Computable Rings, Groups and Their Isomorphisms

B. Khoussainov, A. Slinko

Abstract: We investigate computable isomorphism types of groups. Our main result states that for any $n \in \omega \cup \{\omega\}$ there exists a computably categorical nilpotent of class 2 group G which being expanded by a finite number of constants has exactly n computable isomorphism types. This result is based on the similar result for computable nonassociative rings.

1. Introduction, Basic Notions and Main Results.

From algebraic point of view there is no distinction between isomorphic algebraic systems. Therefore classification of algebraic systems up to isomorphism constitutes one of the main goals of structure theories of these systems. It can be said that structure theories of algebraic systems study isomorphism types of these systems, i.e., classes of isomorphic algebraic systems. The theory of rings is by no means an exception among them. However in effective theories of the same algebraic systems this view on isomorphism types has to undergo profound changes since isomorphism types and computable isomorphism types become different.

Computable algebraic systems such as computable groups, boolean algebras, vector spaces, lattices, have been intensively investigated in recent years [1], [2]. Intensive research efforts have been made in attempts to understand the effective content of a variety of model-theoretic and algebraic notions, results and constructions. We refer the reader to the recent surveys by Harizanov [3], Millar [4] as well as to the classic papers by Frölich and Shepherdson [5], Malcev [6] and Rabin [7] devoted to these issues. In this paper we consider computable rings and investigate relationship between isomorphism types and computable isomorphism types of these algebraic systems.

Let us recall several basic notions from the computability theory [8]. Throughout the paper ω is the set of all natural numbers. A set $X \subset \omega$ is *computable* if there is a procedure which being applied to any number n tells us if $n \in X$. A function $f\colon \omega \to \omega$ is *computable* if the set of pairs $X = \{(n, f(n)) \mid n \in \omega\} \subseteq \omega \times \omega$ is computable under the standard Cantor's identification of $\omega \times \omega$ and ω. A set $X \subset \omega$ is *computably enumerable* if it is the range of a computable function $f\colon \omega \to \omega$.

In this paper by a ring $\mathcal{R} = (R, +, \times, 0)$ we understand a nonassociative ring, i.e. a ring for which the associative law for the multilication is not assumed. While nonassociative rings are less commonly metthan their associative counterpart, they do have a number of significant applications. For instance, apart from Lie rings which are widely used, nonassociative rings have been also studied in relations to projective geometry [9] and their applications to physics [10] and genetics [11].

Definition 1.1 A ring $\mathcal{R} = (R, +, \times, 0)$ is *computable* if the set R is a computable subset of ω and the ring operations $+$ and $\times$ are computable functions from R^2 into R.

Informally, a computable ring is a ring whose elements can be enumerated and whose operations can be computed by Turing machines.

Definition 1.2 A ring $\mathcal{R}$ is said to be *computably presentable* if its isomorphism type contains a computable ring. If $\mathcal{R}'$ is a computable ring isomorphic to $\mathcal{R}$, then $\mathcal{R}'$ is called a *computable presentation* of $\mathcal{R}$.

For example, the field of rational numbers $\mathbb{Q}$ and the ring of integers $\mathbb{Z}$ are computably presentable rings, where the standard presentations are computable presentations.

Definition 1.3 An isomorphism $f\colon \mathcal{R}_1 \to \mathcal{R}_2$ from a computable ring $\mathcal{R}_1$ onto a computable ring $\mathcal{R}_2$ is said to be *computable* if f itself is a computable function. In this case we say that $\mathcal{R}_1$ is computably isomorphic to $\mathcal{R}_2$.

Definition 1.4 The notion of computable isomorphism defines an equivalence relation on the class of all computable presentations of a given computably presentable ring $\mathcal{R}$. The classes of the partition corresponding to this equivalence relation are called *computable isomorphism types* of $\mathcal{R}$. The number of computable isomorphism types of $\mathcal{R}$ is called the *algorithmic dimension* of $\mathcal{R}$.

Thus, informally one can say that the number of computable isomorphism types of a ring is the number of its effective presentations which cannot be effectively transformed one into another. Rings of algorithmic dimension 1 are the rings with exactly one computable isomorphism type. Algebraic structures with exactly one computable isomorphism type are also called *computably categorical*. Computably categorical structures have been the subject of extensive investigations: [1], [3], [4], [12], [13], [14], [15]. The following simple proposition gives examples of rings of algorithmic dimension 1 or, equivalently, computably categorical rings.

Proposition 1.1 Any two computable presentations of a finitely generated ring $\mathcal{R}$ are computably isomorphic.

Sketch of the Proof. Let $\mathcal{R}_1$ and $\mathcal{R}_2$ be two computable presentations of $\mathcal{R}$. Let $b_1, \ldots, b_n$ be generators of $\mathcal{R}$, with $m_1, \ldots, m_n$ and $k_1, \ldots, k_n$ being the respective images of these generators in the computable presentations $\mathcal{R}_1$ and $\mathcal{R}_2$ under respective isomorphisms. Then the partial mapping $m_i \mapsto k_i$ can be extended to a computable isomorphism from $\mathcal{R}_1$ to $\mathcal{R}_2$ in the obvious way.

Goncharov [13], [14] and independently LaRoche and Remmel [15] studied computably categorical boolean algebras and linearly ordered sets. They proved the following two theorems.

Theorem 1.1 A boolean algebra is computably categorical if and only if the number of its atoms is finite. Moreover, every boolean algebra, which is not computably categorical, has infinitely many computable isomorphism types.

Theorem 1.2 A linear ordering is computably categorical if and only if the number of its successive pairs, that is pairs (a, b) for which $a < b$ and the interval $[a, b]$ consists of a and b only, is finite. Moreover, every linear ordering, which is not computably categorical, has infinitely many computable isomorphism types.

Thus, the algorithmic dimension of any Boolean algebra or linear ordering is either ω or 1. For abelian groups, as Goncharov [13], [14] showed in the theorem that follows, the same result holds, but for groups in general the situation is more complicated.

Theorem 1.3 The algorithmic dimension of any abelian group is either 1 or ω. For any natural number n there exists a (noncommutative) group of algorithmic dimension n.

The latter result Goncharov proved by encoding his family into a metabelian group [16]. The same approach was applied in [17]. In this paper we use the same approach to show that a similar result holds also for rings. Namely, we prove:

Theorem A For every $n \in \omega \bigcup \{\omega\}$ there exists a (noncommutative and nonassociative) ring of algorithmic dimension n.

There are basically two reasons why the notion of a computably categorical structure has attracted a significant attention of researchers in computable algebra and model theory. The first reason is that computably categorical structures are exactly those structures which do not depend on a particular computable presentation. Thus, from the computable-model-theoretic point of view there is no distinction between two computable presentations of a computably categorical structure.

The second reason comes from model theory. The basic model-theoretic notion, which motivated the study of computably categorical structures, is the notion of countably categorical model. In classical model theory a theory T is called *(countably) categorical* if all (countable) models of T are isomorphic. A (countable) structure $\mathcal{A}$ is *(countably) categorical* if its theory $Th(\mathcal{A})$ is (countably) categorical. The analogous concept for the effective model theory deals only with computable structures and isomorphisms. It is the notion of a computably categorical structure.

Any algebraic structure $\mathcal{A}$ can be expanded by a finite number of constants $a_1, \ldots, a_n \in \mathcal{A}$. The expanded structure will be denoted $(\mathcal{A}, a_1, \ldots, a_n)$ or simply $\mathcal{A}$ when ambiguity cannot happen. Algebraically, it means that we consider n unary operations $u_i(x) = a_i$, $i = 1, 2, \ldots, n$, on $\mathcal{A}$ together and on equal rights with the existing operations in $\mathcal{A}$. From the computational point of view we also fix some algorithms which output these constants. From categorical point of view this is the change of the category as morphisms now have to respect new operations. For example, we call a mapping $f \colon \mathcal{A}_1 \to \mathcal{A}_2$

from an expanded structure $\mathcal{A}_1 = (\mathcal{A}_1, a_1, \ldots, a_n)$ onto an expanded structure $\mathcal{A}_2 = (\mathcal{A}_1, b_1, \ldots, b_n)$ an *isomorphism* if it is an isomorphism of non-expanded structures and also $f(a_i) = b_i$ for $i = 1, 2, \ldots, n$.

The notion of expansion by constants has strong connections with classical categoricity of a structure. For instance, it is an easy consequence of the classical Ryll-Nardzewski Theorem that, if the theory of an arbitrary structure $\mathcal{A}$ is countably categorical, then so is the theory of any expansion of $\mathcal{A}$ by finitely many constants. In effective model theory computably categorical structures are analogues of countably categorical ones. Millar [18] proved that a certain amount of decidability is enough to guarantee that the property of being computably categorical is preserved under expansions by finitely many constants. Without this assumption of partial decidability the problem, which was known as Ash-Goncharov problem [19], remained open for some time. It was solved negatively in [20].

Theorem 1.4 For every natural number n there exists a computably categorical graph G such that for any $c \in G$, the expanded graph (G, c) has exactly n computable isomorphism types.

It is the analogous problem for computable rings and computable groups that we wish to address in this paper. The second and the third theorems of this paper shows that the same phenomenon can also occur not only for graphs but also in the class of rings and even in the class of nilpotent groups of class 2.

