UDC 512.54 + 510.5

R.K. Tyulyubergenev

D.Serikbayev East Kazakhstan State Technical University, Ust-Kamenogorsk, Kazakhstan
(E-mail: rustem.tylybergenev@gmail.com)

On computable subgroups of the group of all unitriangular matrices over a ring

The problems of existence and uniqueness of computable numberings are fundamental in theory of computably numbered groups. In connection with the development of the theory of algorithms a study of the problems of computability of important classes of algebraic systems are currently relevant. Groups of unitriangular matrices over the ring are a classic representative of the class of nilpotent groups and have numerous applications both in group theory and in its applications. In this paper we obtain a criterion of computability of subgroups of the group of all unitriangular matrices $UT_n(K)$ over a computable associative ring with unity.

Keywords: numbering, group of unitriangular matrices, constructive group, nilpotent subgroup, subgroup, rational number, theory of algorithms.

Let ω be the set of natural numbers, G a group, and $\nu : \omega \longrightarrow G$ a mapping from ω onto G, also called a *numbering* of G. The pair (G, ν) is called a *constructive group* if there is an algorithm which, for any triple of natural numbers n, m and s, determines whether the equalities $\nu n = \nu m$ and $\nu n \cdot \nu m = \nu s$ are true. A group G is called *computable* (or *constructivizable*) if there exists a numbering ν such that the pair (G, ν) is a constructive group. A subgroup H of a numbered group (G, ν) is called *computable* (*computably enumerable*) in (G, ν) if the set $\nu^{-1}H$ is computable (computably enumerable). If (G, ν) is a constructive group, then ν is called a *computable numbering* of the group G. The problems of existence and uniqueness of computable numberings are fundamental here, i.e., which groups are computable, and, if they are, how many non-equivalent computable numberings do they admit. These problems have been investigated by A.I. Malcev, Yu.L. Ershov, S.S. Goncharov, R. Downey, J. Knight, A.S. Morozov, V.A. Roman'kov, V.P. Dobritsa, N.G. Khisamiev, I.V. Latkin and other authors.

V. Roman'kov and N. Khisamiev proved [1] that the group $UT_n(K)$ of all unitriangular matrices, $n \geq 3$, over a commutative associative ring K with unity, is computable if and only if K is computable (where a *computable ring* is defined in the obvious way, following the definition of a computable group). In [2] the same authors constructed a ring K that is not computable, but the group $UT_2(K)$ is computable. Let $\mathbb{Q}$ be the additive group of rational numbers. In [3] A.I. Malcev proved that a subgroup $G \leq \mathbb{Q}^n$ is computable if and only if G is a computably enumerable subgroup in $(\mathbb{Q}^n, \gamma)$, where γ is a standard numbering of the set of n-tuples of rational numbers. In [4] it is obtained criteria for computability of torsion-free nilpotent groups of finite dimension and it is proved the existence of a principal computable numbering of the class of all computable torsion-free nilpotent groups of finite dimension. In this article we obtain a criterion of computability of subgroups of the group of all unitriangular matrices $UT_n(K)$ over a computable associative ring with unity.

Our basic references for models, groups and rings are respectively [5–7], of which we adopt terminology and notations. If in a torsion-free abelian group A there is a finite maximal linearly independent system of elements, then we say that the *dimension* of the group A is *finite*. If a nilpotent torsion-free group G has a central series whose factors are all abelian groups of finite dimensions, then G is called a group of *finite dimension*.

Theorem 1. Let (G, ν) be a constructive nilpotent torsion-free group of finite dimension, and let

$$e = G_0 < G_1 < \ldots < G_n = G, \tag{1}$$

be a central series of G. Then each G_i is a computable subgroup in (G, ν), for all $i \leq n$.

Proof. By induction on i. The claim is obvious for $i = 0$. Suppose that the claim holds of i, and

$$g_{k1}, g_{k2}, \ldots, g_{km_k};$$

are elements of G such that the sequence

$$\overline{g}_{k1}, \overline{g}_{k2}, \ldots, \overline{g}_{km_k},$$

is a maximal linearly independent system of elements of the quotient $\overline{G}_k = G_k/G_{k-1}$, $0 < k \le n$. Since (1) is a central series of the group G, the equivalence

$$g \in G_{i+1} \Longleftrightarrow g_{kj} \cdot g = g \cdot g_{kj} \mod G_i, \tag{2}$$

holds, i.e., $[g_{kj}, g] \in G_i$, for all $0 < k \le n$, $0 < j \le m_k$.

