UNIFORMLY DISTRIBUTED SEQUENCES IN COMPUTER ALGEBRA OR HOW TO CONSTRUCT RANDOM NUMBER GENERATORS

V. S. Anashin

UDC 519.248: 648.5

INTRODUCTION

0.0. Statement of the Problem

Although this work is of a purely mathematical nature, its source was an applied problem, and therefore I deem it necessary to give some preliminary remarks, which motivate the statement of the mathematical problem considered in the work. Since the remarks concern applications, I permit myself not to use mathematical formalism here and give all exact formulations and definitions in the next sections. The problem mentioned above can be formulated as follows: *how to write a program for a computer which would quickly generate random numbers*?

It stands to reason that randomness must be understood here in a purely "Pickwick" sense, namely, in the sense used by Knuth in the third chapter of his famous book *The Art of Computer Programming* [8]. In this monograph, the reader will also find examples of various fields where this kind of problem is encountered. Their list can be complemented by one more field, cryptography. However, the aim of this work is not cryptographic applications (although the results given below can certainly be used in this field), but the construction of a mathematical theory that would refer, generally speaking, to the theory of uniformly distributed sequences on algebraic systems. Computer programs, "random" number generators, can indeed be written with the use of the results obtained if we understand a "random" sequence as a uniformly distributed sequence. Knuth, in his monograph, treats "random" numbers precisely in this sense.

In the same book, Knuth states that the best known (at the time the book was written) random number generators are generators of the sequences $\{z_i\}$ of elements of the set $\{0, 1, 2, \ldots, m-1\}$ with recursion laws of the form $z_i \equiv az_{i-1} + b \pmod m$, where a, b are integers. In this case, the uniform distribution of the sequence $\{z_i\}$ means that this sequence is periodic with period m, and each element of the set $\{0, 1, 2, \ldots, m-1\}$ is encountered on the period exactly once. Thus, the main problem is to find conditions imposed on a, b under which the sequence $\{z_i\}$ has period m. These conditions are given by Theorem A from Sec. 3.2.1.2 of the monograph mentioned above, which serves as a mathematical basis of the so-called linear congruent method of constructing random number program generators.

It pays to view this example from algebraic positions. First, the operations (commands) of the processor which are used to generate random numbers are regarded as operations of a certain algebraic system A. (In this example, A can be regarded either as a cyclic group of order m relative to the operation"+" or as a residue class ring modulo m.) Second, any uniformly distributed sequence of elements of A of the form

$$z_0,\ z_1 = f(z_0),\ \ldots,\ z_i = f(z_{i-1}) = f^i(z_0) = \underbrace{f(f(\ldots f}_{i \text{ times}}(z_0)\ldots)), \ldots,$$

Translated from Itogi Nauki i Tekhniki, Seriya Sovremennaya Matematika i Ee Prilozheniya. Tematicheskie Obzory, Vol. 31, Computing Mathematics and Cybernetics–2, 1995.

where f is a polynomial over A, is considered to be "random." The main problem is to describe the polynomials f which ensure the uniform distribution of the corresponding sequence.

This work is a review of the results connected with the construction of uniformly distributed sequences over algebraic systems as recurrent sequences, the laws of whose recursion are defined by polynomials over these systems. However, the choice of algebraic systems considered in this work was dictated by considerations of applications, namely, algebraic systems which are customary for computer algebra are considered, i.e., simulating systems of commands of some kind of processors.

A typical processor processes information presented by words of a fixed length in some alphabet. If V is the set of all the words and Ω is the list of commands of the processor, i.e., some set of functions defined on V and assuming values in V, then the processor is naturally associated with the universal algebra $A = \langle V, \Omega\rangle$ with supporter V and signature Ω. Since a computer program is an ordered collection of commands successively applied to the running values of the operands, every collection-command of this kind defines the function $F = (f_1, \dots, f_m)$: $A^{(n)} \to A^{(m)}$ of n arguments whose values are collections of m elements from A (which can be regarded as elements from $A^{(n)}$, the nth direct power of the universal algebra A, i.e., the direct product of n isomorphic copies of A). In this case, the components $f_1, \dots, f_m$ of the function F are *polynomials* in the variables $x_1, \dots, x_n$ over A since a polynomial over the universal algebra A is a composition of the characters of the operations from Ω, the constants from V, and the variables. From this point of view, the problem of writing a program generator of "random" numbers consists in constructing the corresponding polynomials over A (namely, components $f_1, \dots, f_n$ such that the sequence $a, F(a), F(F(a)), \dots$ of elements from $A^{(n)}$ is uniformly distributed over $A^{(n)}$) and, consequently, refers to the polynomial algebra whose principal concepts can be found in [21]. Then the performance of the program is determined by the complexity of the polynomials as compositions of operations and the performance of carrying out the operations appearing in these polynomials.

It stands to reason that the solution of such a problem of polynomial algebra in the general statement is impossible since it is necessary to impose some constraints on the universal algebra A. Then we run the risk of losing some cases that are most interesting for applications. Therefore, let us see what universal algebras can simulate the systems of processor commands in the sense mentioned above.

As a rule, the list of processor commands includes as least one group operation. For instance, the list of commands (to be more precise, the assembler) of the Intel 80∗86 processor includes the operation of addition in the $\mathbb{Z}/2^n$ and the operation of addition of n-dimensional vectors over the field $\mathrm{GF}(2)$, where n is the word length of the processor. All the more so, the languages of higher-degree programming contain group operations as the main operations. Let us stipulate that in our sense it is natural to regard as a processor not the integral microcircuit itself but a certain language of programming (or even its compilator) since any program was first written in some language and then was compiled. In this case, the "list of commands" is interpreted as a collection of principal ("elementary") procedures of the language.

We can thus consider the universal algebra A to be a group whose signature is complemented by some additional operations, i.e., A is a *group with multioperators* according to the terminology of Kurosh [11]. The lists of these additional operations will be elucidated below since they are different for different processors. We can now say, however, that the most important for applications are the cases where A is a finite associative and commutative ring or a finite group with a certain (possibly, empty) set of operators. Indeed, the list of commands of a processor contains, as a rule, besides addition, multiplication (then we deal with a ring) and commands interpreted as linear operators (shifts, for instance). In turn, the universal algebras most often encountered in applications are those which are of order 2^n, since the typical microcircuit, i.e., the processor of a modern computer, executes operations with information presented by words of length n in the alphabet $\{0, 1\}$.

Thus, we consider a certain finite group A with multioperators and a certain *polynomial* function $F = (f_1, \dots, f_n)$: $A^{(n)} \to A^{(n)}$ (i.e., $f_1, \dots, f_n$ are polynomials in the variables $x_1, \dots, x_n$ over A). What conditions must be satisfied by F for the sequence $a, F(a), F(F(a)), \dots$ of elements from $A^{(n)}$ to be uniformly distributed over $A^{(n)}$, i.e., to have a period of length $|A|^n$, every element from $A^{(n)}$ occuring exactly once on this period? We

say that these functions are *ergodic*. In the final analysis, we have to obtain the description of all polynomial ergodic functions over each of the universal algebras of the class being considered and all polynomials that define these functions. However, since the existence of a polynomial ergodic function over a universal algebra strongly restricts the possible structure of the latter, we must first describe the universal algebras from the given class which admit of polynomial ergodic functions.

We can generalize somewhat the technique of constructing "random" numbers by considering uniformly distributed sequences of the form $\{\psi(F^i(a))\}$, where F is an ergodic polynomial function and $\psi\colon A^{(n)} \to A^{(m)}$ is a polynomial function. Then the problem arises of finding the conditions which must be satisfied by ψ for the sequence $\{\psi(F^i(a))\}$ to be uniformly distributed for the ergodic F. Clearly, if all points from $A^{(m)}$ have the same number of ψ-co-images in $A^{(n)}$ (we say that these functions are *equiprobable*), then the sequence $\{\psi(F^i(a))\}$ is uniformly distributed for any ergodic F. Thus the problem arises of describing *equiprobable polynomial functions* over universal algebras from the class under consideration. In the special case $m = n$, it consists in describing *bijective* polynomial functions.

Finally, if we denote the group operation in A by $+$, the neutral element by 0, and the inverse of a relative to this operation by $-a$, then it is clear that two polynomials $f(x_1, \dots, x_n)$ and $g(x_1, \dots, x_n)$ over A define the same function if and only if the polynomial $h(x_1, \dots, x_n) = f(x_1, \dots, x_n) - g(x_1, \dots, x_n)$ assumes the value 0 at all points from A^n. We call polynomials h with this property *mixed identities over* A. Thus, when describing *ergodic* or *equiprobable polynomials* (i.e., polynomials that define ergodic or equiprobable functions respectively), we have to consider the facts connected with the description of *mixed identities over a given universal algebra*. Note that for applications especially significant is the description of ergodic and equiprobable polynomials themselves and not only the functions they define, since the complexity of the program realization of the same function is defined by its specific polynomial representation used in the listing of the program.

The problems mentioned above differ in their mathematical nature. The problem of describing universal algebras that admit of ergodic polynomial functions is a typical algebraic problem of classification of universal algebras by some property. Problems of this kind are frequently encountered in the theory of finite groups and finite rings and reduce to studying the corresponding universal algebras with restrictions to subalgebras or quotient algebras. The description of mixed identities of a given universal algebra is a problem close in ideology to the *theory of varieties* of universal algebras, since identities can be regarded as mixed identities without coefficients. As to the description of polynomial ergodic or equiprobable functions over universal algebras that correspond, in the sense indicated above, to the majority of types of processors, this problem, strange as it may seem at first glance, is from a different field of mathematics, namely, the *non-Archimedean analysis*. Here is an example elucidating the last thesis, which is most important for applications.