Theorem B For every natural number n there exists a computably categorical (noncommutative and nonassociative) ring $\mathcal{R}$ such that for some $c \in \mathcal{R}$ the expanded ring $(\mathcal{R}, c)$ has exactly n types of computable isomorphisms.

Theorem. C For every prime $p > 2$ and for every $n \in \omega \bigcup \{\omega\}$ there exists a computably categorical nilpotent group $\mathcal{G}$ of class 2 satisfying $x^p = 1$ such that for some constants $a_1, a_2, a_3 \in \mathcal{G}$ the expanded group $(\mathcal{G}, a_1, a_2, a_3)$ is of algorithmic dimension n.

2. Computable Families and Enumerations.

The ring which we need to present to establish Theorem A will be constructed by encoding a certain (uniformly) computably enumerable family of sets of natural numbers into a ring.

Definition 2.1 A family of nonempty sets S is called *computably enumerable* if there exists a mapping $f\colon \omega \to F$ such that the set of pairs $\{(i,x) \mid x \in f(i)\}$ is computably enumerable. We then call f a *(computable) enumeration* of S. If f is one-to-one we say that it is a *one-to-one* enumeration of S.

Technically, it is more convenient to view a computable enumeration of S as a procedure which produces a 2-dimensional array $\{f^i(n) \mid i, n \in \omega\}$ of finite subsets of ω according to the following rules:

(i) At stage 0 it produces empty or one element subset $f^0(0)$;

(ii) At stage k it produces subsets $f^k(0), \ldots, f^1(k-1), f^0(k)$ such that $f^{k-1}(i) \subseteq f^k(i)$, $i = 1, \ldots, k-1$, and such that

$$\mathrm{card}(f^{k-1}(0) \cup \ldots \cup f^0(k-1)) \leq \mathrm{card}(f^k(0) \cup \ldots \cup f^0(k)) + 1;$$

(iii) $\bigcup\limits_{i \geq 0} f^i(n) = f(n)$.

We define a preordering on the set of all computable enumerations of a family S that will naturally induce an equivalence relation on this set. The equivalence classes of this relation will correspond to computable isomorphism types of the ring that we will construct.

Definition 2.2 Let f and g be two computable enumerations of a family S. We say that f is *reducible* to g and denote it as $f \leq g$, if there is a computable function $\Phi\colon \omega \to \omega$ such that $f = g\Phi$. If $f \leq g$ and $g \leq f$ then we say that f and g are *equivalent* and denote this relation by $f \sim g$.

The equivalence classes of one-to-one enumerations are the minimal elements in the induced partial ordering. One-to-one enumerations will be needed to define a family of sets that will be encoded. Theorem A will be based on the following theorem of Goncharov [12].

Theorem 2.1 For any $n \in \omega$ there exists a family S of computably enumerable sets such that S has up to equivalence exactly n one-to-one computable enumerations.

We now present the basic notions involved in the proof of Theorem B. We need to consider families of k-tuples of sets. We give all definitions for the case $k = 2$. We will indicate later how the case $k > 2$ can be handled.

In what follows we use r and l as the right and left projections from pairs, that is, $l(A,B) = A$ and $r(A,B) = B$.

Definition 2.3 Let S be a family of pairs (A,B) of nonempty sets. A family S is called *symmetric* if $(A,B) \in S$ implies that $(B,A) \in S$. A family S is said to be *computably enumerable* if there exists a mapping $f\colon \omega \to S$ such that the set of triples $\{(i,x,y) \mid x \in lf(i),\ y \in rf(i)\}$ is computably enumerable. We then call f a *(computable) enumeration* of S. If f is one-to-one, we say it is a *one-to-one* enumeration of S.

The notion of reducibility and equivalence between enumerations of a symmetric family S are exactly the same as for families of computably enumerable sets. If f is a one-to-one computable enumeration of a symmetric family S of pairs of sets then there is another computable enumeration $\tilde{f}$ of S which is a natural companion of f, namely, if $f(i) = (A_i, B_i)$, then $\tilde{f}(i) = (B_i, A_i)$.

The notion of algorithmic dimension can be also applied to a family S of pairs of sets as follows:

Definition 2.4 If f is a one-to-one computable enumeration of a symmetric family S of pairs of sets, we say that S has algorithmic dimension 2 if f and $\tilde{f}$ are not equivalent but every computable one-to-one enumeration of S is equivalent to either f or $\tilde{f}$.

Such a family was constructed in [20]:

Theorem 2.2 There exists a computably enumerable symmetric family of algorithmic dimension 2.

This family will be encoded into a ring in order to prove Theorem B.

3. Rings of a Finite Algorithmic Dimension.

(a) Encoding a set into a field. We first show how to encode a set of natural numbers into a ring, in fact, into a field. Our reference book in relation to field theory will be [21]. Let $F = \mathbb{Z}_p$ be a finite field of residues modulo p. In the construction that follows p may be an arbitrary prime number. To motivate the construction we consider the class of all algebraic extentions of F which lie in some fixed copy $\overline{F}$ of algebraic closure of F (pp.166–173). If $F \subseteq K$ is such an extention, then

$$[F : K] = \dim_F K$$

is called the *degree* of the extention K. The extention K is called *finite* if its degree is finite. For a tower of finite extentions

$$F \subseteq K \subseteq L$$

the degrees are multiplicative, i.e. $[F : L] = [F : K][K : L]$ (p. 162).

For any $\alpha_1, \ldots, \alpha_n, \ldots \in \overline{F}$ by $F[\alpha_1, \ldots, \alpha_n, \ldots]$ we denote the minimal subfield of $\overline{F}$ containing F and $\alpha_1, \ldots, \alpha_n, \ldots$. Extentions of the form $F[\alpha]$ are called *simple*. If a simple extention $F[\alpha]$ is finite, the element α is said to be *algebraic* over F. For such an element α there exist polynomials $f(x) \in F[x]$ which annihilate it, that is $f(\alpha) = 0$. All annihilating polynomials form an ideal I_α in the polynomial ring $F[x]$. This ideal is generated by a polynomial called *the minimal irreducible polynomial* of α, denoted $\mathrm{Irr}_\alpha(x)$. The degree of the extention $F \subseteq F[\alpha]$ is equal to the degree of the minimal irreducible polynomial $\mathrm{Irr}_\alpha(x)$. We will refer to this degree as to the *order* of α. The multiplicity of degrees implies that for every element $\alpha \in K$ of a finite extention K of F the order of α is a divisor of $[F : K]$.

Constructively, for an element α of order n, $F[\alpha]$ can be viewed as the quotient-algebra $F[x]/I_\alpha$, where the coset $x + I_\alpha$ corresponds to α, that is the set of polynomials $\{g(x) \mid \deg g(x) \leq n\}$ with their usual addition and usual multiplication truncated modulo $\mathrm{Irr}_\alpha(x)$. The field $F[\alpha_1, \ldots, \alpha_n]$ can now be inductively defined as

$$F[\alpha_1, \ldots, \alpha_n] = F[\alpha_1, \ldots, \alpha_{n-1}][\alpha_n]$$

and also

$$F[\alpha_1, \ldots, \alpha_n, \ldots] = \bigcup_{n=1}^{\infty} F[\alpha_1, \ldots, \alpha_n].$$

It is essential for our purposes that F has simple finite extentions of all possible degrees (Theorem 10, p.184).

Let $M = \{m_0, m_1, \ldots, m_n, \ldots\}$ be a subset of ω. If M is empty, then we assume that the field F encodes it. If M is not empty, we will put in correspondence to M the algebraic extention of F

$$F_M = F[\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots],$$

where α_i is an algebraic element of order p_{m_i}, the m_ith prime. We fix these elements and always use them for our coding purposes or alternatively, from the constructive point of view, we may think that we have fixed their minimal irreducible polynomials $P_i(x) = \mathrm{Irr}_{\alpha_i}(x)$.

Lemma 3.1 The set of prime factors of orders of elements of F_M is exactly the set $\{p_{m_0}, \ldots, p_{m_i}, \ldots\}$. The set S_i of all elements of order p_{m_i} in F_M consists of $p^{p_{m_i}}$ elements and $S_i = F[\alpha]$ for every element α of order p_{m_i}.

Proof: Let $a \in F_M$. Then, for some n, the element a belongs to a finite extention

$$G_n = F[\alpha_0, \alpha_1, \ldots, \alpha_n], \tag{1}$$

Since degrees in towers are multiplicative, observing the tower

$$F \subseteq F[\alpha_i] \subseteq G_n$$

we see that the degree of G_n is divisible by p_{m_i} and therefore is divisible by $p_{m_0} p_{m_1} \ldots p_{m_n}$. As the degree of α_i over $F[\alpha_0, \alpha_1, \ldots, \alpha_{i-1}]$ is less than or equal to p_{m_i} the degree of G_n cannot be greater than this product.

Now by considering the tower

$$F \subseteq F[a] \subseteq G_n$$

we see that the order of a must be a divisor of this product.

Let $q = p_{m_i}$ and α be an element of order q. Then the subfield $F[\alpha]$ has p^q elements. It is isomorphic to the Galois field $\mathrm{GF}(p^q)$ of this order which, being a subfield of $\overline{F}$ is known to coincide with the set of all roots of the polynomial $x^{p^q} - x$ in $\overline{F}$. Therefore such subfield is unique and $F[\alpha] = F[\beta]$ for any two elements of order q.