Let $m_{kj} \in \omega$ be numbers such that $\nu m_{kj} = g_{kj}$. Then (2) yields

$$s \in \nu^{-1}G_{i+1} \Longleftrightarrow [\nu m_{kj}, \nu s] \in G_i, \quad 0 < k \le n,\ 0 < j \le m_k. \tag{3}$$

Since, by the induction hypothesis, the subgroup G_i is computable in the constructive group (G, ν), the right-hand side of (3) can be effectively verified. From this, the set $\nu^{-1}G_{i+1}$ is computable, i.e., the subgroup G_{i+1} is computable in (G, ν). The theorem is proved.

Corollary 1. If G is a computable nilpotent torsion-free group of finite dimension, then the factors of any central series of G are computable.

Let K be a computable associative ring with unity, and $UT_n(K)$ the group of all unitriangular matrices over K, of order $n \ge 2$. From any computable numbering γ of the ring K one can determine a numbering γ_* of the group $UT_n(K)$, such that from a γ_*-number of a matrix A one can effectively find γ-numbers of the elements of the matrix A.

Theorem 2. A subgroup G of the group $UT_n(K)$ of all unitriangular matrices over a computable associative ring K, whose additive group is torsion-free and of finite dimension, is computable if and only if G is a computably enumerable subgroup in $(UT_n(K), \gamma_*)$, i.e., the set $\gamma_*^{-1}G$ is computably enumerable.

Proof. Let μ be a computable numbering of G and let

$$e = G_0 < G_1 < \ldots < G_m = G,$$

be a central series such that each quotient $\overline{G}_i = G_i/G_{i-1}$, $0 < i \le m$, is an abelian group of finite dimension. By Theorem 1, the set $\mu^{-1}G_i$ is computable. Let

$$\overline{g}_{i1}, \overline{g}_{i2}, \ldots, \overline{g}_{im_i},$$

be a maximal linearly independent system of elements in the quotient $\overline{G}_i$. In each class $\overline{g}_{ij}$, $0 < j \le m_i$, we fix a matrix A_{ij}. Since there are finitely many such matrices, we can assume that γ-numbers of the elements of these matrices are known.

By induction on i, we prove that the subgroup G_i is computably enumerable in $(UT_n(K), \gamma_*)$, and from any number $s \in \mu^{-1}G_i$ one can effectively find t such that $\mu s = \gamma_* t$. This is obvious for $i = 0$. Assume that for i it has been proved that $\gamma_*^{-1}G_i$ is a computably enumerable set of numbers, and there exists a partial computable function f_i, with domain $\delta f_i = \mu^{-1}G_i$, such that $\mu k = \gamma_* f_i(k)$, for all $k \in \mu^{-1}G_i$.

By definition of the matrices A_{i+1j}, $0 < j \le m_{i+1}$, the following holds: For every $k \in \omega$, we have that $\mu k \in G_{i+1}$ if and only if there are integers $s, t, r_1, r_2, \ldots, r_{m_{i+1}}$, with $t \in \mu^{-1}G_i$, such that

$$(\mu k)^s = A_{i+11}^{r_1} \cdot \ldots \cdot A_{i+1m_{i+1}}^{r_{m_{i+1}}} \cdot \mu t. \tag{4}$$

Suppose that (4) is true. By induction, $\mu t = \gamma_* f_i(t)$. By definition of the numbering γ_* of the group $UT_n(K)$, it follows that from the number $f_i(t)$ we can effectively find γ-numbers of the elements of the matrix $B = \gamma_* f_i(t)$. Hence from the numbers $r_1, r_2, \ldots, r_{m_{i+1}}$ we can effectively find γ-numbers of the elements of the matrix

$$C = A_{i+11}^{r_1} \cdot \ldots \cdot A_{i+1m_{i+1}}^{r_{m_{i+1}}} \cdot B.$$

Since $UT_n(K)$ is a nilpotent torsion-free group, roots of elements when they exist are unique, see [6, Theorem 16.2.8]. So, from C we can effectively determine a unique D, and r, such that $D^s = C$, and $\gamma_* r = D$. From this and (4) it follows that there is an algorithm that lists the γ_*-numbers of matrices of the subgroup G_{i+1}, and from a number $k \in \mu^{-1}G_{i+1}$ one can effectively find γ-numbers of the elements of the matrix μk, hence a number s such that $\mu k = \gamma_* s$, therefore completing the proof of the induction step.