Let us consider an n-digit processor that operates with words of length n in the alphabet $\{0, 1\}$, which we shall interpret in the sequel as numbers from the set $\mathbb{Z}/2^n = \{0, 1, 2, 3, \dots, 2^n - 1\}$ written in a binary system. As a rule, the standard collection of commands of such a processor contains arithmetic operations (the addition $\oplus$ and multiplication $\odot$ which are, respectively, the addition and the multiplication in a ring of integers with subsequent reduction of the result to modulo 2^n), bit-by-bit logical operations of the type OR, XOR, AND, and computer operations of the type of left and right shifts SHL and SHR. This processor is associated with the universal algebra

$$A = \langle \mathbb{Z}/2^n, \{\oplus, \odot, \mathrm{XOR}, \mathrm{OR}, \mathrm{AND}, \mathrm{SHL}, \mathrm{SHR}\}\rangle.$$

Its operations (i.e., commands of the processor) admit of simple and natural extensions to the set $\mathbb{N}_0$ of nonnegative rational integers. However, relative to the 2-adic metric, the latter is an everywhere dense subset in the compact space $\mathbb{Z}_2$ of all 2-adic integers. The most remarkable fact here is that the corresponding extensions of the above-mentioned operations are continuous (and, hence, uniformly continuous) functions on $\mathbb{Z}_2$. Consequently, the polynomial functions over A can also be extended to uniformly continuous functions on $\mathbb{Z}_2$.

This approach makes it possible to establish correspondences between "discrete" and "continuous" properties of some classes of functions. For instance, from this point of view functions known as *determinate*

functions in the theory of automata turn out to be exactly those functions which satisfy the Lipschitz condition with coefficient 1. There is also a correspondence between bijective functions on the $\mathbb{Z}/2^n$ and 2-adic functions that preserve the Haar measure; between maximal period sequences, generated by congruent generators, and uniformly distributed sequences of 2-adic integers; between ergodic polynomials over the universal algebra A and functions, ergodic with respect to the Haar measure, on the ring $\mathbb{Z}_2$ of 2-adic integers. It appears that these correspondences are not anything external; they demonstrate the non-Archimedean essence of computer commands. It is usually possible to regard the list of commands of a processor (or a considerable part of it) as a set of uniformly continuous 2-adic functions and, having proved by means of the non-Archimedean analysis a certain statement concerning a definite composition of these functions, to obtain a statement concerning the corresponding computer program. In this work, this approach is demonstrated by way of example of program generators of random numbers. However, I am sure that it can be successfully used for solving other programming problems or problems of computer algebra.

Thus, the above-formulated problem of describing ergodic (or equiprobable) polynomials over universal algebras being considered can be reduced to the description of functions continuous on $\mathbb{Z}_2$, *ergodic or equiprobable relative to the Haar measure*. In this paper, this problem is studied as applied to a more general situation of functions on a ring of p-adic integers $\mathbb{Z}_p$, where p is an arbitrary prime number.

In the example given above, we can regard the universal algebra $A = \langle \mathbb{Z}/2^n, \{\oplus, \odot, \mathrm{XOR}, \mathrm{OR}, \mathrm{AND}, \mathrm{SHL}, \mathrm{SHR}\}\rangle$ corresponding to the processor as an *Abelian* group with multioperators (we can take $\oplus$ or XOR as a group operation). However, we can encounter situations in applications where the universal algebra is a *non-Abelian* group with multioperators, especially if the realization of a certain operation depends on the value of the one-bit register, a "flag." For instance, if the flag is equal to 0, then addition is carried out, and if it is 1, then subtraction is carried out. In this way, the $*$ operation of the non-Abelian group appears (in this example, an operation of *dihedral* group): if ε, ξ are the values of the flag, a, b are n-bit words in the alphabet $\{0, 1\}$, then $(\varepsilon, a) * (\xi, b) = (\varepsilon + \xi, b \oplus (-1)^{\xi} a)$, where $\oplus$ is addition modulo 2. As is customary in algebra, a commutative and a noncommutative case must be considered separately, and therefore this work is divided into two chapters which correspond to these two cases. Both cases are studied in the same sequence, i.e., first groups with multioperators are classified that admit of ergodic polynomial functions, and then the functions themselves are described (as well as equiprobable polynomial functions), which often leads to the necessity of describing mixed identities. The last problem in the commutative case does not usually present any difficulties. However, in order to describe mixed identities of non-Abelian groups with multioperators we must develop a special apparatus close, in essence, to the theory of varieties of universal algebras.

On the whole, we can call the sum of the results of this work, connected with the description of ergodic polynomial functions, the theory of *nonlinear congruent generators*, especially if we compare them with the above-mentioned criterion of ergodicity of a linear polynomial over the $\mathbb{Z}/m$ [8, Theorem A, Sec. 3.2.1.2]. The latter result (which goes back to Lehmer) admits of the following equivalent formulation: *a linear polynomial with integer coefficients induces an ergodic function on the ring $\mathbb{Z}/p^m$, $m \geq 2$, where p is a prime number, if and only if it induces an ergodic function on the ring $\mathbb{Z}/p^2$*. This proved to be a typical situation. As a rule, the *polynomial f over the universal algebra $\langle \mathbb{Z}/p^m, \Omega\rangle$ induces an ergodic function for all sufficiently large m if it is ergodic for some $m = m_0(f)$*. (Note that a similar situation occurs with equiprobability and biinjectivity.) Consequently, the problem consists in finding $m_0(f)$ for one or another class of polynomials f. Thus, we can regard this group of results of this work as generalizations of the indicated Lehmer theorem to the case of arbitrary-degree polynomials and over different universal algebras (and not only residue rings). In particular, we consider arbitrary-degree polynomials with integer coefficients, polynomials with rational coefficients that assume integer values at integer points, rational functions with the same property, polynomials over the universal algebra $A = \langle \mathbb{Z}/2^n, \{\oplus, \odot, \mathrm{XOR}, \mathrm{OR}, \mathrm{AND}, \mathrm{SHL}, \mathrm{SHR}\}\rangle$, and others. Here is a typical result, for example: *the function $\frac{f(x)}{1+2g(x)}$ (where $f(x)$, $g(x)$ are polynomials with rational integer coefficients) is ergodic on the ring $\mathbb{Z}/2^n$, $n \geq 3$, if and only if it induces an ergodic function modulo* 8. By the way, generators with this recursion law can be easily realized as a program since they only use the operations of addition,

multiplication, and taking the inverse element modulo 2^n.

Finally, the remark last in order but not in significance. By no means do I insist on constructing good program generators of random numbers only by the methods described in this paper. There are many other well-developed methods; the reader can find them, for instance, in [15, 24, 25]. However, to my mind, the theory presented below is of interest since it demonstrates how, in the process of solving an applied problem, different and seemingly nonintersecting divisions of mathematics suddenly merge into some logical whole, revealing unexpected connections. In some cases, purely theoretical concepts prove to have a "physical meaning" as some model of the real environment. Hensel began studying p-adic numbers more than half a century before the first microchip appeared, and the fact that the commands of the latter could be represented by continuous functions on the space of p-adic integers is one more example of the "incomprehensible effectiveness of mathematics" (M. Kline [7]).

0.1. Preliminaries

Uniformly distributed sequences on topological groups. Before speaking of the uniform distribution of a sequence on a universal algebra, we must define a measure on this algebra. All universal algebras considered in this paper are groups with multioperators, and we shall assume that they are compact topological groups. This constraint by no means restricts the class of groups that are interesting for applications, since it is satisfied by all finite groups as well as infinite groups, which are encountered in this work when uniformly distributed sequences are studied on finite groups with multioperators. A natural, *Haar measure*, exists on a compact topological group whose definition can be found in any book on topological groups, and therefore we omit its general form but will only formulate it for special cases which we shall consider. Here are some necessary concepts and main definitions from the theory of uniformly distributed sequences (see [6]).

Suppose that A is a compact topological group and μ is its Haar measure. Suppose that $\{a_n\}_{n=0}^{\infty}$ is a sequence of elements from A, N is a nonnegative rational integer, U is a subset in A. We set $\nu_N(U) = \sum_{n=0}^{n=N} \chi_U(a_n)$, where χ_U is a characteristic function of the subset U. In other words, $\nu_N(U)$ is the number of terms of the sequence $\{a_n\}_{n=0}^{\infty}$ which lie in U and whose subscripts do not exceed N. Our main definition in the most general form can be formulated as follows.

0.1.1. Definition. The sequence $\{a_n\}_{n=0}^{\infty}$ is *uniformly distributed on* A if

$$\varliminf_{N\to\infty} \frac{\nu_N^{(U)}}{N} \geq \mu(U)$$

for all open subsets $U \subseteq A$ (equivalently, if

$$\varlimsup_{N\to\infty} \frac{\nu_N^{(U)}}{N} \leq \mu(U)$$

for all closed subsets $U \subseteq A$). Or, what is the same, if

$$\lim_{N\to\infty} \frac{\nu_N^{(U)}}{N} = \mu(U)$$

for all Borel subsets $U \subseteq A$ with boundary of measure 0, i.e., such that $\mu(\overline{U} \setminus \operatorname{Int} U) = 0$, where $\operatorname{Int} U$ is the interior of the set U (= the union of all open subsets of U), $\overline{U}$ is the closure of U.

In what follows, we shall use, as a rule, not the general form, but a reformulation applicable to the class of topological groups being considered.

Suppose that S and T are spaces with measures μ and τ, respectively, $f\colon S \to T$ is a measurable function (i.e., every set $f^{-1}(U)$ is μ-measurable for τ-measurable $U \subseteq T$). The function f is said to be *proportional* if $\mu(f^{-1}(U)) = \mu(f^{-1}(V))$ for any two τ-measurable sets U, $V \subseteq T$ when $\tau(U) = \tau(V)$. If μ, τ are probabilistic measures (say, Haar measures), then the proportional function is said to be *equiprobable*. When $S = T$ and

$\mu = \tau$, we say that f *preserves measure* if $\mu(f^{-1}(U)) = \mu(U)$ for every measurable set U. Finally, if f preserves measure and $f^{-1}(U) = U$ implies either $\mu(U) = 0$ or $\mu(U) = 1$ for every μ-measurable set U, then the function f is *ergodic*.

Uniform, measure-preserving, and ergodic mappings are useful tools for constructing uniformly distributed sequences on topological groups, namely, the following proposition is valid.

0.1.2. Proposition. *Suppose that S and T are compact topological groups, $f\colon S \to T$ is a continuous function measurable with respect to the Haar measure. If $\{a_n\}_{n=0}^{\infty}$ is a uniformly distributed sequence over S and f is an equiprobable function, then the sequence $\{f(a_n)\}_{n=0}^{\infty}$ is uniformly distributed over T. In particular, if $S = T$ and f preserves the Haar measure, then $\{f(a_n)\}_{n=0}^{\infty}$ is uniformly distributed. If, moreover, f is ergodic and S is separable, then the sequence $\{f^n(a)\}_{n=0}^{\infty}$ is uniformly distributed for almost all $a \in S$ (by definition $f^n(a) = f(f^{n-1}(a))$, $f^0(a) = a$).*

The proof easily follows from the main definitions and results of [6, see Chapter 3: Definition 1.1, Exercise 1.10, Lemma 2.2].