Lemma 3.2 The set M is computably enumerable if and only if the field F_M is computably presentable.

Proof: Let $m_0, m_1, \ldots, m_n, \ldots$ be an effective enumeration of M. Define the field G_n as in (1). We saw in the proof of the previous lemma that the dimension of the field G_n over F is $p_{m_0} p_{m_1} \ldots p_{m_n}$.

As a vector space G_n has a spanning set consisting of monomials

$$\alpha_0^{k_0} \alpha_1^{k_1} \ldots \alpha_n^{k_n}, \tag{2}$$

where $0 \le k_i < p_{m_i}$. This spanning set has cardinality $p_{m_0} p_{m_1} \ldots p_{m_n}$. Therefore this spanning set is a basis. These monomials can be multiplied as usual monomials in α_i but with powers of α_i being multiplied modulo the minimal irreducible polynomial of α_i. Since the union of all such bases is a basis for F_M, this certainly gives a computable presentation of F_M.

Let now $\mathcal{A}$ be a computable presentation of F_M and $a_1, a_2, \ldots, a_n, \ldots$ be the enumeration of elements of $\mathcal{A}$ which arises from this presentation. Take $a = a_1 \in \mathcal{A}$ and consider powers $a, a^2, \ldots$ until $a^s = a^n$ for $s < n$. Then $a^{n-s} = e$ is the unit element of $\mathcal{A}$. Thus $F_1 = \{0, e, 2e, \ldots, (p-1)e\}$ will be the only subfield of $\mathcal{A}$ isomorphic to F.

Since F is finite we can now constructively determine the minimal irreducible polynomial of a_1 as its degree is less than or equal to $n-s$. We know that $m \in M$ iff there exists an element $x \in \mathcal{A}$ such that the order of x over F_1 is p_m. The prime divisors of the degree of this polynomial, say $p_{m_1}, \ldots, p_{m_k}$, will show that there are elements of such orders and give us the first set of elements of M to list, namely $m_1, \ldots, m_k$. Hence M is a computably enumerable set. The lemma is proved.

Lemma 3.3 The field F_M is computably categorical.

Proof: Let $\mathcal{A}$ and $\mathcal{B}$ be two computable presentations of F_M. Consider the subfields F_1 and F_2, of $\mathcal{A}$ and $\mathcal{B}$, respectively, isomorphic to F and constructed as in the proof of the previous lemma. The only isomorphism between them can be established by assigning one unit element to another and multiples of one unit to the corresponding multiples of another. Denote $\mathcal{A}_0 = F_1$, $\mathcal{B}_0 = F_2$ and let $\sigma_0 \colon \mathcal{A}_0 \to \mathcal{B}_0$ be the established isomorphism. Suppose that we established already an isomorphism $\sigma_i \colon \mathcal{A}_i \to \mathcal{B}_i$ between subfields $\mathcal{A}_i$ and $\mathcal{B}_i$ such that for an arbitrary prime number q either all elements of $\mathcal{A}$ and $\mathcal{B}$ of prime order q belong to $\mathcal{A}_i$ and $\mathcal{B}_i$, respectively, or none of them. This isomorphism can be readily extended to the isomorphism $f(x) \mapsto f^{\sigma_i}(x)$ of polynomial rings $\mathcal{A}_i[x]$ and $\mathcal{B}_i[x]$, which is defined as follows: if $f(x) = a_0 + a_1 x + \ldots + a_m x^m$, then $f^{\sigma_i}(x) = a_0^{\sigma_i} + a_1^{\sigma_i} x + \ldots + a_m^{\sigma_i} x^m$. Now we look for the first element α in the effective enumeration of $\mathcal{A}$ which is of prime order q over $\mathcal{A}_0 = F_1$ and which is not in $\mathcal{A}_i$. Then we find $\beta \in \mathcal{B}$ with exactly the same minimal irreducible polynomial over $\mathcal{B}_0 = F_2$ and construct an isomorphism $\sigma_{i+1} \colon \mathcal{A}_i[\alpha] \to \mathcal{B}_i[\beta]$ defining the mapping σ_{i+1} for every polynomial $f(x) \in \mathcal{A}_i[x]$ of degree less than q by the following formula

$$\sigma_{i+1}(f(\alpha)) = f^{\sigma_i}(\beta).$$

It is easy to check that σ_{i+1} is again an isomorphism (see p.171). We denote then $\mathcal{A}_{i+1} = \mathcal{A}_i[\alpha]$ and $\mathcal{B}_{i+1} = \mathcal{B}_i[\beta]$. Since all elements of order q lie in $F[\alpha]$, and hence in $\mathcal{A}_{i+1}$ and $\mathcal{B}_{i+1}$, the construction can be effectively continued further. The lemma is proved.

(b) Encoding a family of sets into an algebra. Let S be a countable family of countable sets. We will list them in some order which will not be important later:

$$S = \{M_0, M_1, \dots, M_i, \dots\}.$$

Consider the free product in the variety of all (nonassociative) rings

$$A(S) = F_{M_0} \star F_{M_1} \star \dots \star F_{M_n} \star \dots$$

of fields F_{M_i} such that each field encodes the set M_i in the way it was described in the previous section. Up to isomorphism this algebra does not depend on the order in which we listed the sets of our family. In this section we will use the family of sets S, constructed in [12], which up to equivalence has exactly n one-to-one computable enumerations $f_1, \dots, f_n$, to construct n computable presentations $A_{f_1}(S), \dots, A_{f_n}(S)$ of $A(S)$, such that no two of them are computably isomorphic but any other computable presentation of $A(S)$ is computably isomorphic to one of the computable algebras $A_{f_1}(S), \dots, A_{f_n}(S)$.

We will refer to the fields F_{M_i} as to components of $A(S)$. This algebra, as it is the free product of the components, has a basis consisting of nonassociative products

$$(a_1 a_2 \dots a_n)_q, \qquad n \geq 1, \tag{3}$$

where elements $a_1, \dots, a_n$ are basic monomials (2) and any two neighbouring monomials a_{i-1} and a_i situated in the bracket $(a_{i-1}a_i)$ belong to different components. For example, in the product $(a_1(a_2((a_3a_4)(a_5a_6))))$ in each pair a_3, a_4 and a_5, a_6 the monomials must be from different components, while a_1, a_2 may be arbitrary.

We will refer to the products (3) as to the *basic products*. The multiplication table on the basis is as follows: if $(a_1a_2 \dots a_n)_p$ and $(b_1b_2 \dots b_m)_q$ are two basic products and $\max(m, n) > 1$ or $m = n = 1$ and a_1, b_1 belong to different components, then

$$(a_1a_2 \dots a_n)_p \cdot (b_1b_2 \dots b_m)_q = ((a_1a_2 \dots a_n)_p(b_1b_2 \dots b_m)_q), \tag{4}$$

If $m = n = 1$ and a_1, b_1 belong to the same component, then $a_1 b_1 = \sum_{i=1}^{\ell} \beta_i c_i$, where c_i's are basis monomials of the component to which both of them belong, and

$$(a_1) \cdot (b_1) = \sum_{i=1}^{\ell} \beta_i (c_i). \tag{5}$$

Let $u = (a_1 a_2 \dots a_n)_q$ be a basic product. We set $|u| = n$, and for an element $a = \sum_{i=1}^{\ell} \beta_i u_i$ of $A(S)$ we set $|a| = \max_i |u_i|$. It is clear from the multiplication table (4) and (5) that

$$|a \cdot b| = |a| + |b|, \tag{6}$$

unless $|a| = |b| = 1$ and a, b are from the same component. Unfortunately when the free product is taken in the class of associative rings the equation (6) is no longer valid and that is why we have to consider nonassociative products.

Let us recall that an element e of a ring $\mathcal{R}$ is called an *idempotent* if $e^2 = e$.

Lemma 3.4 The fields F_{M_i} are isomorphically imbedded in $A(S)$. The unit elements $e_0, e_1, \dots, e_n, \dots$ of the fields F_{M_i} are the only idempotents of $A(S)$. An element $a \in A(S)$ belongs to F_{M_i} iff $e_i a = a e_i = a$.

Proof: As it can be seen from the multiplication table, the field F_{M_i} is a subring of $A(S)$ and the unit element e_i of it is an idempotent. Suppose that $e^2 = e$ and $e \neq 0$. Then (6) implies that $|e| = 1$. It is also clear that if e is equal to the sum of basic monomials from different components, then $|e^2| = 2$ and $e^2 \neq e$. Therefore e belongs to one of the components. But it is a field and has a unique idempotent, namely the unit element of this field.

The field F_{M_i} is a subring of $A(S)$ and $e_i a = a e_i = a$ for all $a \in F_{M_i}$. Suppose that $e_i a = a e_i = a$. Then the multiplication table of $A(S)$ implies that a is a linear combination of basic monomials from F_{M_i} and thus is an element of F_{M_i}. The lemma is proved.

Note: The statement that e_i are the only idempotents of this free product is no longer valid if this product is associative. For example, $e = e_2 e_1 e_2 - e_2 e_1 + e_2$ will be also an idempotent.