Thus, $G_m = G$ is a computably enumerable subgroup in $(UT_n(K), \gamma_*)$, i.e., necessity has been proved.

Sufficiency follows from the fact that a computably enumerable subgroup of a constructive group is computable. This completes the proof of the theorem.

Let ν_1 and ν_2 be two computable numberings of the group G. Then say that ν_1 is *m-reducible to* ν_2 if there is a computable function f such that $\nu_1 n = \nu_2 f(n)$, for all $n \in \omega$. If all computable numberings are m-reducible to each other, then the group is called *computably stable*.

From the proof of the previous theorem we have:

Corollary 2. If G is a computable subgroup of the group $UT_n(K)$ over a computable associative ring K with unity, whose additive group is torsion-free and of finite dimension, then any computable numbering of the group G is m-reducible to the numbering γ_* of the group $UT_n(K)$.

Corollary 3. Any computable subgroup of the group $UT_n(K)$ over a computable associative ring K with unity, whose additive group is torsion-free and of finite dimension, is computably stable.

Corollary 4. A subgroup G of the group $UT_n(P)$ of all unitriangular matrices over a field P of finite degree and of characteristic 0, is computable if and only if G is a computably enumerable subgroup in $(UT_n(P), \gamma_*)$.

Corollary 5. If G is a computable subgroup of the group $UT_n(P)$ over a field P of finite degree and of characteristic 0, then any computable numbering of G is m-reducible to the numbering γ_* of the group $UT_n(P)$.

In particular, Corollaries 4 and 5 are valid when P is the field of rational numbers.

Let K be a computable associative ring with unity, whose additive group is torsion-free and of finite dimension, let G be a subgroup of the group of unitriangular matrices $UT_n(K)$, and let

$$e = G_0 < G_1 < \ldots < G_n = G, \quad (5)$$

be a central series of it. Let us fix some maximal linearly independent system

$$\overline{A}_{i1}, \overline{A}_{i2}, \ldots, \overline{A}_{im_i}$$

in the quotient $\overline{G}_i = G_{i+1}/G_i$, $i < n$. Let

$$S_i(G) = \{\langle \alpha_{i0}, \alpha_{i1}, \cdots, \alpha_{im_i} \rangle | \alpha_{ij} \in \mathbb{Z}, j \leq m_i, \ \& \ \exists \overline{B} \in \overline{G}_i (\overline{B}^{\alpha_{i0}} = \overline{A}_{i1}^{\alpha_{i1}} \cdot \ldots \cdot \overline{A}_{im_i}^{\alpha_{im_i}})\}.$$

Using this notation, we introduce the following

Definition 1. We say that a subgroup G is *pure* in $UT_n(K)$ with respect to the central series (5), if for every $i < n$ and sequence $\langle \alpha_{i0}, \alpha_{i1}, \cdots, \alpha_{im_i} \rangle \in S_i(G)$, and for every element $c \in G_i$ the following is true: From solvability of the equation $x^{\alpha_{i0}} = A_{i1}^{\alpha_{i1}} \cdot \ldots \cdot A_{im_i}^{\alpha_{im_i}} \cdot c$ in the group $UT_n(K)$, it follows solvability of this equation in G.

Let γ be a computable numbering of the ring K, and let γ_* be a numbering of $UT_n(K)$, defined through γ, so that from any number $n \in \omega$ we can effectively find γ-numbers of the elements of the matrix $\gamma_* n$. Then we have

Theorem 3. Let G be a subgroup $G \leq UT_n(K)$, and let (5) be a central series of it, such that the following are true:

a) all factors of the series (5) are computable;

b) G is pure in $UT_n(K)$ with respect to the series (5).

Then G is a computably enumerable subgroup in $(UT_n(K), \gamma_*)$.

Proof. By induction on i, we prove that the subgroup G_i is computably enumerable in $(UT_n(K), \gamma_*)$. The claim is obvious for $i = 0$.