For greater clarity, we shall reformulate the definitions given above for a case which is trivial from the point of view of topology but very important for applications, where the group A is of the finite order $|A|$ and, consequently, is a discrete topological group. In this case, every subset U in A is simultaneously open, closed, and measurable with Haar measure $\mu(U) = |U|\,|A|^{-1}$. Then the uniform distribution of the sequence $\{a_n\}_{n=0}^{\infty}$ means that

$$\lim_{N\to\infty} \frac{\nu_N^{(U)}}{N} = \frac{|U|}{|A|}$$

for every subset $U \subseteq A$. Moreover, if the groups A and B are of finite orders, then the function $f\colon A \to B$ is equiprobable if and only if $|f^{-1}(a)| = |f^{-1}(b)|$ for all $a, b \in B$. The function $f\colon A \to A$ preserves measure if and only if it is bijective. Finally, f is ergodic if and only if it induces on A a permutation which is a cycle of length $|A|$. In this case, we also say that f is *transitive on A*.

Polynomials over universal algebras. In what follows, we shall also need some concepts from polynomial algebra, which we shall recall or introduce following [21]. We shall first define the concept of a polynomial over a universal algebra.

We shall use the same symbol A for the universal algebra A and for the set of all its elements and shall denote its signature by Ω. Let us consider a nonempty and not more than countable set X of the symbols $x_1, \ldots, x_n, \ldots$ such that $X \cap A = \varnothing$. We say that the elements of the set X are *variables*. Then we can formulate the following inductive definition, which is the most general definition of a *polynomial in the variables $x_1, \ldots, x_n, \ldots$* over the universal algebra A.

0.1.3. Definition. (1) Any variable from X is a polynomial in the variables $x_1, \ldots, x_n, \ldots$ over the universal algebra A; (2) any element of the universal algebra A is a polynomial in the variables $x_1, \ldots, x_n, \ldots$ over the universal algebra A; (3) if $g_1, \ldots, g_m$ are polynomials in the variables $x_1, \ldots, x_n, \ldots$ over the universal algebra A and ω is the symbol of an m-aric operation from Ω, then $\omega(g_1, \ldots, g_m)$ is a polynomial in the variables $x_1, \ldots, x_n, \ldots$ over the universal algebra A; (4) there are no other polynomials in the variables $x_1, \ldots, x_n, \ldots$ over the universal algebra A.

It pays to use this definition if a polynomial over a universal algebra corresponding (in the sense of Sec. 0.0 of this work) to the processor for which the computer program is written must be associated with this program. However, it is not very convenient for mathematical reasoning since, for instance, we must then consider the polynomials $2x + 1$ and $(x + 1) + x$ over $\mathbb{Z}$ to be different. This is not surprising for a programmer, since these programs are different indeed because they are different sequences of commands. As for a mathematician who remembers the classical definition of a polynomial over a commutative ring, he will immediately say that it is the same polynomial. Therefore, the following definition will be more to his taste.

0.1.4. Definition ([21]). Suppose that ν is a variety of universal algebras and $A \in \nu$. We denote by $F(X)$ the free algebra of the variety ν freely generated by the set X, where $X = \{x_1, \ldots, x_n, \ldots\}$, or $X = \{x_1, \ldots, x_n\}$, or $X = \{x\}$, with $X \cap A = \varnothing$. Then the *algebra of polynomials* in the set of variables X over the universal

algebra A is the ν-free product $A[X] = A*F(X)$ and its elements are *polynomials* over the universal algebra A.

We shall also use the notations $A[x_1, \dots, x_n]$ and $A[x]$ in the cases where we consider polynomials in n variables or in one variable respectively. The appearance of elements from A in the notation of the polynomial g represented as an element of the ν-free product $A[X]$ in an irreducible form will be called *coefficients* of the polynomial g. The definition of a polynomial in the form of an irreducible representation of an element of some ν-free product makes it possible to speak of a certain "canonical" form of the polynomial, which we shall write out every time when we study some specific variety ν. By virtue of (3) above, we can regard the set of all polynomials (in the sense of Definition 0.1.3) in the variables X over A as a universal algebra (which we shall denote, for the time being, by $A\{X\}$) of signature Ω. Obviously, $A\{X\}$ is a free universal algebra of signature Ω freely generated by the set $A \cup X$ and $A[X]$ is isomorphic to the quotient algebra of the universal algebra $A\{X\}$ by the congruence defined by the identities of the variety ν (we exclude from consideration the degenerate case of the so-called semidegenerate algebras, see [21]). In this case, the corresponding epimorphism $o\colon A\{X\} \to [X]$ acts identically on X and on the elements from A.

In what follows, we shall also call elements from the universal algebra A (or its Cartesian degree) *points* (or *constants*). The use of the latter term is due to the fact that first of all we shall be interested not in the properties of the polynomials as elements of the corresponding ν-free product, but in the properties of functions defined by the polynomials over the universal algebra A, or *polynomial functions*.

It is clear by intuition how the polynomial $g = g(x_1, \dots, x_n)$ in the variables $x_1, \dots, x_n$ over the universal algebra A defines the polynomial function $\varphi_g(x_1, \dots, x_n)$: its value $\varphi_g(a_1, \dots, a_n)$ at the point $(a_1, \dots, a_n) \in A^{(n)}$ is the value of the polynomial g at this point which results if we replace all appearances of all the variables x_i in the notation of g as elements of the ν-free product $A[x_1, \dots, x_n]$ by the elements $a_i \in A$, $i = 1, \dots, n$, respectively and carry out the corresponding computations in A. The formal definition reads as follows: let us consider the sequence $\{a_i \in A\colon\ i = 0, 1, 2, \dots\}$, and then, according to the properties of ν-free products, the map $\varepsilon'\colon X \cup A \to A$ such that $x_i \mapsto a_i$ $(i = 1, 2, \dots)$, $a \mapsto a$ for all $a \in A$, can be uniquely continued to the epimorphism $\varepsilon\colon A[X] \to A$ of universal algebras. Then the image $g\varepsilon$ of the polynomial g under the epimorphism ε is the *value of the polynomial* g (or, what is the same, the *value of the polynomial function* $\varphi_g(x_1, \dots, x_n)$ at the point $(a_1, \dots, a_n)$). In a similar way, we could give the definition of a polynomial function using Definition 0.1.3 rather than 0.1.4. It is easy to understand, however, that in both cases we shall define the same function (in the sense that polynomial functions defined by the polynomials $w \in A\{X\}$ and $g \in A[X]$ coincide if $g = wo$). In the sequel we shall use the same symbol for a polynomial and the corresponding polynomial function in cases where no ambiguity arises. The functions $F\colon A^{(n)} \to A^{(m)}$ of the form

$$F(x_1, \dots, x_n) = (f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)),$$

where $f_1, \dots, f_m$ are polynomials over A, are also polynomial.

Generally speaking, polynomial functions defined by different polynomials $f, g \in A[X]$, $f \neq g$, can coincide. For instance, if A is a group with multioperators and the group operation $+$ (not necessarily commutative) and neutral element 0, then the polynomials f and g define the same function on A if and only if they lie in the same coset with respect to the normal subgroup $I[X] \subseteq A[X]$ consisting of only those polynomials which define the function all of whose values at all points are 0. The elements of the subgroup $I_A[X]$ are called *mixed identities* of the group A and play a significant part in the study of polynomial functions as well as in applications. For instance, if we have to write the shortest program that would realize a given function, then we have to solve a rather typical problem of the combinatorial group theory, namely, choose a representative of the minimal length in the coset with respect of a certain subgroup of a free product (in this case using the subgroup $I_A[X]$). To solve this problem, it is usually necessary to have some description of the subgroup $I_A[X]$. The naturally arising supposition that all mixed identities can be deduced from the identities of the universal algebra A prove, in general, to be incorrect already in the class of noncommutative groups with an empty set of multioperators. However, we sometimes manage to obtain such a description for certain important classes of commutative groups with multioperators.

Typical problems of polynomial algebra are the description of the class of all polynomial functions over a given universal algebra and the description of the class of all algebras on which the polynomial functions satisfy some condition. One of the problems formulated in the introduction to this work refers to the second type, i.e., we mean the description of universal algebras which admit polynomial ergodic functions. This class a fortiori contains all universal algebras C such that every function of n arguments on C, which assumes the values in C, is defined by a certain polynomial over C in n variables, $n = 1, 2, 3, \ldots$. These universal algebras C are said to be *polynomially complete*. For instance, in the class of all commutative rings with identity all finite fields, and only they, are polynomially complete, and in the class of all groups all finite simple non-Abelian groups, and only they, are polynomially complete.

Polynomial functions possess an important property for the formulation of which we shall need the following concept. The function $F\colon A^{(n)} \to A^{(m)}$ of the form $F(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$ is said to be *compatible with all congruences of the universal algebra* A, or, to make it shorter, *compatible*, if for any congruence η of the universal algebra A and every pair $(a_1, \ldots, a_n)$, $(b_1, \ldots, b_n) \in A^{(n)}$ of elements from $A^{(n)}$, congruent modulo η (i.e., elements such that $a_i \eta b_i$, $i = 1, \ldots, n$), their images with respect to F are also congruent modulo η, i.e., $f_j(a_1, \ldots, a_n) \eta f_j(b_1, \ldots, b_n)$, $j = 1, 2, \ldots, m$. Here we deviate from the terminology of [1, 13], where these functions are said to be conservative, and use the terminology accepted by Foster and his followers (see [21, p. 45]), who called them compatible and used the term "conservative" in a different sense. It immediately follows from Definition 0.1.3 that any polynomial function is compatible.

Let $f\colon A \to A$ be a compatible function. If $\phi\colon A \to B$ is any epimorphism of universal algebras, $x, y \in A$ are arbitrary elements from A such that their images with respect to ϕ coincide, i.e., $x\phi = y\phi$, then necessarily $f(x)\phi = f(y)\phi$. This means that every compatible function on A correctly defines a unique function on every epimorphic image of the universal algebra A. Since any epimorphism of the algebra A defines a unique congruence on it and vice versa, we say that f *possesses a certain property* $\mathcal{P}$ *modulo congruence* η if the function induced by the function f on the corresponding epimorphic image possesses $\mathcal{P}$. The corresponding concept for the multidimensional function $F\colon A^{(n)} \to A^{(m)}$ can be introduced by analogy. The following proposition is valid.