Now, given a one-to-one computable enumeration f let us construct a computable presentation $A_f(S)$ of $A(S)$. Let us now denote $M_i = f(i)$. Since

f is computable, there exists a procedure which produces a 2-dimensional array $\{M_{in} = f^i(n) \mid i, n \in \omega\}$ of finite subsets of ω according to the following rules:

(M1) At stage 0 it produces an empty or one element subset M_{00};

(M2) At stage k it produces finite subsets $M_{k0}, \dots, M_{1k-1}, M_{0k}$ so that $M_{k-1i} \subseteq M_{ki}$, for $i = 1, \dots, k-1$, and such that

$$\mathrm{card}(M_{k-10} \cup \ldots \cup M_{0k-1}) \leq \mathrm{card}(M_{k0} \cup \ldots \cup M_{0k}) + 1;$$

(M3) $\bigcup_{i \geq 0} M_{in} = M_n$.

Thus using f we can construct an effective sequence of computable partial algebras

$$A(f, 0),\ A(f, 1),\ \dots\ ,\ A(f, n),\ \dots$$

such that:

(A1) $A(f, i)$ is a subalgebra of $A(f, i+1)$;

(A2) $A(f, i)$ is isomorphic to $(F_{M_{i0}} \star \ldots \star F_{M_{0i}})^{(i)}$, the latter being the subspace of $A(S)$ spanned by the basic products of degree $\leq i$ depending only on elements from $F_{M_{0i}}, \dots, F_{M_{i0}}$ with the addition and multiplication inherited from $A(S)$;

(A3) $A_f(S) = \bigcup_{k=0}^{\infty} A(f, i)$ is isomorphic to $A(S)$.

As the sets M_{ki} are finite the fields $F_{M_{ki}}$ are finite-dimensional, hence finite, and partial algebras $A(f, i)$ are also finite-dimensional, and hence also finite. It is important to note that at stage i, when we extend $A(f, i-1)$ to $A(f, i)$ the only one idempotent will be added, namely the unit element e_i of the field F_{M_i}. In order to separate stages we start each time enumeration of additional elements with e_i.

Lemma 3.5 The ring $A_f(S)$ is computable for every computable one-to-one enumeration f of S. One-to-one enumerations f and g are equivalent, iff $A_f(S)$ and $A_g(S)$ are computably isomorphic.

Proof: The computable presentation for $A(S)$ has been constructed above. It is also straightforward that if two one-to-one enumerations f and g of S are equivalent, then the algebras $A_f(S)$ and $A_g(S)$ are computably isomorphic. On the other hand, if the algebras $A_f(S)$ and $A_g(S)$ are computably isomorphic, then for every idempotent $e_i \in A_f(S)$ we can effectively compute its image in $A_g(S)$ and compute at which stage it appears in the construction of $A_g(S)$. If it were, say the jth stage, then we set $\Phi(i) = j$. This gives us a computable function $\Phi: \omega \to \omega$ such that $f = g\Phi$.

Lemma 3.6 Let $\mathcal{A}$ be a computable presentation of $A(S)$. Then one can construct a one-to-one computable enumeration $f = f(\mathcal{A})$ of S such that $\mathcal{A}$ and $A_f(S)$ are computably isomorphic.

Proof: Let $\mathcal{A} = \{a_0, a_1, \ldots\}$ be all elements of $\mathcal{A}$ listed in a sequence. We can effectively list all idempotents $e_0, e_1, \ldots$ of $\mathcal{A}$ which will form a subsequence of this sequence. By Lemma 3.4 these idempotents are the unit elements of the components. Let $F_i = \{e_i, 2e_i, \ldots, pe_i\}$ be the copy of the base field F which is contained in the component F_{M_i}. An element x belongs to the component F_{M_i} iff the condition $x = xe_i = e_ix$ is satisfied. Therefore

$$f(i) = \{m \mid \exists x \ (x = xe_i = e_ix \text{ and } x \text{ is algebraic of degree } p_m \text{ over } F_i)\}$$

enumerates S and $f = f(\mathcal{A})$ is a computable enumeration of S. Moreover f is one-to-one. Clearly $\mathcal{A}$ and $A_f(S)$ are computably isomorphic. We will sketch the construction of this computable isomorphism:

Step 0: Compute the number of e_0 in the sequence, say $e_0 = a_s$, and set $M_{00} = \emptyset$ if among $a_0, \ldots, a_{s-1}$ there are no elements x such that $xe_0 = e_0x = x$ which are algebraic over F_0 of prime degree. If such an element α, say of prime degree p_m, existed, we set $M_{00} = \{m\}$ and and put in correspondence σ_0 the subfield $F_0[\alpha] \subseteq \mathcal{A}$ with the field $F(M_{00}) \subseteq A(S)$.

Step i: We compute the number of e_i, say $e_i = a_t$, and look for the first element $x \in \{a_0, a_1, \ldots, a_{t-1}\}$ in the sequence such that $x = xe_j = e_jx$, for one of the numbers $j = 1, 2, \ldots, i$, and such that x is algebraic of a prime degree p_n over F_j. Then take

$$M_{i0} = M_{i-10}, \ \ldots, \ M_{i-jj} = M_{i-j-1j} \cup \{n\}, \ \ldots, \ M_{0i},$$

where $M_{0\,i} = \emptyset$ or $\{n\}$ if $j = i$. If such x is not found we leave all the sets as they were, just add an empty $M_{0\,i}$. We can now find a partial subalgebra of $\mathcal{A}$ which will be in a computable correspondence σ_i with the partial subalgebra $(F_{M_{i0}} \star \ldots \star F_{M_{0i}})^{(i)}$. The lemma is proved.

Theorem A For every positive integer n there exists a computable ring of algorithmic dimension n.

Proof. Let S be a family of computable enumerable sets which has up to equivalence exactly n one-to-one computable enumerations. Such a family exists due to Theorem 2.1. Let $f_1, \ldots, f_n$ be any n mutually non-equivalent computable one-to-one enumerations of S. We construct the algebra $A(S)$ as shown in the beginning of this section. By Lemma 3.5 the computable presentations $A_{f_1}(S), \ldots, A_{f_n}(S)$ are not computably isomorphic. Let $\mathcal{A}$ be an arbitrary computable presentation of $A(S)$. Then by Lemma 3.6 $\mathcal{A}$ is computably isomorphic to a computable algebra $A_f(S)$ for some one-to-one computable enumeration $f = f(\mathcal{A})$. Since f is equivalent to one of the enumerations $f_1, \ldots, f_n$, the algebra $A_f(S)$ is computably isomorphic to one of the algebras $A_{f_1}(S), \ldots, A_{f_n}(S)$. The theorem is proved.

4. Computably Categorical Rings and Their Expansions by Constants.

In this section our task will be more difficult as we will encode a family S of pairs of sets into a ring. In order to define the algebra $A(S)$ in which the family S is encoded we have to enumerate S somehow, simply for having notations necessary for the abstract definition of this algebra. This enumeration is not assumed to be computable. As in the section 3 immediately after $A(S)$ is defined this enumeration will be forgotten and we will consider how computable enumerations of S lead to computable presentations of $A(S)$. Suppose that

$$S = \{(M_0, N_0), (M_1, N_1), (M_2, N_2), \ldots\}.$$

Let us consider the free product (in the variety of all nonassociative rings)

$$B(S) = F[x] \star F[y] \star (F_{M_0} \oplus F_{N_0}) \star \ldots \star (F_{M_k} \oplus F_{N_k}) \star \ldots ,$$

where $F[x]$ and $F[y]$ be two polynomial rings in x and y (we view these polynomials without constant terms), and F_{M_k} and F_{N_k} denote the fields encoding M_k and N_k as was described in the previous section. Finally we consider the quotient-algebra

$$A(S) = B(S)/R,$$

where R is the ideal of $B(S)$ generated by all sets $xF_{M_i} \cup F_{M_i}x$ and $yF_{N_i} \cup F_{N_i}y$. This algebra has also the following description. A basis of $A(S)$ can be chosen consisting of nonassociative products

$$(a_1 a_2 \dots a_n)_q, \qquad n \geq 1, \tag{7}$$

where $a_1, \dots, a_n$ belong to the standard monomial bases of the polynomial rings $F[x]$, $F[y]$, or else they are basic monomials of fields F_{M_i} and F_{N_i}. Referring to the sets

$$F_{M_0} \oplus F_{N_0}, \ \dots, \ F_{M_i} \oplus F_{N_i}, \dots \tag{8}$$

as to the components we stipulate that any two neighbouring monomials a_{i-1} and a_i situated in the bracket $(a_{i-1}a_i)$ belong to different components and, in addition, if one of the elements a_{i-1}, a_i is x then the other cannot belong to F_{M_i} or, similarly, if one of the elements a_{i-1}, a_i is y then the other cannot belong to F_{N_i}.

The multiplication table on the basic products defined in (7) is as follows: if $(a_1 a_2 \dots a_n)_p$ and $(b_1 b_2 \dots b_m)_q$ are two basic products and $\max(m, n) > 1$, then

$$(a_1 a_2 \dots a_n)_p \cdot (b_1 b_2 \dots b_m)_q = ((a_1 a_2 \dots a_n)_p (b_1 b_2 \dots b_m)_q), \tag{9}$$

If $m = n = 1$ and a_1, b_1 belong to the same component, then $a_1 b_1 = \sum_{i=1}^{\ell} \beta_i c_i$, where c_i's are basis monomials of the component to which both of them belong, and we define

$$(a_1) \cdot (b_1) = \sum_{i=1}^{\ell} \beta_i (c_i). \tag{10}$$

If one of the elements a_1, b_1 is equal to x and the other belongs to the component F_{M_i}, or else if one of the elements a_1, b_1 is equal to y and the other belongs to F_{N_i}, then $a_1 \cdot b_1 = 0$. Otherwise $a_1 \cdot b_1 = (a_1 b_1)$.

