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields, New Mathematical Monographs, 2007, Cambridge University Press.

[79] A. Tarski, A decision method for elementary algebra and geometry, 2nd revised ed., Berkeley, Los Angeles, 1951.

[80] A. M. Turing, On computable numbers, with an application to the Eutschelidungs problem, Proc. London Math. Soc., Ser. 2, 1936, v. 42, p. 236—265.

[81] W. van der Kallen, $SL_3(\mathbb{C}[x])$ does not have bounded word length, Lec. Notes in Math., v.966, 1982,p. 357-361.