Assume that G_i is a computably enumerable subgroup in $(UT_n(K), \gamma_*)$. Since the dimension of the quotient G_{i+1}/G_i is finite, then there is a finite sequence of matrices

$$A_{i1}, A_{i2}, \ldots, A_{im_i},$$

such that the cosets

$$\overline{A}_{i1}, \overline{A}_{i2}, \ldots, \overline{A}_{im_i} \quad (6)$$

form a linearly independent system in the quotient $\overline{G}_i = G_{i+1}/G_i$, $i < n$. Since $\overline{G}_i$ is computable, then the set of all sequences of integers

$$S_i = \{\langle \alpha_{i0}, \alpha_{i1}, \cdots, \alpha_{im_i} \rangle | \exists \overline{B} \in \overline{G}_i (\overline{B}^{\alpha_{i0}} = \overline{A}_{i1}^{\alpha_{i1}} \cdot \ldots \cdot \overline{A}_{im_i}^{\alpha_{im_i}}), \alpha_{ij} \in \mathbb{Z}, j \leq m_i\}$$

is computably enumerable. We prove that the following equivalence is true:

$$s \in \gamma_*^{-1} G_{i+1} \Leftrightarrow (UT_n(K), \gamma_*) \models \exists \langle \alpha_{i0}, \ldots, \alpha_{im_i} \rangle \exists r \in \gamma_*^{-1} G_i;$$

$$(\langle \alpha_{i0}, \alpha_{i1}, \cdots, \alpha_{im_i} \rangle \in S_i \ \& \ (\gamma_* s)^{\alpha_{i0}} = A_{i1}^{\alpha_{i1}} \cdot \ldots \cdot A_{im_i}^{\alpha_{im_i}} \cdot \gamma_* r). \tag{7}$$

($\Rightarrow$.) Let $s \in \gamma_*^{-1} G_{i+1}$ and $B = \gamma_* s$. Since (6) is a maximal linearly independent system of elements of the quotient $\overline{G}_i$, then there are a sequence of integers $\langle \alpha_{i0}, \alpha_{i1}, \cdots, \alpha_{im_i} \rangle$ and a matrix $C \in G_i$ such that

$$B^{\alpha_{i0}} = A_{i1}^{\alpha_{i1}} \cdot \ldots \cdot A_{im_i}^{\alpha_{im_i}} \cdot C. \tag{8}$$

Hence, it follows that the right-hand side of (7) is true.

($\Leftarrow$.) Assume, now, the right-hand side of (7), and suppose that $B = \gamma_* s$, $\gamma_* r = C \in G_i$. Then we have (8). Hence, by purity of the subgroup G in $UT_n(K)$ with respect to (5), and uniqueness of roots in $UT_n(K)$, we have that $B \in G$, and therefore $B \in G_{i+1}$, as desired.

We show that by the equation (8) the elements of the matrix B can be effectively identified. Indeed, from a number r, we can effectively determine γ-numbers of the elements of the matrix $\gamma_* r = C$. Since the number of matrices A_{ij} is finite, we can assume that γ-numbers of the elements of these matrices are known. From this, we find effectively γ-numbers of the elements of the matrix in the right-hand side of (8). By uniqueness of roots in $UT_n(K)$, we can find γ-numbers of the elements of the matrix B such that (8) holds, and therefore we can find also a γ_*-number of the matrix B.

From this and (7), by the induction hypothesis we get that G_{i+1} is a computably enumerable subgroup in the group $(UT_n(K), \gamma_*)$. The induction step, and thus the sufficiency of the theorem, has been proved.

Corollary 6. Suppose that $G \leq UT_n(K)$ is pure in $UT_n(K)$ with respect to the central series (5). Then the group G is computable if and only if the factors of the series (5) are computable.

Corollary 7. If G is pure in $UT_n(K)$, then it is pure with respect to any central series of it.

From this and Corollary 6, it follows.

Corollary 8. Let $G \leq UT_n(K)$ be pure in $UT_n(K)$. Then the group G is computable if and only if all factors of some central series of it are computable.

References

1 Романьков В.А. О конструктивных матричных и упорядоченных группах / В.А. Романьков, Н.Г. Хисамиев // Алгебра и логика. — 2004. — Т. 43. — № 3. — С. 198–204.

2 Романьков В.А. О конструктивизируемых матричных группах / В.А. Романьков, Н.Г. Хисамиев // Алгебра и логика. — 2004. — Т. 43. — № 5. — С. 339–345.

3 Мальцев А.И. О рекурсивных абелевых группах / А.И. Мальцев // Доклады АН СССР. — 1962. — Т. 46. — № 5. — С. 1009–1012.