Let $u = (a_1 a_2 \dots a_n)_q$ be a basic product. We set $|u| = n$, and for an element $a = \sum_{i=1}^{\ell} \beta_i u_i$ of $A(S)$ we set $|a| = \max_i |u_i|$. It is clear from the multiplication table (4) and (5) that

$$|a \cdot b| = |a| + |b|, \tag{11}$$

unless $|a| = |b| = 1$ and a, b are from the same component or else one of them is x and the other is from F_{M_i} or one of them is y and the other is from F_{N_i}.

Lemma 4.1 1) The ring $A(S)$ contains isomorphic copies of the components (8).

2) The subset $U_M = F_{M_0} \cup F_{M_1} \cup \ldots \cup F_{M_n} \cup \ldots$ of $A(S)$ can be characterized as the set of all elements $a \in A(S)$ satisfying the condition that $xa = ax = 0$. The subset $U_N = F_{N_0} \cup F_{N_1} \cup \ldots \cup F_{N_n} \cup \ldots$ of $A(S)$ can be characterized as the set of all elements $a \in A(S)$ satisfying the condition that $ya = ay = 0$.

3) The set $E_M = \{e_0, \ldots e_n, \ldots\}$ of unit elements of fields $F_{M_0}, \ldots, F_{M_n}, \ldots$ can be characterized as the set of all idempotents $e \in A(S)$ such that $xe = ex = 0$. The set $E_N = \{f_0, \ldots f_n, \ldots\}$ of unit elements of fields $F_{N_0}, \ldots, F_{N_n}, \ldots$ can be characterized as the set of all idempotents $f \in A(S)$ such that $yf = fy = 0$.

4) The fields F_{M_i} and F_{N_i} can be characterized as the set of all elements $a \in A(S)$ satisfying the conditions $xa = ax = 0$ and $e_i a = ae_i = a$ and $ya = ay = 0$ and $f_i a = af_i = a$, respectively.

5) Two idempotents $e \in E_M$ and $f \in E_N$ are in the same component (i.e., identities of F_{M_i} and F_{N_i} for some i) iff $ef = fe = 0$.

Proof: These statements follow directly from the properties of the multiplication table of $A(S)$.

Lemma 4.2 Let $S = \{(M_i, N_i) \mid i \in \omega\}$ be a symmetric family of pairs of sets. Then there exists an automorphism α of $A(S)$ such that $\alpha(x) = y$.

Proof: The family S is symmetric. Therefore together with every component $F_A \oplus F_B$, with $A \neq B$, we will have also a component $F_B \oplus F_A$ and these components are isomorphic under the isomorphism $\alpha(h_1, h_2) = (h_2, h_1)$. Also every component $F_A \oplus F_A$ has a natural automorphism defined by the same formula. Conditions $\alpha(x) = y$ and $\alpha(y) = x$ define an automorphism of $F[x] \star F[y]$. All of them can be lifted to an isomorphism α of $A(S)$.

Now, given a one-to-one computable enumeration f of S let us construct a computable presentation $A_f(S)$ of $A(S)$. Let us now denote $f(i) = (M_i, N_i)$. Since f is computable, there exists a procedure which produces a 2-dimensional array $\{(M_{in}, N_{in}) \mid i, n \in \omega\}$ of pairs of finite subsets of ω according to the following rules:

(M1) At stage 0 it produces a pair (M_{00}, N_{00}), where the subsets M_{00} and N_{00} are either both empty or contain one element each;

(M2) At stage k it produces pairs of subsets $(M_{k0}, N_{k0}), \ldots, (M_{1k-1}, N_{1k-1})$, (M_{0k}, N_{0k}) so that $M_{k-1i} \subseteq M_{ki}$ and $N_{k-1i} \subseteq N_{ki}$, $i = 1, \ldots, k-1$, and such that for every k

$$\text{card}(M_{k-10} \cup \ldots \cup M_{k-1k-1}) \leq \text{card}(M_{k0} \cup \ldots \cup M_{kk}) + 1;$$

$$\text{card}(N_{k-10} \cup \ldots \cup N_{k-1k-1}) \leq \text{card}(N_{k0} \cup \ldots \cup N_{kk}) + 1.$$

(M3) $\bigcup_{i \geq 0} M_{in} = M_n, \quad$ and $\quad \bigcup_{i \geq 0} N_{in} = N_n.$

Thus using f we can construct an effective sequence of computable partial algebras

$$A(f, 0), A(f, 1), \ldots, A(f, n), \ldots$$

such that:

(A1) $A(f, i)$ is a subalgebra of $A(f, i{+}1)$;

(A2) $A(f, i)$ is isomorphic to

$$(F[x] \star F[y] \star (F_{M_{i0}} \oplus F_{N_{i0}}) \star \ldots \star (F_{M_{0i}} \oplus F_{N_{0i}}))^{(i)},$$

the latter being the subspace of $A(S)$ spanned by the basic products of degree $\leq i$ depending only on elements from $F[x]$, $F[y]$, $F_{M_{i0}}, \ldots, F_{M_{0i}}$, $F_{N_{i0}}, \ldots, F_{N_{0i}}$, with the addition and the multiplication inherited from $A(S)$;

(A3) $A_f(S) = \bigcup_{k=0}^{\infty} A(f, i)$ is isomorphic to $A(S)$.

As the sets M_{ki} and N_{ki} are finite the fields $F_{M_{ki}}$ and $F_{N_{ki}}$ are finite-dimensional, hence finite, and partial algebras $A(f, i)$ are also finite-dimensional, and hence also finite. It is important to note that at stage i, when we extend $A(f, i{-}1)$ to $A(f, i)$ only three idempotents will be added, namely the unit element e_i of the field F_{M_i}, the unit element f_i of the field F_{N_i}, and their sum $e_i{+}f_i$. They can be distinguished multiplying by x and y. For example, e_i is the only idempotent out of the three with the property $xe_i = e_i x = 0$. In order to separate stages we start each time enumeration of additional elements with e_i followed by f_i and $e_i{+}f_i$.

Lemma 4.3 1) The ring $A_f(S)$ is computable for every computable one-to-one enumeration f of S.

2) Let f and g be one-to-one computable enumerations. Then

(i) The expanded rings $(A_f(S), x)$ and $(A_g(S), x)$ are computably isomorphic, iff $f \sim g$;

(ii) The expanded rings $(A_f(S), x)$ and $(A_g(S), y)$ are computably isomorphic, iff $f \sim \tilde{g}$.

Proof: The computable presentation for $A(S)$ has been constructed above. The rest of the proof is similar to that of Lemma 3.5.

Lemma 4.4 Let $\mathcal{A}$ be a computable presentation of $A(S)$. Then one can construct a one-to-one computable enumeration $f = f(\mathcal{A})$ of S such that $\mathcal{A}$ is computably isomorphic to both $A_f(S)$ and $A_{\tilde{f}}(S)$.

Proof: Firstly, we can list all idempotents $a_0, a_1, \ldots, a_k, \ldots$ such that $xa_i = a_i x = 0$ in order in which they occur in the given enumeration of $\mathcal{A}$. Secondly, we find a pair for each of them listing the idempotents b_i such that $yb_i = b_i y = 0$ and $a_i b_i = b_i a_i = 0$.

Let $F_i = \{a_i, 2a_i, \ldots, pa_i\}$ and $G_i = \{b_i, 2b_i, \ldots, pb_i\}$ be the corresponding copies of the base field F. By Lemma 4.1 $f(i) = (M_i, N_i)$, where

$$M_i = \{m \mid \exists z\ (z = za_i = a_i z \text{ and } z \text{ is algebraic of degree } p_m \text{ over } F_i)\}$$

$$N_i = \{n \mid \exists z\ (z = zb_i = b_i z \text{ and } z \text{ is algebraic of degree } p_n \text{ over } G_i)\}$$

enumerates S and $f = f(\mathcal{A})$ is a computable enumeration of S. Moreover f is one-to-one. Clearly $\mathcal{A}$ and $A_f(S)$ are computably isomorphic.

If we listed b_i first and in the order in which they occur in the given enumeration of $\mathcal{A}$, we would get the enumeration $\tilde{f}$. Thus $\mathcal{A}$ and $A_{\tilde{f}}(S)$ are also computably isomorphic.

Lemma 4.5 Suppose that S is symmetric and its algorithmic dimension is 2. Then $A(S)$ is computably categorical.

Proof: Let $\mathcal{A}$ and $\mathcal{B}$ be any two computable presentations of $A(S)$. Let us apply Lemma 4.4 now and construct one-to-one computable enumerations $f_1 = f(\mathcal{A})$ and $f_2 = f(\mathcal{B})$ of S such that $\mathcal{A}$ and $\mathcal{B}$ are computably isomorphic to $A_{f_1}(S)$ and $A_{f_2}(S)$, respectively. Since the algorithmic dimension of S is 2 we know that either f_1 is equivalent to f_2 or f_1 is equivalent to $\tilde{f}_2$. By Lemma 4.4 $\mathcal{A}$ and $\mathcal{B}$ are computably isomorphic.