0.1.5. Proposition ([1]). *Suppose that A is a finite group, η is its congruence, $F\colon A^{(n)} \to A^{(m)}$ (where $m \leq n$) is an equiprobable (bijective, transitive, resp.) compatible function. Then F is equiprobable (bijective, transitive, resp.) modulo η. Moreover, if A is the direct product of the groups B and C, $A = B \times C$, then F is equiprobable on A if and only if it is equiprobable both on B and on C (i.e., modulo every congruence corresponding to the projection onto a direct cofactor). Finally, the function $F\colon A \to A$ is transitive if and only if it is transitive both on B and on C and the orders of $|B|$ and $|C|$ are coprime.*

This proposition is usually used as a tool that makes it possible to reduce the problems on describing polynomial ergodic or equiprobable functions on finite arbitrary order groups with multioperators to the corresponding problems for a primary order group, say, if the initial group A of order $n = p_1^{m_1}, p_2^{m_2}, \ldots, p_s^{m_s}$ (where $p_1, \ldots, p_s$ are primes and $m_1, \ldots, m_s$ are positive rational integers) with multioperators can be decomposed into the direct product s of groups with primary order multioperators $p_1^{m_1}, p_2^{m_2}, \ldots, p_s^{m_s}$ respectively. The latter is valid a fortiori if, for instance, the group A with multioperators is a commutative ring, an Abelian or nilpotent group with an arbitrary (positive, empty) set of operators, and in some other cases.

Non-Archimedean analysis. We have just made sure that the situation where a group with the multioperators under study is of a primary order is distinguished: it is usually possible to reduce to it the general case of an arbitrary finite group with multioperators and, in addition, universal algebras of order 2^n are most frequently encountered in applications (see Sec. 0.0). It turns out that in a number of important cases we can reduce the study of uniformly distributed sequences, defined by polynomials over the primary order groups with multioperators, to a similar problem for a ring of p-adic integers $\mathbb{Z}_p$, i.e., apply the methods developed for continuous functions to a discrete problem. In this work, we use the methods of non-Archimedean analysis. Therefore, another important special case is uniformly distributed sequences of p-adic integers. Let us reformulate for it the definitions given at the beginning of this section.

The reader can find the main concepts of the p-adic analysis in [9] or [22]. However, we shall recollect

some of them. We fix a certain prime number p and, for any rational integer $n \in \mathbb{Z}$, denote by $\operatorname{ord}_p n$ the exponent of the maximal power p which divides n (i.e., $p^{\operatorname{ord}_p n} \mid n$, but $p^{\operatorname{ord}_p n+1} \nmid n$). In this case $\operatorname{ord}_p n = 0$ for $(n,p) = 1$, $\operatorname{ord}_p 0 = \infty$ by definition. Then any rational integer $n \neq 0$ admits of a unique representation of the form $n = \hat{n}p^{\operatorname{ord}_p n}$, where $(\hat{n}, p) = 1$. We define the *p-adic norm* of any rational number n/m as

$$\left\|\frac{n}{m}\right\|_p = p^{\operatorname{ord}_p m - \operatorname{ord}_p n},$$

with $\|0\|_p = 0$ by definition. With the aid of the p-adic norm, a *p-adic metric* $d_p(u,v) = \|u-v\|_p$ is given on the space $\mathbb{Q}$ of rational numbers. The complement of the space $\mathbb{Q}$ with respect to this metric to a complete metric space is denoted by $\mathbb{Q}_p$ and is called a space of p-adic numbers. This space is *non-Archimedean*, i.e., the Archimedean principle is not satisfied in it (recall that the axiom states that for any two line segments a, b there exists a nonnegative rational integer I such that the length of the segment Ia exceeds that of the segment b). The set $\mathbb{Z}_p$ of all *p-adic integers* is defined by the condition

$$\mathbb{Z}_p = \{s \in \mathbb{Q}_p\colon\ \|s\|_p \leq 1\}$$

and, consequently, is a compact subspace in $\mathbb{Q}_p$. Every p-adic integer s admits of a single *canonical representation* of the form

$$s = \sum_{i=0}^{\infty} \delta_i(s) p^i,$$

where $\delta_i(s) \in \{0, 1, \ldots, p-1\}$. The arithmetic of p-adic integers (i.e., the operations of addition, multiplication, subtraction), represented in canonical form, resemble that of natural numbers represented in the p-ary system with the only difference that, roughly speaking, notations are admitted with an infinite number of significant digits (because of which fact the numbers are usually written left to right and not right to left). Note that negative rational integers have canonical notations with an infinite number of significant digits. For instance, for $p = 2$ the number -1 is written as $11111\ldots$. Using these infinite notations, we can visualize how the bit-by-bit logical operations of a processor are extended to the space $\mathbb{Z}_2$. For example,

$$(-3)\,\mathrm{XOR}\,(-1) = (1011\ldots)\,\mathrm{XOR}\,(1111\ldots) = 0100\ldots = 2,$$

whereas in the language of canonical representations the XOR operation admits of the formal representation

$$\delta_i(s\,\mathrm{XOR}\,t) \equiv \delta_i(s) + \delta_i(t) \pmod 2, \qquad i = 0, 1, 2, \ldots.$$

Other bit-by-bit logical operations (OR, AND, ...) can be defined by analogy. Note that δ_i is also a "computer" operation of taking the ith binary position of a number called an operand. The operation of "elementary" masking with mask consisting of all zeros and having a unity at the ith place will then be written as $2^i\delta_i$, and the operation of an arbitrary masking with mask $\varepsilon_0\varepsilon_1\varepsilon_2\ldots\varepsilon_k$ (where $\varepsilon_i \in \{0,1\}$) is, obviously, $\sum_{i=0}^{k} \varepsilon_i 2^i \delta_i$.

It is easy to verify that all these operations are continuous functions on the topological group $\mathbb{Z}_p$. Its basis of open sets is constituted by balls $a + p^k\mathbb{Z}_p$, where $k = 1, 2, \ldots, a \in \mathbb{Z}_p$. They are all closed sets and in their totality form a basis of Borel sets of the space $\mathbb{Z}_p$, and, therefore, in order to define a Haar measure on $\mathbb{Z}_p$, it is sufficient to determine its value on each of them. By definition, we assume that $\mu(a + p^k\mathbb{Z}_p) = p^{-k}$ for all $k = 1, 2, \ldots, a \in \mathbb{Z}_p$. The topological metric space $\mathbb{Z}_p$ is compact, separable (the set $\mathbb{N}_0$ of all nonnegative rational integers is everywhere dense in $\mathbb{Z}_p$) and has a countable base. The measure μ defined on $\mathbb{Z}_p$ is a real nonnegative normed Borel regular measure (and, hence, a probabilistic measure). The general definition of a uniformly distributed sequence on a compact topological group introduced at the beginning of this section assumes in this case the following form.

0.1.6. Definition. The sequence $\{a_n\}_{n=0}^{\infty}$ of points of the space $\mathbb{Z}_p$ *is uniformly distributed over* $\mathbb{Z}_p$ if

$$\lim_{N\to\infty} \frac{\nu_N(a + p^k\mathbb{Z}_p)}{N} = p^{-k}$$

for all $k = 1, 2, \ldots, a \in \mathbb{Z}_p$. If this relation is satisfied only for a certain $k = k_0$, then we say that the sequence $\{a_n\}_{n=0}^{\infty}$ *is uniformly distributed modulo* p^{k_0}. In the corresponding definition of the n-dimensional uniformly distributed sequence $\{a_n \in \mathbb{Z}_p^{(n)}\}_{n=0}^{\infty}$ the relation given above is replaced by

$$\lim_{N\to\infty} \frac{\nu_N(a + p^k\mathbb{Z}_p^{(n)})}{N} = p^{-kn}.$$

Let us now establish some correspondences between the algebraic properties of $\mathbb{Z}_p$ as a commutative ring and as a metric space. We shall see that this will allow us to establish the correspondences, mentioned in the introduction, between "discrete" and "continuous" properties of computer operations and reduce some problems concerning the construction of uniformly distributed sequences on $\mathbb{Z}/p^k$ to similar problems for $\mathbb{Z}_p$.

Let us consider the function $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ satisfying the Lipschitz condition with coefficient 1, i.e., $\|f(a) - f(b)\|_p \le \|a - b\|_p$ for all $a, b \in \mathbb{Z}_p$. The last condition is obviously equivalent to the system of inclusions $f(a + p^k\mathbb{Z}_p) \subseteq f(a) + p^k\mathbb{Z}_p$ for all open balls $a + p^k\mathbb{Z}_p$ in $\mathbb{Z}_p$. Since $p^k\mathbb{Z}_p$ is an ideal of the ring $\mathbb{Z}_p$ and all ideals in $\mathbb{Z}_p$ are of this form, it follows that what we said above means that *f is a function compatible with all congruences of the ring $\mathbb{Z}_p$ if and only if it satisfies the Lipschitz condition with coefficient* 1. A similar statement is also true for n-dimensional ($n > 1$) functions.

It should be pointed out that these functions f are themselves of interest for the theory of automata, where they are known as *determinate functions*. The latter are defined on the set of all infinite sequences of 0 and 1, assume values in this set, and if $\mathbf{a}, \mathbf{b}$ are two sequences such that their initial segments of length k coincide, then the initial segments of the sequences $f(\mathbf{a})$ and $f(\mathbf{b})$ also coincide. Since we can associate the infinite 0–1-sequence with a unique 2-adic integer in the canonic notation and vice versa, it follows that our statement is valid, i.e., *determinate functions are exactly the functions from $\mathbb{Z}_2$ which satisfy the Lipschitz condition with coefficient* 1.