4 Нуризинов М.К. Вычислимые нильпотентные группы без кручения конечных размерностей / М.К. Нуризинов, Р.К. Тюлюбергенев, Н.Г. Хисамиев // Сиб. мат. журн. — 2014. — Т. 55. — № 3. — С. 580–591.

5 Гончаров С.С. Конструктивные модели / С.С. Гончаров, Ю.Л. Ершов. — Новосибирск: Науч. кн., 1999.

6 Каргаполов М.И. Основы теории групп / М.И. Каргаполов, Ю.И. Мерзляков. — Т. 1. — М.: Наука, 1996.

7 Б.Л. ван дер Варден. Алгебра / Б.Л. ван дер Варден. — Т. 1. Спрингер. — Нью-Йорк: Спрингер-Верлаг, 1991.

Р.К. Тюлюбергенев

Сақинадағы барлық униүшбұрышты матрицалар тобының есептелінетін іштоптары туралы

Мақалада негізгі мәселелер ретінде қандай да бір топтар кластары үшін конструктивизацияның бар болуы, жалғыздығы және жалғасы қарастырылды. Алгоритмдер теориясының дамуына байланысты алгебралық жүйелердің маңызды кластарының есептелімділік мәселелерін шешуді зерттеу өзекті мәселелердің біріне айналды. Сақинадағы униүшбұрышты матрицалар тобы нильпотентті топтар кластарының классикалық өкілі болып табылады және көптеген қолданылымдары тек қана топтар теориясында ғана емес, оның қосымшалары үшін де маңызды орын алған. Автор есептелінетін ассоциативті сақинадағы бірлікпен $UT_n(K)$ барлық униүшбұрышты матрицалар тобындағы есептелімді іштоптардың болу критерийін алған.

Кілт сөздер: нөмірлеу, униүшбұрышты матрицалар тобы, конструктивті топ, нильпотентті топ, алгоритм теориясы.

Р.К. Тюлюбергенев

О вычислимых подгруппах группы всех унитреугольных матриц над кольцом

Основными проблемами статьи являются проблемы существования, единственности и продолжения конструктивизации для тех или иных классов групп. В связи с развитием теории алгоритмов актуальным является исследование проблем вычислимости важных классов алгебраических систем. Группы унитреугольных матриц над кольцом составляют важный класс нильпотентных групп, имеющий многочисленные применения как в самой теории групп, так и в её приложениях. Автором получен критерий вычислимости подгруппы группы всех унитреугольных матриц $UT_n(K)$ над вычислимым ассоциативным кольцом с единицей.

Ключевые слова: нумерация, группа унитреугольных матриц, конструктивная группа, нильпотентная подгруппа, подгруппа, рациональное число, теория алгоритмов.

References

1 Roman'kov, V.A., Khisamiev, N.G. (2004). O konstruktivnykh matrichnykh i uporiadochennykh hruppakh [Constructive matrix and orderable groups]. *Alhebra i lohika – Algebra and Logic, Vol. 43, 3,* 198–204 [in Russian].

2 Roman'kov, V.A., Khisamiev, N.G. (2004). O konstruktiviziruemykh matrichnykh hruppakh [Constructible matrix groups]. *Alhebra i lohika – Algebra and Logic, Vol. 43, 5,* 339–345 [in Russian].

3 Malcev, A.I. (1962). O rekursivnykh abelevykh hruppakh [On recursive abelian groups]. *Doklady AN SSSR – Reports AS SSSR, Vol. 46, 5,* 1009–1012 [in Russian].

4 Nurizinov, M.K., Tyulyubergenev, R.K., Khisamiev, N.G. (2014). Vychislimye nilpotentnye hruppy bez krucheniia konechnykh razmernostei [Computable torsion-free nilpotent groups of finite dimension]. *Sibirskii Matematicheskii Zhurnal – Siberian Mathematical Journal, Vol. 55, 3,* 580–591 [in Russian].

5 Goncharov, S.S., Ershov, Yu.L. (1999). *Konstruktivnye modeli [Constructive Models].* Novosibirsk: Nauchnaya Kniha [in Russian].

6 Kargapolov, M.I., Merzljakov, Yu.I. (1996). *Osnovy teorii hrupp [Fundamentals of the Theory of Groups].* (Vol. 1). Moscow: Nauka [in Russian].

7 B.L. van der Waerden (1991). *Alhebra [Algebra],* Vol. 1. Springer. New York: Springer-Verlad [in Russian].