Theorem B (case $n = 2$) There exists a computably categorical ring $\mathcal{R}$ and a constant $c \in \mathcal{R}$ such that the expanded ring $(\mathcal{R}, c)$ has exactly 2 computable isomorphism types.

Proof: Let S be a symmetric family of pairs of sets which algorithmic dimension is 2 with a computable enumeration f which is not equivalent to $\tilde{f}$. Then by Lemma 4.5 the ring $A(S)$ is computably categorical. Let us show that the expanded ring $(A(S), x)$ has algorithmic dimension 2. The expanded rings $(A(S), x)$ and $(A(S), y)$ are isomorphic by Lemma 4.2 but $(A_f(S), x)$ and $(A_f(S), y)$ are not computably isomorphic as, if they were, enumerations f and $\tilde{f}$ would be equivalent by Lemma 4.3.

Let now $(\mathcal{A}, z)$ be a computable presentation of $(A(S), x)$. Then either $f_{\mathcal{A}} \sim f$ or $f_{\mathcal{A}} \sim \tilde{f}$. Hence by the previous lemmata $(A(S), x)$ has exactly two computable isomorphism types. The theorem is proved.

To conclude this section we will briefly explain the guidelines for constructing a computably categorical ring which has exactly k recursive isomorphism types, $k \in \omega$, when expanded by any finite number of constants. A natural step is to consider families of k-tuples of computably enumerable sets and define an appropriate notion of symmetry.

Let $X = (X_1, \ldots, X_k)$ be a k-tuple of sets. Define pX to be equal to $(X_k, X_1, \ldots, X_{k-1})$. Thus p is a map defined on the set of all k-tuples of sets.

Definition 4.1 A family S of k-tuples of sets is called *symmetric* if $X = (X_1, \ldots, X_k) \in S$ implies that $pX = (X_k, X_1, \ldots, X_{k-1}) \in S$, that is if S is closed under p. We call the sequence X, pX, p^2X , …, $p^{k-1}X$ the *orbit* of X.

It is obvious that $p^kX = X$. We define also $p^0X = X$.

Suppose that S is a symmetric family of k-tuples. Suppose that f is a one-to-one computable enumeration of S. For each $i \leq k-1$, we define the enumeration f_i by setting $f_i(n) = p^i f(n)$ for all $n \in \omega$. In particular, we see from this definition that f_0 is f.

Definition 4.2 A symmetric family of k-tuples of computably enumerable sets has *dimension* k if there exists a one-to-one computable enumeration f of S with the following two properties:

1) The enumerations $f_0, f_1, \ldots, f_{k-1}$ are pairwise inequivalent.

2) Each computable one-to-one enumeration of S is equivalent to one of the enumerations f_0, f_1, …, f_{k-1}.

In [20] it is proved that there exists a symmetric family S of k-tuples of computably enumerable sets whose dimension is k. Using this result and the ideas of the previous section we can encode S into a ring and prove the following theorem:

Theorem B (general case) For every natural number k there exists a computably categorical ring $\mathcal{R}$ such that for an $c \in \mathcal{R}$, the expanded ring $(\mathcal{R}, c)$ has exactly k types of computable isomorphisms.

Sketch of the Proof: Let S be a symmetric family of dimension k. Suppose that

$$S = \{(M_1^{(i)}, M_2^{(i)}, \ldots, M_k^{(i)}) \mid i \in \omega\}.$$

The algebra $B(S)$ will be constructed as follows. Let us consider the free product (in the variety of all nonassociative rings)

$$B(S) = F[x_1] \star \ldots \star F[x_k] \star B^0(S) \star \ldots \star B^n(S) \star \ldots,$$

where $F[x_i]$ is a polynomial ring in x_i (without constant terms), $B^i(S) = F_{M_1^{(i)}} \oplus \ldots \oplus F_{M_k^{(i)}}$ and $F_{M_j^{(i)}}$ denotes the fields encoding $M_j^{(i)}$ as was described in the previous section. Finally we consider the quotient-algebra

$$A(S) = B(S)/R,$$

where R is the ideal of $B(S)$ generated by all sets $x_j F_{M_j^{(i)}} \cup F_{M_j^{(i)}} x_j$, for all $i \in \omega$.

Due to the symmetry of the family there exists an isomorphism α of $A(S)$ such that $\alpha(x_i) = x_{i+1}$ (addition modulo k).

Let f be a computable enumeration of S which satisfies properties 1) and 2) of Definition 4.2. As in Section 4 we construct a computable presentation $A_f(S)$ of $A(S)$. In a similar way it can be shown that the ring $A(S)$ is computably categorical but its extention $(A(S), x_1)$ has algorithmic dimension k with $(A_f(S), x_1), \ldots, (A_f(S), x_k)$ being k non-equivalent computable presentations of it.

5. Computably Categorical Groups and Their Expansions by Constants.

In this section we will start with the construction of a nilpotent of class 2 group $G(\mathcal{R})$ from an arbitrary nonassociative ring $\mathcal{R}$ with a unit element 1 which is due to Malcev [25]. In addition to Malcev's assumptions we will assume that the ring $\mathcal{R}$ is computable and we will observe that the group $G(\mathcal{R})$ also can be considered as a computable group. We will show that $G(\mathcal{R})$ can be expanded by constants a_1 and a_2 so that the computable isomorphism types of $\mathcal{R}$ are in one-to-one correspondence with the computable isomorphism types of the expanded group $(G(\mathcal{R}), a_1, a_2)$.

Let $\mathcal{R}$ be an arbitrary nonassociative ring of characteristic $p > 2$. In this case it can be considered as an algebra over a finite field $\mathbb{Z}_p$. We assume that $\mathcal{R}$ has a unit element 1. According to Malcev, the group $G(\mathcal{R})$ is the set of all triples (a, b, c) of elements $a, b, c \in \mathcal{R}$ with the multiplication given by the formula

$$(a, b, c)(x, y, z) = (a + x, b + y, bx + c + z). \tag{12}$$

It is easy to check that, so defined, this multiplication is associative, no matter what the ring $\mathcal{R}$ were, that the triple $e = (0, 0, 0)$ is the identity element for it and that

$$(a, b, c)^{-1} = (-a, -b, ba - c). \tag{13}$$

When $\mathcal{R}$ is associative, this group can be represented as the group of upper triangular 3×3 matrices via the isomorphism

$$(a, b, c) \mapsto \begin{pmatrix} 1 & b & c \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix}, \qquad a, b, c \in \mathcal{R},$$

in which form $G(\mathcal{R})$ is known as the Heisenberg group.

Clearly, if $\mathcal{R}$ is a computable ring, then under the standard enumeration of triples the group $G(\mathcal{R})$ is a computable group.

From the formula (12) we see that the centre $\mathcal{Z}$ of the group $G(\mathcal{R})$ consists of triples $(0, 0, c)$, $c \in \mathcal{R}$, and since

$$(a, b, c)(x, y, z)(a, b, c)^{-1}(x, y, z)^{-1} = (0, 0, bx - ya) \tag{14}$$

we see that the group $G(\mathcal{R})$ is nilpotent of class 2. We will put in correspondence ϕ to $\mathcal{R}$ the expansion of $G(\mathcal{R})$ by the following two constants: $a_1 = (1, 0, 0)$ and $a_2 = (0, 1, 0)$, i.e., we set

$$\phi(\mathcal{R}) = (G(\mathcal{R}), a_1, a_2).$$

Lemma 5.1 If two computable rings $\mathcal{R}_1$ and $\mathcal{R}_2$ are computably isomorphic, then their corresponding computable expanded groups $\phi(\mathcal{R}_1)$ and $\phi(\mathcal{R}_2)$ are also computably isomorphic.

Proof: Let $\sigma: \mathcal{R}_1 \to \mathcal{R}_2$ be a computable isomorphism of rings. Then it takes the identity 1_1 of $\mathcal{R}_1$ to the identity 1_2 of $\mathcal{R}_2$. It is now easy to check that the mapping

$$\bar{\sigma}((a,b,c)) = (a^\sigma, b^\sigma, c^\sigma) \tag{15}$$

is a computable isomorphism of the corresponding expanded groups.

Let us now consider the folowing five properties for an expanded group $\mathcal{G} = (\mathcal{G}, a_1, a_2)$ introduced in the Malcev's paper [25]:

(G1) $\mathcal{G}$ is nilpotent of class 2;

(G2) The subsets

$$\mathcal{C}_i = \{x \in G \mid xa_i = a_i x\}, \quad i = 1, 2,$$

are abelian subgroups of $\mathcal{G}$;

(G3) The intersection of $\mathcal{C}_1$ and $\mathcal{C}_2$ is exactly the centre $\mathcal{Z}$ of the group $\mathcal{G}$, i.e., $\mathcal{C}_1 \cap \mathcal{C}_2 = \mathcal{Z}$;

(G4) For each pair $z_1, z_2 \in \mathcal{Z}$ there exists an element $h(z_1, z_2) \in \mathcal{G}$ such that

$$a_1 h(z_1,z_2) a_1^{-1} h(z_1,z_2)^{-1} = z_1, \qquad a_2 h(z_1,z_2) a_2^{-1} h(z_1,z_2)^{-1} = z_2; \tag{16}$$

(G5) There exist isomorphisms $f_i: \mathcal{Z} \to \mathcal{C}_i$ of $\mathcal{Z}$ into $\mathcal{C}_i$ $(i = 1, 2)$ such that for $c = a_2 a_1 a_2^{-1} a_1^{-1}$ the following conditions hold: $f_1(c) = a_1$, $f_2(c) = a_2^{-1}$, and

$$a_2 f_1(z) a_2^{-1} f_1(z)^{-1} = a_1 f_2(z) a_1^{-1} f_2(z)^{-1} = z. \tag{17}$$

Theorem 5.1 Let $\mathcal{R}$ be a computable nonassociative ring of characteristic $p > 2$ with a unit element 1. Then $G(\mathcal{R})$ is a computable group with the properties (G1)-(G5) satisfying $x^p = e$. The functions h, f_1, f_2 are computable.