Let us now consider the arbitrary canonical epimorphism $\phi_k\colon \mathbb{Z}_p \to \mathbb{Z}_p/p^k\mathbb{Z}_p = \mathbb{Z}/p^k$ of the ring $\mathbb{Z}_p$ onto the residue ring $\mathbb{Z}_p/p^k\mathbb{Z}_p$ modulo p^k. This mapping ϕ_k is continuous and measurable. It is obvious that the sequence $\{a_n \in \mathbb{Z}_p\}_{n=0}^{\infty}$ is uniformly distributed modulo p^k if and only if the sequence $\{\phi_k(a_n)\}_{n=0}^{\infty}$ is uniformly distributed over $\mathbb{Z}/p^k$. Next, the compatible function $F = (f_1, \ldots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ is equiprobable if and only if it is *equiprobable modulo* p^k for every k, i.e., $|F_k^{-1}(a)| = |F_k^{-1}(b)|$ for all $a, b \in (\mathbb{Z}/p^k)^{(m)}$, $k = 1, 2, 3, \ldots$. Here F_k is a function induced by the function F on $\mathbb{Z}/p^k$, i.e.,

$$F_k(x_1, \ldots, x_n) = (\phi_k(f_1(x_1, \ldots, x_n)), \ldots, \phi_k(f_m(x_1, \ldots, x_n)))$$

for all $x_1, \ldots, x_n \in \mathbb{Z}/p^k$. In particular, if $m = n$, then F preserves measure if and only if every function $F_k\colon (\mathbb{Z}/p^k)^{(n)} \to (\mathbb{Z}/p^k)^{(n)}$ is bijective. Finally, F is ergodic if and only if every function F_k is transitive. In the remaining part of the article, we shall state that *F is bijective* (*transitive*) *modulo* p^k if F_k is bijective (transitive) on $\mathbb{Z}/p^k$. The criterion of ergodicity of a linear polynomial over a residue ring, mentioned in the introduction, provides an important example of an ergodic function on $\mathbb{Z}_p$.

0.1.7. Theorem ([8, Chapter 3, Theorem A]). *The function $f(x) = m + nx$ with rational integer coefficients m, n is transitive on $\mathbb{Z}/p^k$ if and only if m and p are coprime and either $n \equiv 1 \pmod p$ or $p = 2$, $k > 1$, and $n \equiv 1 \pmod 4$.*

It immediately follows from this criterion that the function $f(x) = m + nx$ with the p-adic integer coefficients m, n is ergodic if and only if it is ergodic modulo p for an odd prime p or modulo 4 for $p = 2$, i.e., these conditions are sufficient and necessary for the sequence $\{f^n(a)\}_{n=0}^{\infty}$ to be uniformly distributed over $\mathbb{Z}_p$ (here a is an arbitrary p-adic integer).

Theorem 0.1.7 was used to construct linear congruent pseudorandom generators with a maximal period length (see [8]). The results presented below, together with 0.1.5, can also be used to construct new (no longer linear) congruent generators with a maximal period length modulo arbitrary $n \in \mathbb{N}$. For possible cryptographic applications of the latter, see [5], where it is pointed out, in particular, that even truncated

linear congruent generators (whose output sequences consist only of higher-order digits) are cryptographically unsecure, whereas the methods of decoding nonlinear truncated congruent generators are not known.

Chapter 1

POLYNOMIALS OVER COMMUTATIVE GROUPS WITH MULTIOPERATORS

Everywhere in this chapter, we consider the case where the group A with multioperators is commutative (Abelian), imposing particular constraints on the set of multioperators. One of the most important special cases consists in the fact that all multioperators are operators, i.e., unitary operations acting as endomorphisms relative to the commutative group operation.

1.1. Polynomials over Abelian Groups with Operations

Suppose that G is an additive Abelian group with the set Ω of operators (possibly, empty). We denote the result of the action of the operator $\omega \in \Omega$ on the element $g \in G$ by ωg. Then any polynomial $w(x)$ in the variable x over G can be written as

$$w(x) = a + (n_1\omega_1 + \ldots + n_s\omega_s)x,$$

where $a \in G$, $\omega_1, \ldots, \omega_s \in \Omega$, $n_1, \ldots, n_s \in \mathbb{Z}$. Since the linear combination $n_1\omega_1 + \ldots + n_s\omega_s$ acts on G as the endomorphism ε, any polynomial function over the group G can be represented as $a + \varepsilon x$.

Let the group G be finite. Then the polynomial $w(x)$ is obviously bijective if and only if the operator $n_1\omega_1 + \ldots + n_s\omega_s$ is nonsingular, i.e., induces the automorphism of the group G. We have thus completely described the measure-preserving polynomial functions in one variable over the arbitrary finite Abelian group G with operators. As to polynomial ergodic functions in one variable, they exist far from over every group.

1.1.1. Theorem ([5]). *The finite Abelian group G with a set of operators Ω admits of a polynomial ergodic function if and only if it belongs to one of the following types:*

(i) *a cyclic group with an arbitrary set of operators,*

(ii) *an elementary Abelian group of type* (2.2) (*a direct product of two cyclic groups of order* 2, *i.e., the Klein group K_4*), *with a certain operator from Ω inducing an involution on G,*

(iii) *a direct product of a group of type* (ii) *by a group of type* (i) *of an odd order.*

Ergodic polynomial functions in one variable over groups of type (i) are completely characterized by Theorem 0.1.7, together with 0.1.5, since a finite cyclic group is isomorphic to an additive group of a suitable residue class ring, the action of the operator consisting in the multiplication by a certain number. In other words, if the cyclic group G of order s with some set of operators is identified with an additive group of the ring $\mathbb{Z}/s$, then any polynomial function $f(x)$ over it can be represented as $f(x) = m + nx$, where m and n are rational integers, and the transitivity criterion consists in the fact that m and s are coprime, $n \equiv 1 \pmod{p}$ for every prime p that divides s, and if $4 \mid s$, then, additionally, $n \equiv 1 \pmod{4}$.

Ergodic polynomial functions in one variable over groups of type (ii) are completely described by the following theorem.

1.1.2. Theorem ([5]). *The polynomial function $a + \varepsilon x$ over the Klein group K_4 is ergodic if and only if ε is an involution in the group of automorphisms of the Klein group* (*i.e., ε^2 is an identity mapping*), *and $\varepsilon a \neq a$.*

Theorems 1.1.1 and 1.1.2, together with Proposition 0.1.5, describe in an obvious way ergodic functions in one variable over groups of type (iii).

As to polynomial functions in several variables over the group G, this case can be reduced to functions in one variable over the direct power of the group G. Indeed, any polynomial function $F\colon G^{(n)} \to G^{(m)}$ can be represented as

$$F(x_1, \ldots, x_n) = (a_1 + \varepsilon_{11}x_1 + \ldots + \varepsilon_{1n}x_n, \ldots, a_m + \varepsilon_{m1}x_1 + \ldots + \varepsilon_{mn}x_n),$$

or, in matrix form, as

$$F(x_1, \ldots, x_n) = (a_1, \ldots, a_n) + (x_1, \ldots, x_n) \begin{pmatrix} \varepsilon_{11} & \ldots & \varepsilon_{m1} \\ \ldots & \ldots & \ldots \\ \varepsilon_{1n} & \ldots & \varepsilon_{mn} \end{pmatrix},$$

where $a_1, \ldots, a_n \in G$, ε_{ij} are endomorphisms of the group G, $i = 1, \ldots, m$, $j = 1, \ldots, n$. We can regard the matrix appearing on the right-hand side as an endomorphism of the Abelian group $G^{(n)}$, and therefore we can regard the function F as a function in one variable on the group $G^{(n)}$ and apply the above-mentioned theorems.

Functions of the form $x \mapsto a + \varepsilon x$ on the Abelian group G, where ε is some endomorphism, are also called *affine transformations* of the group G. Ergodic transformations of infinite Abelian groups were studied by a number of authors. The corresponding results and literature are given in [5]. With this remark, we finish the consideration of polynomial functions on Abelian groups with operators and pass to another important special case of commutative groups with multioperators, namely, commutative rings.

1.2. Polynomial Functions on Commutative Rings

Just as in the preceding section, we shall begin with finite rings. Everywhere below, R is a finite associative and commutative ring. The existence of an identity in R is not presupposed, but if it is present, then it is denoted by e or 1. It immediately follows from the general definition of a polynomial over a universal algebra that the polynomial $f(x_1, \ldots, x_n)$ in the variables $x_1, \ldots, x_n$ over the ring R has the canonical representation

$$\begin{cases} \sum\limits_{(i_1,\ldots,i_n)} r_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n} + \sum\limits_{(j_1,\ldots,j_n)} s_{j_1,\ldots,j_n} x_1^{j_1} \cdots x_n^{j_n}, \\ \sum\limits_{(i_1,\ldots,i_n)} r_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}, \end{cases}$$

where $(i_1, \ldots, i_n) \in \mathbb{N}_0^{(n)}$, $(j_1, \ldots, j_n) \in \mathbb{N}^{(n)}$, $s_{j_1,\ldots,j_n} \in \mathbb{Z}$, $r_{i_1,\ldots,i_n} \in R$, with almost all $s_{j_1,\ldots,j_n}$, $r_{i_1,\ldots,i_n}$ being 0, $\mathbb{N}$ is the set of all positive rational integers, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For $i_k = 0$, the variable x_k in the monomial $x_1^{i_1} \ldots x_n^{i_n}$ is absent and, by definition, $r_{0,\ldots,0} x_1^0 \ldots x_n^0 = r_{0,\ldots,0} = r_0$.

It is known (see [23]) that a finite associative and commutative ring decomposes into a direct sum of rings of pairwise coprime primary orders and every direct summand is either a local ring (i.e., a ring with a single maximal ideal, not coincident with the whole ring) or a nilpotent ring (i.e., a ring a certain power of which is zero). Consequently, by virtue of Proposition 0.1.5, the study of equiprobable, measure-preserving, and ergodic polynomial functions on R reduces to the case where R is of a primary order and is either local or nilpotent. If R is a field, then we can consider the problem of describing functions of this kind to be solved, since in this case any $R^{(n)} \to R$ function can be defined by a suitable polynomial whose explicit form can be found with the aid of the interpolation formula of Newton or Lagrange. Therefore, we assume in the sequel that R is not a field.

We shall also need the concept of the *derivative* of the polynomial with respect to some variable which need not be recalled for the case of a polynomial over a ring with identity. Now if R is a nilpotent ring and $f(x_1, \ldots, x_n)$ is a polynomial over it, represented in the canonical form given above, then, by definition, we

set its derivative $\frac{\partial}{\partial x_i} f(x_1, \dots, x_n)$ with respect to the variable x_i equal to $s_{0,\dots,0,1,0,\dots,0}$, where 1 in the subscript occupies the ith position. The *Jacobi matrix* and the *Jacobian* of the polynomial map $F = (f_1, \dots, f_n)\colon R^{(n)} \to R^{(m)}$ can now be defined in the standard way.

We denote by $J(R)$ the Jacobson radical (i.e., the maximal ideal) of the local ring R and by $\overline{R} = R/J(R)$ the residue field of the ring R. For the nilpotent ring R we denote by $\operatorname{Ann}(R) = \{r \in R\colon rR = 0\}$ its annihilator.

The following proposition is valid.

1.2.1. Proposition. *Suppose that R is a local ring and $J(R) \neq 0$.*

1. *The polynomial function $F\colon R^{(n)} \to R^{(m)}$, where $m \leq n$, is equiprobable if it is equiprobable on $\overline{R}^{(n)}$ (i.e., equiprobable modulo $J(R)$) and the rank of its Jacobi matrix modulo $J(R)$ is equal to m at every point from $\overline{R}^{(n)}$.*

2. *For $m = n$, the function F given above is bijective (i.e., preserves measure) on $R^{(n)}$ if and only if it is bijective on $\overline{R}^{(n)}$ and its Jacobian does not turn into zero at any point from $\overline{R}^{(n)}$ (equivalently: if and only if it is bijective on $(R/J(R)^2)^{(n)}$).*

The proof of this proposition can actually be found in [2, Chapter 4, Propositions 4.31 and 4.34]. When we compare statements 1 and 2, a natural conjecture suggests itself that the sufficient conditions of the equiprobability of the function F are also necessary conditions. Unfortunately, this conjecture is not correct in the general case; the corresponding counterexample can be found in [18], where the polynomial $f(x, y) \in \mathbb{Z}[x, y]$ is constructed which is equiprobable modulo p^n (p is a prime number) for every $n > 1$ and is such that for any polynomial $g(x, y) \in \mathbb{Z}[x, y]$ the map $\phi\colon (a, b) \mapsto (f(a, b), g(a, b))$ is not bijective modulo p^n for any $n > 1$. We can show, however, that if our conjecture is correct, then, for any equiprobable polynomial f, there exists a polynomial g such that the corresponding map ϕ is bijective. Thus, the sufficient conditions of equiprobability formulated in Sec. 1.2.1 are not, generally speaking, necessary, at least for residue rings. As to the case of nilpotent rings, here we can obtain a criterion of equiprobability of polynomial functions.

1.2.2. Proposition. *Suppose that R is a nilpotent ring of order p^k and p is a prime number. The function $F = (f_1, \dots, f_m)\colon R^{(n)} \to R^{(m)}$ with $m \leq n$ is equiprobable if and only if the rank of its Jacobi matrix modulo p is equal to m (equivalently: if and only if F is equiprobable modulo R^2).*

It is easy to carry out the proof of this proposition by induction on k and use the fact that modulo R^2 the function F acts as the affine transformation $h \mapsto hF' + r_0$, where F' is a Jacobi matrix of the transformation of F.

Before describing ergodic polynomial transformations of finite associative and commutative rings, we must first find out what rings admit of these transformations. The following theorem holds true.

1.2.3. Theorem. *The ring R admits of an n-dimensional polynomial ergodic transformation (i.e., there exist polynomials $f_1, \dots, f_n \in R[x_1, \dots, x_n]$ such that the transformation $F = (f_1, \dots, f_n)\colon R^{(n)} \to R^{(n)}$ is ergodic) if and only if one of the following cases is valid:*

(a) *$n > 2$ and R is a direct sum of finite fields with pairwise coprime characteristics,*

(b) *$n = 2$ and R is a direct sum of rings of pairwise coprime orders, and every direct summand is either a finite field or is isomorphic to one of the following rings:*

$$\mathbb{Z}/4, \quad \mathrm{GF}(2)[\xi]/(\xi^2), \quad \xi\,\mathrm{GF}(2)[\xi]/(\xi^2);$$

(c) *$n = 1$ and R is the direct sum of rings of pairwise coprime orders, every direct summand being isomorphic to one of the following rings:*

(1) *a finite field;*

(2) *$\mathbb{Z}/p^m$, p is a prime number, $m \in \mathbb{N}$;*

(3) *$\mathrm{GF}(p)[\xi]/(\xi^2)$, p is a prime number;*

(4) *$\mathrm{GF}(p)[\xi]/(\xi^3)$, $p = 2$ or $p = 3$;*

(5) *$\mathbb{Z}/p^2[\xi]/(\xi^3, \xi^2 - p e)$, $p = 2$ or $p = 3$;*

(6) $\mathbb{Z}/9[\xi]/(\xi^3, \xi^2 + 3e)$;

(7) $p^k\mathbb{Z}/p^{k+m} \subset \mathbb{Z}/p^{k+m}$, *p is a prime number,* $k, m \in \mathbb{N}$;

(8) $\xi\,\mathrm{GF}\,(p)[\xi]/(\xi^3)$, $p = 2$ *or* $p = 3$.

The proof of this theorem for case (c) under the condition that R is a ring with unity was published in [2]. I hope to publish the proof for the other cases in the near future.

The next problem is the description of ergodic (transitive) polynomials over each of the rings enumerated in the formulated theorem. In order to get this description, we shall have to do the same in each case, which we shall first illustrate using an example of finite fields.

Thus, suppose that $R = \mathrm{GF}\,(q)$ is a finite field of q elements. Then any transformation $\tau\colon \mathrm{GF}\,(q) \to \mathrm{GF}\,(q)$ can be uniquely defined by means of the polynomial $f_\tau(x)$, whose power does not exceed $q - 1$ and whose explicit form can be found from Newton's or Lagrange's formulas. We call the polynomial $f_\tau(x)$ an *interpolation polynomial of the transformation* τ. It is well known that the polynomial $g(x) \in \mathrm{GF}\,(q)[x]$ vanishes at all points from $\mathrm{GF}\,(q)$ if and only if $x^q - x \mid g(x)$. In other words, the ideal $I_{\mathrm{GF}\,(q)}[x]$ of all mixed identities of the variable x is generated by the polynomial $x^q - x$. Summing up what we have said, we get the following description of ergodic polynomials in one variable over $\mathrm{GF}\,(q)$: the polynomial $f(x) \in \mathrm{GF}\,(q)[x]$ is transitive on $\mathrm{GF}\,(q)[x]$ if and only if it has the form $f(x) = f_\tau(x)+(x^q-x)h(x)$, where $f_\tau(x)$ is an interpolation polynomial of the transformation τ transitive on $\mathrm{GF}\,(q)$ and $h(x)$ is an arbitrary polynomial over $\mathrm{GF}\,(q)$.

Note that the description given above was obtained on the basis of solutions of the following three problems:

first, all ergodic functions on R were described (in this case exactly the functions which define on R the substitution τ which is a cycle of length q),

second, the polynomical representation was found for each of these functions (i.e., its interpolational polynomial $f_\tau(x)$),

third, all mixed identities of the ring R were described.

This is the general scheme of the description of all polynomials which represent the class $\mathcal{F}$ of functions on the group A with multioperators. First, we construct an *interpolation algorithm* which associates every function $\phi \in \mathcal{F}$ with a single polynomial f_ϕ over A that defines ϕ, i.e., we associate the functions ϕ of the representative f_ϕ of the coset $f_\phi + I_A$ with respect to the subgroup I_A of the mixed identities of the universal algebra A. All polynomials from $f_\phi + I_A$ and only they define the same function ϕ, and therefore, having described I_A, i.e., all mixed identities of the universal algebra A, we complete the description of all polynomials which define the functions from $\mathcal{F}$. This procedure (known as an *interpolation procedure*) was used to describe ergodic, equiprobable, measure-preserving polynomials, and in this way all transitive polynomials over each of the rings enumerated in Theorem 1.2.3 were described. However, in this work we shall only consider some of them, which, to my mind, are of special interest for pure mathematics and for its applications. Since it is usually required in applications that a recurrent sequence, generated by an ergodic polynomial, have a long period (otherwise, it is difficult to consider its elements to be "random" in any sense), we immediately exclude from consideration rings of "small" orders, i.e., rings of the types $c4$–$c6$ and $c8$, as well as rings of the b type which are not fields. In addition, since, by virtue of Proposition 0.1.5, the description of ergodic polynomials over direct sums of rings of pairwise coprime orders obviously reduces to the description of ergodic polynomials on each direct summand, it is expedient to exclude from further consideration rings of nonprimary orders as well. Thus, only finite fields, residue class of rings, and $c3$ and $c7$ rings remain.

Formally, we can consider the problem of the description of ergodic polynomials over finite fields to be already solved (see the characterization of these polynomials in one variable given above). However, this is hardly sufficient for applications since, when we construct an ergodic polynomial over a field of q elements, say, with the use of Newton or Lagrange interpolation formula, we have to compute q coefficients of the interpolation polynomial, and this is, as a rule, impractical since it is required in applications that the period of the corresponding sequence and, hence, the number q be of utmost importance. For instance, in cryptography this boundary is of order 10^{20} and higher (to resist " a brute force attack"). In other words, q must be large enough for the time spent on this exhaustive search to be beyond all reasonable bounds. But

then the time spent on the construction (with the use of Newton or Lagrange interpolation procedure) of an ergodic polynomial will be beyond the practical bounds. It stands to reason that we can pose the problem of describing low-degree polynomials ergodic over a finite field (or, at least, polynomials which have a small number of nonzero monomials). However, I do not know of any essential results obtained in this direction.

Similar arguments can be used in the consideration of rings of R type $c3$ which are of order p^2 and are, consequently, large enough only when p is sufficiently large. Since the description of ergodic polynomials on such a ring R immediately implies the description of ergodic polynomials over a field of p elements (by means of the reduction of the corresponding polynomials modulo the Jacobson radical), all that we have said above about the possibility of using ergodic polynomials over finite fields for constructing program generators of random numbers also refers to the case under study.