Proof: Most of these facts were proved in [25]. We should only check that when $\mathcal{R}$ is computable, then $G(\mathcal{R})$ is computable also and to show the computability of the three functions involved. Direct calculations show that

$\mathcal{C}_1$ consists of all triples $(\alpha, 0, \gamma)$ and $\mathcal{C}_2$ consists of all triples $(0, \beta, \gamma)$, and the centre $\mathcal{Z}$ consists of all triples $(0, 0, \gamma)$, where $\alpha, \beta, \gamma \in \mathcal{R}$.

If $z_1 = (0, 0, \gamma_1)$, $z_2 = (0, 0, \gamma_2)$, then $h(z_1, z_2) = (-\gamma_2, -\gamma_1, 0)$ is a computable function satisfying (16).

If $z = (0, 0, \gamma)$, then $f_1(z) = (\gamma, 0, 0)$ and $f_2(z) = (0, -\gamma, 0)$ are computable functions satisfying (17).

These functions are clearly computable.

Lemma 5.2 If $\mathcal{G} = (\mathcal{G}, a_1, a_2)$ is a computable expanded group with the identity $x^p = e$, p prime, satisfying (G1)-(G4), then:

(a) The function $h(z_1, z_2)$ is computable ;

(b) The condition (G5) is also satisfied for $\mathcal{G}$ with computable isomorphisms f_1 and f_2.

Proof: (a) is clear. To prove that a computable isomorphism f_1 in (b) exists we first note that the mapping $\lambda\colon \mathcal{C}_1 \to \mathcal{Z}$ given by

$$\lambda\colon x \mapsto [a_2, x]$$

is a homomorphism of $\mathcal{C}_1$ onto $\mathcal{Z}$. Indeed,

$$[a_2, xy] = a_2 xy a_2^{-1} y^{-1} x^{-1} = a_2 x a_2^{-1} a_2 y a_2^{-1} y^{-1} x^{-1} =$$

$$a_2 x a_2^{-1} [a_2, y] x^{-1} = [a_2, x][a_2, y],$$

since $[a_2, y] \in \mathcal{Z}$. Also λ is onto because of (G4).

As the centre $\mathcal{Z}$ is an abelian group with the identity $x^p = e$ it can be considered as a vector space over $\mathbb{Z}_p$ via $k \cdot z = z^k$, $k \in \mathbb{Z}_p$. Since $\mathbb{Z}_p$ is finite, the basis $\{z_i \mid i \in \omega\}$ of $\mathcal{Z}$ as a vector space, with $z_0 = [a_2, a_1]$, can be constructively found as well as the set of elements $\{c_i \mid i \in \omega\}$ of $\mathcal{C}_1$ such that $c_0 = a_1$ and $\lambda(c_i) = z_i$.

Let $z = \sum k_i \cdot z_i = \prod z_i^{k_i}$, then we define $f_1(z) = \sum k_i \cdot c_i$. Then

$$a_2 f_1(z) a_2^{-1} f_1(z)^{-1} = [a_2, f_1(z)] = \lambda(f_1(z)) = \lambda\left(\prod c_i^{k_i}\right) = \prod z_i^{k_i} = z.$$

A computable isomorphism f_2 can be constructed similarly.

Now we will describe the second part of the construction, namely how, given the computable expanded group $\mathcal{G} = (\mathcal{G}, a_1, a_2)$ with the properties (G1)-(G4), we can construct a computable ring $\psi(\mathcal{G})$ with a unit element.

Theorem 5.2 Let $\mathcal{G} = (\mathcal{G}, a_1, a_2)$ be a computable expanded group with the identity element e and such that the properties (G1)-(G4) are satisfied. Then

(a) The centre $\mathcal{Z}$ of this group is a computable set;

(b) Together with the following operations

$$\begin{aligned} z_1 + z_2 &= z_1 z_2, & (18) \\ z_1 \times z_2 &= h(e, z_2)h(z_1, e)h(e, z_2)^{-1}h(z_1, e)^{-1}, & (19) \end{aligned}$$

the zero element e and the identity element $c = a_2 a_1 a_2^{-1} a_1^{-1}$, the centre $\mathcal{Z}$ forms a computable ring $\psi(\mathcal{G}) = (\mathcal{Z}, +, \times, e, c)$.

(c) The multiplication (19) does not depend on the function $h(z_1, z_2)$.

Proof: Since according to (G3)

$$\mathcal{Z} = \{z \in \mathcal{G} \mid za_1 = a_1 z \text{ and } za_2 = a_2 z\},$$

the centre $\mathcal{Z}$ is a computable subset of ω. The ring addition (18) is clearly computable because the group multiplication is computable. The ring multiplication (19) is also computable since h is a computable function.

Let h and g be two functions satisfying (16). Let us denote $x_1 = h(z_1, e)$, $x_2 = h(e, z_2)$ and $y_1 = g(z_1, e)$, $y_2 = g(e, z_2)$. We have to prove that

$$x_2 x_1 x_2^{-1} x_1^{-1} = y_2 y_1 y_2^{-1} y_1^{-1}. \tag{20}$$

According to (16) we have $a_i y_i a_i^{-1} y_i^{-1} = a_i x_i a_i^{-1} x_i^{-1}$, from which it follows that $a_i x_i^{-1} y_i = x_i^{-1} y_i a_i$, i.e., $x_i^{-1} y_i \in \mathcal{C}_1 \cap \mathcal{C}_2 = \mathcal{Z}$. But then (20) follows as it is equivalent to $x_1 x_2^{-1}(x_1^{-1} y_1) = (x_2^{-1} y_2) y_1 y_2^{-1}$, which is true since $x_i^{-1} y_i \in \mathcal{Z}$. We again refer to the Malcev's paper [25] for the rest of the proof.

Theorem 5.3 (a) Let $\mathcal{R}$ be a computable ring with a unit element. Then $\psi(\phi(\mathcal{R}))$ is computably isomorphic to $\mathcal{R}$.

(b) Let $\mathcal{G} = (\mathcal{G}, a_1, a_2)$ be a computable expanded group, satisfying $x^p = e$, with the properties (G1)-(G4). Then $\phi(\psi(\mathcal{G}))$ is computably isomorphic to $\mathcal{G}$.

Proof: (a) The mapping $(0, 0, \gamma) \mapsto \gamma$ could be verified to be a required isomorphism.

(b) As Lemma 5.2 shows the condition (G5) is also true with computable functions f_1 and f_2. Now we have to follow Malcev and we have to verify only the effectiveness of his construction. Let us construct the ring $\mathcal{R} = \psi(\mathcal{G}) = (\mathcal{Z}, +, \times, e, c)$ as in part (b) of Theorem 5.2 and then let us form the set of triples of elements of $\mathcal{Z}$ to construct $G(\mathcal{R})$. As Malcev showed - and the condition (G5) is essential for that - the mapping

$$z = (z_1, z_2, z_3) \mapsto \tau(z) = f_1(z_1) f_2(z_2)^{-1} z_3 \tag{21}$$

is an isomorphism of $\phi(\mathcal{R})$ onto $\mathcal{G}$. Since f_1 and f_2 are computable functions τ is also computable.

Lemma 5.3 Let $\mathcal{G} = (\mathcal{G}, a_1, a_2)$ and $\tilde{\mathcal{G}} = (\tilde{\mathcal{G}}, \tilde{a}_1, \tilde{a}_2)$ be two isomorphic computable expanded groups, satisfying $x^p = e$, and $\mathcal{G}$ satisfies the conditions (G1)-(G4). Then

(a) $\tilde{\mathcal{G}}$ also satisfies conditions (G1)-(G4);

(b) $\mathcal{G}$ and $\tilde{\mathcal{G}}$ are computably isomorphic to $\phi(\mathcal{R})$ and $\phi(\tilde{\mathcal{R}})$ for some isomorphic computable rings $\mathcal{R}$ and $\tilde{\mathcal{R}}$. The expanded groups $\mathcal{G}$ and $\tilde{\mathcal{G}}$ are computably isomorphic, if and only if the rings $\mathcal{R}$ and $\tilde{\mathcal{R}}$ are computably isomorphic.

Proof: (a) Let $\sigma: \mathcal{G} \to \tilde{\mathcal{G}}$ be the given isomorphism. Then $\sigma(\mathcal{Z}) = \tilde{\mathcal{Z}}$ and $\tilde{\mathcal{C}}_i = \sigma(\mathcal{C}_i)$. It implies that conditions (G1)-(G3) hold for $\tilde{\mathcal{G}}$. To prove (G4) we need to equip $\tilde{\mathcal{G}}$ with an appropriate function $\tilde{h}$. In order to do this we may define

$$\tilde{h}(\sigma(z_1), \sigma(z_2)) = \sigma(h(z_1, z_2)).$$

As σ is an isomorphism the condition (G4) for $\tilde{\mathcal{G}}$ is satisfied.

(b) By Theorem 5.3 (b) $\mathcal{G}$ and $\tilde{\mathcal{G}}$ are computably isomorphic to $\phi(\mathcal{R})$ and $\phi(\tilde{\mathcal{R}})$ for the computable rings $\mathcal{R} = \psi(\mathcal{G})$ and $\tilde{\mathcal{R}} = \psi(\tilde{\mathcal{G}})$. It is clear from the way $\tilde{h}$ was introduced that these two rings are isomorphic. Also, if σ was computable isomorphism, then $\mathcal{R}$ and $\tilde{\mathcal{R}}$ are computably isomorphic. On the other hand, if $\mathcal{R}$ and $\tilde{\mathcal{R}}$ are computably isomorphic then $\mathcal{G}$ and $\tilde{\mathcal{G}}$ are computably isomorphic because by Theorem 5.3 they computably isomorphic to $\psi(\mathcal{R})$ and $\psi(\tilde{\mathcal{R}})$, respectively.

Theorem 5.4 Let $\mathcal{R}$ be a computable ring of characteristic $p > 2$ with identity. Then if $S_{\mathcal{R}} = \{\mathcal{R}_\alpha \mid \alpha \in I\}$ is the full set of representatives of the computable isomorphism types of $\mathcal{R}$, then $S_{\mathcal{G}} = \{\phi(\mathcal{R}_\alpha) \mid \alpha \in I\}$ is the full set of representatives of the computable isomorphism types of $\mathcal{G} = \phi(\mathcal{R})$.

Proof: Since $\mathcal{G} = \phi(\mathcal{R})$ satisfies (G1)-(G4) by Theorem 5.1, then by Lemma 5.1 (b) all groups, which are isomorphic to $\mathcal{G}$, are in $S_{\mathcal{G}}$. The rest of the theorem follows from Lemma 5.3.

Corollary 5.1 Let $\mathcal{R}$ be a computable ring of characteristic $p > 2$ with identity. Then the algorithmic dimension of the expanded group $\phi(\mathcal{R}) = (G(\mathcal{R}), a_1, a_2)$ is equal to the algorithmic dimension of $\mathcal{R}$. In particular $\mathcal{R}$ is computably categorical if and only if $\phi(\mathcal{R})$ is computably categorical.

Theorem 5.5 Let $\mathcal{R}$ be a computable ring of characteristic $p > 2$ with identity and $r \in \mathcal{R}$. Let us consider $\phi(\mathcal{R}) = (G(\mathcal{R}), a_1, a_2)$ and define $a_3(r) = (0, 0, r) \in \phi(\mathcal{R})$. Then the algorithmic dimension of the expanded group

$$(\phi(\mathcal{R}), a_3(r)) = (G(\mathcal{R}), a_1, a_2, a_3(r))$$

is equal to the algorithmic dimension of the expanded ring $(\mathcal{R}, r)$.

Proof: Suppose that $(\mathcal{R}_\alpha, r_\alpha)$ and $(\mathcal{R}, r)$ are (computably) isomorphic and let $\sigma: \mathcal{R} \to \mathcal{R}_\alpha$ be a (computable) isomorphism such that $\sigma(r) = r_\alpha$. Then the (computable) isomorphism $\bar{\sigma}$ of $\phi(\mathcal{R})$ onto $\phi(\mathcal{R}_\alpha)$, defined by (15), takes $a_3(r)$ to $a_3(r_\alpha)$, i.e. $(\phi(\mathcal{R}_\alpha), a_3(r_\alpha))$ and $(\phi(\mathcal{R}), a_3(r))$ are (computably) isomorphic.

Suppose that $(\phi(\mathcal{R}_\alpha), a_3(r_\alpha))$ and $(\phi(\mathcal{R}_\beta), a_3(r_\beta))$ are (computably) isomorphic and

$$\mu: \phi(\mathcal{R}_\alpha) \to \phi(\mathcal{R}_\beta)$$

is the corresponding (computable) isomorphism such that $\mu(a_3(r_\alpha)) = a_3(r_\beta)$. Then this (computable) isomorphism induces a (computable) isomorphism $\bar{\mu}$ of

$$\bar{\mu}: \psi(\phi(\mathcal{R}_\alpha)) \to \psi(\phi(\mathcal{R}_\beta))$$

Due to ((21)) after identifying $\psi(\phi(\mathcal{R}_\alpha))$ with $\mathcal{R}_\alpha$ and $\psi(\phi(\mathcal{R}_\beta))$ with $\mathcal{R}_\beta$ we will see that $\bar{\mu}(r_\alpha) = r_\beta$, i.e. $(\mathcal{R}_\alpha, r_\alpha)$ and $(\mathcal{R}_\beta, r_\beta)$ are (computably) isomorphic.

Theorem 5.5 and Theorem B immediately lead to the main Theorem of this paper:

Theorem C For every prime $p > 2$ and for every $n \in \omega \bigcup \{\omega\}$ there exists a computably categorical nilpotent group $\mathcal{G}$ of class 2 satisfying $x^p = 1$

such that for some constants $a_1, a_2, a_3 \in \mathcal{G}$ the expanded group $(\mathcal{G}, a_1, a_2, a_3)$ is of algorithmic dimension n.

Proof: Let us consider a ring $\mathcal{R}$ and its element $r \in \mathcal{R}$ which satisfy Theorem B. Let us construct $\phi(\mathcal{R}) = (G(\mathcal{R}), a_1, a_2)$. Then according to Corollary 5.1 $\phi(\mathcal{R})$ and hence $G(\mathcal{R})$ are computably categorical. At the same time by Theorem 5.5 $(\phi(\mathcal{R}), a_3) = (G(\mathcal{R}), a_1, a_2, a_3)$, where $a_3 = a_3(r)$, is of algorithmic dimension n. The theorem is proved.

References

[1] JN Crossley, ed. Aspects of Effective Algebra. Proceedings of a Conference at Monash University, Australia, 1979, Upside Down A Book, Yarra Glen, 1981.

[2] J Remmel. Recursive Boolean Algebras. In: Handbook of Boolean Algebras, v.3. North Holland, 1990.

[3] V Harizanov. Pure Recursive Model Theory. In: Yu Ershov, S Goncharov, A Nerode, J Remmel eds. Handbook of Recursive Mathematics, to appear.

[4] T Millar. Abstract Recursive Model Theory. In: E Griffor, ed. Handbook of Recursion Theory. North-Holland, to appear.

[5] A Frölich and JC Shepherdson. Effective Procedures in Field Theory. Phil Trans Roy Soc London, ser. A, 248: 407–432, 1956.

[6] AI Malcev. Constructive Algebras. Uspekhi Matem. Nauk. 16:3–60, 1961.

[7] MO Rabin. Computable Algebra, General Theory and Theory of Computable Fields. Trans Amer Math Soc 95:341-360, 1960.

[8] R Soare. Recursively Enumerable Sets and Degrees. Berlin: Springer, 1987.

[9] M Hall Jr. The theory of groups. New York, N.Y: The MacMillan Co, 1959.

[10] P Jordan, J von Neumann, E Wigner. On an algebraic generalization of the quantum mechanical formalism. Ann Math 36: 29–64, 1934.

[11] IMH Etherington. Genetic algebras. Proc Roy Soc Edinburgh 59: 242–258, 1939.

[12] SS Goncharov. The Problem of the Number of Non-Autoequivalent Constructivizations. Algebra i Logika 19:58–61, 1980.

[13] SS Goncharov. Autostability of Models and Abelian Groups. Algebra i Logika 19: 23–44, 1980.

[14] SS Goncharov, VD Dzgoev. Autostability of Models. Algebra i Logika 19:45–58, 1980.

[15] J Remmel. Recursive Isomorphisms Types of Recursive Boolean Algebras. J Symb Logic 46: 572–594, 1981.

[16] SS Goncharov. Groups with a Finite Number of Constructivizations. Soviet Math Dokl. 23:621–639, 1981.

[17] SS Goncharov, AV Molokov, NS Romanovsky, Nilpotent Groups of Finite Algorithmis Dimension. Siberian Math Journal 30:82–88, 1989.

[18] T Millar. Recursive Categoricity and Persistence. J Symb Logic 51: 430–434, 1986.

[19] Yu Ershov and SS Goncharov, eds. Logic Notebook: Problems in Mathematical Logic. Novosibirsk: Novosibirsk University, 1986.

[20] P Cholak, S Goncharov, B Khoussainov, R Shore. Computably Categorical Structures and Expansions by Constants, submitted.

[21] S Lang. Algebra. Addison-Wesley Pub. Co., Advanced Book Program, 1984.

[22] B Khoussainov, R Shore. Categoricity and Scott Families. In: Eds: DS Bridges ...[at al.]. Combinatorics, Complexity and Logic: Proceedings of DMTCS'96, Springer, 1996, pp 299–307.

[23] B. Khoussainov, R.Shore, Computable Isomorphisms, Degree Spectra of Relations and Scott Families, Ann. of Pure and Applied Logic, to appear.

[24] V. Harizanov, Turing Degree of Nonzero Member in Two Element Degree Spectrum, Ann of Pure and Applied Logic 60:1–30, 1993.

[25] AI Malcev. On one correspondence between rings and groups. Matem Sbornik 50:257–266, 1960.