Finally, the problem of describing ergodic polynomials over rings of the $c7$ type (they are nilpotent rings isomorphic to the ideals of rings of the $c2$ type) proves to be reducible to a similar problem for rings of the $c2$ type. Indeed, if $R = p^k\mathbb{Z}/p^{k+m}$, $k \geq 1$, $m \geq 1$, and $f(x) \in R[x]$, then $f(x)$ can be represented in the form $f(x) = r(x) + u(x)$, where $r(x)$ is a polynomial all of whose coefficients lie in R and $u(x)$ is a polynomial with rational integer coefficients and without a constant term (see the canonical representation of polynomials over rings without an identity at the beginning of this section). Since any element of the ring R can be represented as rp^k, where $r \in \mathbb{Z}$, the polynomial $r(x)$ admits of the representation

$$r(x) = r_0p^k + r_1p^kx + \ldots,$$

where $r_i \in \mathbb{Z}$, $i = 0, 1, 2, \ldots$. We represent the polynomial $u(x)$ in the form

$$u(x) = u_1x + u_2x^2 + \ldots,$$

where $u_i \in \mathbb{Z}$, $i = 1, 2, 3, \ldots$. Substituting now $x = p^kz$ into the expression for $f(x)$, we find that $f(x) = f(p^kz) = p^kg(z)$, where

$$g(z) = r_0 + (r_1p^k + u_1)z + (r_2p^{2k} + u_2p^k)z^2 + \ldots + (r_ip^{ik} + u_ip^{(i-1)k})z^i + \ldots.$$

It follows immediately that $f(p^kg^n(z)) = p^kg^{n+1}(z)$ (recall that $f^n(x) = f(f^{n-1}(x))$, $f^0(x) = x$), and simple induction on n shows that $f^n(x) = p^kg^n(z)$ for all $n = 1, 2, \ldots$, which means that the polynomial $f(x)$ is ergodic on R if and only if the polynomial $g(z)$, being a polynomial with rational integer coefficients, is transitive modulo p^m.

The arguments we have used make it possible to leave for further consideration a single type of rings, namely, residue class ring modulo some power of prime integer. We shall obtain the description of ergodic polynomials over such rings as a very special case from the solution of the general problem of describing ergodic functions of the space of p-adic integers, to which the next section of this work is devoted.

1.3. p-Adic Functions

Unless otherwise specified, the proofs of the results considered in this section can be found in [1, 14].

Compatible functions and interpolation series. We begin by studying the functions which are compatible with all congruences of the ring $\mathbb{Z}_p$, or compatible functions. As was shown in Sec. 0.1, this class consists of exactly all functions that satisfy the p-adic Lipschitz condition with coefficient 1, and it contains, in particular, all functions polynomial on $\mathbb{Z}_p$. This class is of particular importance for applications. For instance, of all the 2-adic extensions of standard commands of a processor which were mentioned in the introduction (addition and multiplication of binary representations of integers, reduction modulo 2^n, addition and multiplication modulo 2^n, XOR, OR, AND, which are the bit-by-bit logical operations "exceptional or," "or," and "and" respectively, SHR and SHL, which are shifts by one position to the higher or lower orders, masking) only the

extension of the SHL operation is *not* compatible. Hence, all 2-adic extensions of the superpositions of these operations (except for SHL) are compatible with all congruences of the ring $\mathbb{Z}_2$.

In this section, we shall also demonstrate techniques which we use to characterize the measure-preserving and ergodic functions in the class of all compatible functions for $p = 2$. In addition, we suggest a method which can be used for solving similar problems in the class of polynomial functions over universal algebras of the form $\langle \mathbb{Z}_2, \Omega \rangle$, where Ω is any set of compatible functions.

Let $f\colon \mathbb{N}_0 \to \mathbb{Z}_p$ be an arbitrary function, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. It is known (see [22]) that f admits of one and only one representation in the form of the series

$$f(x) = \sum_{i=0}^{\infty} a_i \binom{x}{i},$$

where $\binom{x}{i} = \frac{x(x-1)\dots(x-i+1)}{i!}$ for $i = 1, 2, \dots$, $\binom{x}{0} = 1$, $a_i \in \mathbb{Z}_p$ $(i = 0, 1, 2, \dots)$. This series is known as an *interpolation series of the function* f. The following relation connects the coefficients a_i and the values of the function f:

$$a_i = \sum_{j=0}^{i} (-1)^{n+j} \binom{n}{j} f(j) = \Delta^i f(0),$$

where $\Delta f(x) = f(x+1) - f(x)$, $\Delta^s f = \Delta^{s-1}(\Delta f)$ $(s = 1, 2, \dots)$, $\Delta^0 f = f$.

If f is uniformly continuous on $\mathbb{N}_0$ relative to the p-adic metric, then it admits of a unique continuation to the uniformly continuous function on $\mathbb{Z}_p$. In this case, the corresponding interpolation series converges on $\mathbb{Z}_p$ uniformly. The following statement is valid: the series

$$f(x) = \sum_{i=0}^{\infty} a_i \binom{x}{i} \qquad (a_i \in \mathbb{Q}_p, \quad i = 0, 1, 2, \dots) \tag{$*$}$$

converges on $\mathbb{Z}_p$ uniformly if and only if the p-adic limit of its ith coefficient exists and is equal to zero, i.e., $\lim\limits_{i \to \infty}^{p} a_i = 0$. In this case, the interpolation series defines the uniformly continuous function on $\mathbb{Z}_p$.

By analogy we introduce interpolation series in several variables:

$$f(x_1, \dots, x_n) = \sum_{i} a_i \binom{x_1}{i_1} \binom{x_2}{i_2} \dots \binom{x_n}{i_n},$$

where $a_{i_1,\dots,i_n} \in \mathbb{Z}_p$, $i = (i_1, \dots, i_n)$ runs through $\mathbb{N}_0^{(n)}$. Every function $f(x_1, \dots, x_n)\colon \mathbb{N}_0^{(n)} \to \mathbb{Z}_p$ admits of such a representation, and this representation is unique. It is uniformly continuous if and only if $\|a_{i_1,\dots,i_n}\|_p \to 0$ as $i_1 + \dots + i_n \to 0$.

Thus, everywhere in this section

$$f(x)\colon \mathbb{Z}_p \to \mathbb{Z}_p, \qquad f(x_1, \dots, x_n)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p$$

are uniformly continuous on $\mathbb{Z}_p$ functions which are represented by the corresponding interpolation series. The interpolation series proved to be a convenient tool for describing some important properties of uniformly continuous functions. The first property can be formulated as follows.

1.3.1. Definition. The function $F = (f_1, \dots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ is called an *identity modulo* p^k if the congruence

$$F(u) \equiv (0, \dots, 0) \pmod{p^k}$$

is satisfied for every $u \in \mathbb{Z}_p^{(n)}$.

Identities modulo p^k are needed for describing various properties of compatible functions since two functions of this kind obviously coincide modulo p^k if and only if their difference is an identity modulo p^k.

1.3.2. Proposition. *The function $f(x_1,\dots,x_n)$ is an identity modulo p^k if and only if $\|a_{i_1,\dots,i_n}\|_p \le p^{-k}$ for all $(i_1,\dots,i_n) \in \mathbb{N}_0^{(n)}$.*

Let us now use the language of interpolation series to characterize compatible functions. Recall that $[\alpha]$ for real α denotes the rational integer closest to α but not exceeding α.

1.3.3. Theorem. *The function $f(x_1,\dots,x_n)$ is compatible if and only if*

$$\|a_{i_1,\dots,i_n}\|_p \le p^{-\mu(i_1,\dots,i_n)},$$

where

$$\mu(i_1,\dots,i_n) = \begin{cases} 0 & \text{if } i_1 = i_2 = \dots = i_n = 0; \\ \max\{[\log_p i_k] \colon i_k \ne 0,\ k = 1,2,\dots,n\} & \text{otherwise.} \end{cases}$$

In particular, the function $f(x)\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is compatible if and only if

$$\|a_i\|_p \le p^{-[\log_p i]}$$

for all $i = 1,2,\dots$.

Recall that the polynomial $f(x) \in \mathbb{Q}[x]$ ($f(x) \in \mathbb{Q}_p[x]$, resp.) is *integer-valued* if the function it defines is *integer-valued*, i.e., $f(\mathbb{Z}_p) \subseteq \mathbb{Z}_p$ ($f(\mathbb{Z}) \subseteq \mathbb{Z}$, resp.).

1.3.4. Corollary (cf. [16]). *The integer-valued polynomial $f(x) \in \mathbb{Q}[x]$ is compatible with all congruences on $\mathbb{Z}$ (i.e., for any $m \in \mathbb{N} \setminus \{1\}$, $a, b \in \mathbb{Z}$, the congruence $a \equiv b \pmod m$ implies the congruence $f(a) \equiv f(b) \pmod m$) if and only if it can be represented as*

$$f(x) = a_0 + \sum_{i=1}^{d} a_i \operatorname{LCM}(1,2,\dots,i) \binom{x}{i},$$

where $\operatorname{LCM}(k,l,m,\dots)$ is the least common multiple of the numbers $k,l,m,\dots \in \mathbb{N}$.

The proof follows immediately from Theorem 1.3.3 since the function of a rational integer argument is obviously compatible in the sense specified in the hypothesis of the corollary if and only if it is compatible as a function of an integer p-adic argument for every prime p and $p^{[\log_p i]}$ is the highest power of p not exceeding i.

Let us now characterize all measure-preserving or ergodic functions in the class of all compatible functions for $p = 2$. Everywhere in this subsection, $p = 2$. Recall that, as was stated in Sec. 0.1, a compatible function preserves measure (is ergodic, resp.) if and only if it is bijective (transitive, resp.) every modulo 2^k for $k = 1,2,\dots$, i.e., induces a substitution on $\mathbb{Z}/2^k$ (a substitution which is a cycle of length 2^k, resp.).

1.3.5. Theorem. *The function $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$, represented as the series*

$$f(x) = \sum_{i=0}^{\infty} a_i \binom{x}{i},$$

is compatible and preserves measure if and only if

$$\|a_1\|_2 = 1, \qquad \|a_i\|_2 \le 2^{-[\log_2 t]-1}, \quad i = 2,3,\dots.$$

It is compatible and ergodic if and only if

$$\begin{gathered} a_0 \equiv 1 \pmod 2; \\ a_1 \equiv 1 \pmod 4; \\ a_i \equiv 0 \pmod{2^{[\log_2(i+1)]+1}}, \qquad i = 2,3,\dots. \end{gathered}$$

These theorems yield a number of important corollaries. The first corollary concerns integer-valued polynomials over the field of 2-adic numbers $\mathbb{Q}_2$.

1.3.6. Corollary. *If $f(x)$ is an integer-valued compatible polynomial over $\mathbb{Q}_2$, then there exists a rational integer $c = c(f)$ ($r(f)$, resp.) such that the polynomial f preserves measure (is ergodic, resp.) if and only if*

it is bijective modulo $2^{c(f)}$ *(is transitive modulo* $2^{r(f)}$*, resp.). Moreover, there exists an efficient procedure of computing these quantities* $c(f)$ *and* $r(f)$ *for each polynomial* f *of this kind. Finally, if* f *is a polynomial over* $\mathbb{Z}$ *or* $\mathbb{Z}_p$*, then we can take* $c(f) = 2$ $(r(f) = 3$*, resp.).*

By virtue of this corollary, in order to find out whether a given polynomial is ergodic (or preserves measure), we must study the behavior of the corresponding function modulo 2^k, i.e., the criterion does not directly depend on the coefficients of the given polynomial. However, if we represent the polynomial in a different basis, this relationship becomes explicit, namely, let us represent $f \in \mathbb{Z}_2[x]$ in the basis

$$\{x^{(0)} = 1,\ x^{(i)} = x(x-1)\dots(x-i+1)\colon\ i = 1, 2, \dots\},$$

i.e.,

$$f = \sum_{i=0}^{d} c_i x^{(i)} \qquad (c_i \in \mathbb{Z}_2;\ \ i = 0, 1, 2, \dots).$$

Then the following corollary is valid.

1.3.7. Corollary. *The polynomial* f *presented above preserves measure if and only if the following three congruences are simultaneously valid:*

$$c_1 \equiv 1 \pmod 2, \qquad c_2 \equiv 0 \pmod 2, \qquad c_3 \equiv 0 \pmod 2.$$

The polynomial f *is ergodic if and only if the following four congruences are simultaneously valid*:

$$c_0 \equiv 1 \pmod 2, \qquad c_1 \equiv 1 \pmod 4, \qquad c_2 \equiv 0 \pmod 2, \qquad c_3 \equiv 0 \pmod 4.$$

M. V. Larin was the first to give a complete description (but using a different terminology) of polynomials over $\mathbb{Z}$, transitive modulo p^k, for all prime p and all $k \in \mathbb{N}$. His method was different from that used in this work and did not use the p-adic technique. (Some examples of non-linear ergodic modulo 2^k polynomials due to R.R.Coveyou were mentioned in [8], as well as the conditions for the polynomial of degree 2 with integral coefficient to be ergodic modulo some m - *the text in brackets was added by V.S.Anashin to the text of the original paper after its publication*)

The theorems proved above can also be used for describing all compatible and measure-preserving or ergodic polynomials over the universal algebras A of the form $\langle \mathbb{Z}_2, \Omega \rangle$. The idea is to represent all operations from Ω in the form of interpolation series and then, using these representations, calculate the coefficients $a_i(f)$ of the interpolation series of the specific polynomial f over A as compositions of interpolation series which are operations from Ω. The coefficients $a_i(f)$ are functions of the coefficients of f. Therefore, by virtue of Theorems 1.3.3 and 1.3.5, the polynomial f is compatible, preserves measure, or is ergodic, if and only if all coefficients $a_i(f)$ satisfy the congruences described in the corresponding theorems. Solving the congruence systems obtained in this way, we find the necessary and sufficient conditions which must be satisfied by the coefficients of the polynomials f for this polynomial to be compatible, ergodic, or measure preserving. It stands to reason that not only the solutions of the corresponding systems of congruences but also the finding of the systems themselves in explicit form may turn out to be difficult. Nevertheless, the method works, and below we give some respective examples.

Let us consider certain polynomials over the universal algebra $\langle \mathbb{Z}_2, \{+, \cdot, \mathrm{XOR}, \delta_0, \delta_1, \delta_2, \dots\} \rangle$, which can also be of interest for programming since they have been constructed with the aid of the "computer" operations XOR, $\delta_0, \delta_1, \delta_2, \dots$ defined in Sec. 0.1.

1.3.8. Proposition. 1°. *The function* $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ *of the form*

$$f(x) = a + \sum_{i=1}^{n} a_i (x \,\mathrm{XOR}\, b_i),$$

where $a, a_i, b_i \in \mathbb{Z}_2$*,* $i = 1, 2, 3, \dots$*, preserves measure (is ergodic, resp.) if and only if it is bijective (transitive, resp.) modulo* 2 *(modulo* 4*, resp.).*

2°. *The function* $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ *of the form*

$$f(x) = a + \sum_{i=0}^{\infty} a_i \delta_i(x),$$

where $a, a_i \in \mathbb{Z}_2$, $i = 0, 1, 2, \ldots$, *is compatible and ergodic if and only if the following conditions are simultaneously satisfied:*

$$a \equiv 1 \pmod 2;$$
$$a_0 \equiv 1 \pmod 4;$$
$$\|a_i\|_2 = 2^{-i}, \qquad i = 1, 2, 3, \ldots.$$

It is compatible and measure-preserving if and only if

$$\|a_i\|_2 = 2^{-i}, \qquad i = 0, 1, 2, 3, \ldots.$$

Uniform differentiability modulo p^k. The method of constructing compatible, measure-preserving or ergodic functions as polynomials over algebraic systems of the form $A = \langle \mathbb{Z}_2, \Omega \rangle$, which was described above, is universal in the sense that, formally speaking, it is applicable to an arbitrary number of operations Ω. However, as was already mentioned, in special cases its use may be a difficult problem connected with the finding of explicit expressions for the coefficients $a_i(f)$ or with the solution of the corresponding system of congruences. Therefore, we shall demonstrate in the sequel a different method, which also allows us to describe the indicated functions. This method is no longer universal but can only be applied to functions which are close, in some sense, to uniformly differentiable functions. However, it also works in the case where p is an odd prime number and its application makes it possible to obtain statements of the type of 1.3.6 or 1.3.8(1°) simultaneously for all polynomials over the universal algebra A.

1.3.9. Definition. We say that the function $F = (f_1, \ldots, f_n)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ *is differentiable modulo* p^k *at the point* $u = (u_1, \ldots, u_n) \in \mathbb{Z}_p^{(n)}$ if there are a positive rational integer N and a matrix $F'_k(u)$ over $\mathbb{Q}_p$ of size $n \times m$ (which is known as the *Jacobi matrix modulo* p^k *of the function* F *at the point* u) such that for every positive rational integer $K \geq N$ and every $h = (h_1, \ldots, h_n) \in \mathbb{Z}_p^{(n)}$ from the system of inequalities $\|h_i\|_p \leq p^{-K}$ $(i = 1, 2, \ldots, n)$ it follows that

$$d_p^m(F(u + h), F(u) + hF'_k(u)) \leq p^{-k-K},$$

where d_p^m is a metric on $\mathbb{Q}_p^{(m)}$ induced by the metric d_p on $\mathbb{Q}_p$:

$$d_p^m(a, b) = \max\{d(a_i, b_i)\colon i = 1, 2, \ldots, m\}$$

for all $a = (a_1, \ldots, a_m)$, $b = (b_1, \ldots, b_m) \in \mathbb{Q}_p^{(m)}$. Recall that, by definition, $d(u, v) = \|u - v\|_p$ for all $u, v \in \mathbb{Q}_p$.

The inequality given in Definition 1.3.9 is equivalent to the fact that the function $F(u + h)$, being a function of the argument h, can be represented in the form

1.3.10. $$F(u + h) = F(u) + hF'_k(u) + \alpha(u, h)$$

if h is "sufficiently small," i.e., $\|h\|_p^n \leq p^{-K}$, where

1.3.11. $$\frac{\|\alpha(u, h)\|_p^n}{\|h\|_p^n} \leq p^{-k}.$$

Here the norm $\|v\|_p^s$ of the vector $(v_1, \ldots, v_s) \in \mathbb{Q}_p^{(s)}$ is defined as $\max\{\|v_i\|_p\colon i = 1, 2, \ldots, s\}$ and everywhere in the sequel will be denoted by the same symbol $\| \ \|_p$.

Finally, conditions 1.3.10 and 1.3.11 are equivalent to the condition

1.3.12. $$F(u + h) \equiv F(u) + hF'_k(u) \pmod{p^{k+K}}$$

when $\|h\|_p \le p^{-K}$. Here $a \equiv b \pmod{p^s}$ for $a = (a_1, \dots, a_r)$, $b = (b_1, \dots, b_r) \in \mathbb{Q}_p^{(r)}$ means that $\|a_i - b_i\|_p \le p^{-s}$ (or, what is the same, $a_i = b_i + c_i p^s$ for suitable $c_i \in \mathbb{Z}_p$) for all $i = 1, 2, \dots, s$. These elements a, b will be called *congruent modulo* p^k.

We have thus formulated three equivalent definitions of the differentiability of a function modulo p^k at a point. Since this concept is very important for the whole subsequent theory, we shall carry out a brief discussion.

First, note that Definition 1.3.10 could also be formulated for a function defined on an open subset $E \subseteq \mathbb{Q}_p^{(n)}$ and assuming values in $\mathbb{Q}_p^{(m)}$. However, we shall not need it since in the sequel we shall only study integer-valued functions on $\mathbb{Z}_p^{(n)}$, i.e., functions which map $\mathbb{Z}_p^{(n)}$ into $Z_p^{(m)}$.

Second, it pays to compare the concept that we have introduced with the classical definition of the differentiability of a function at a point. For the above-mentioned function F, the latter assumes the form 1.3.11 and condition 1.3.12 is replaced by the stronger condition

$$\lim_{n \to 0}^{p} \frac{\|\alpha(u,h)\|_p}{\|h\|_p} = 0,$$

where $\lim^p$ is a p-adic limit. This yields the following trivial proposition.

1.3.13. Proposition. *If the function $F = (f_1, \dots, f_m)\colon \mathbb{Q}_p^{(n)} \to \mathbb{Q}_p^{(m)}$ is differentiable at the point $u \in \mathbb{Q}_p^{(n)}$, then it is differentiable modulo p^k at this point for all $k = 1, 2, \dots$.*

Third, whereas the differentiability of the function $f\colon \mathbb{Q}_p \to \mathbb{Q}_p$ means that the ratio $\frac{f(u+h)f(u)}{h}$ can be approximated with any preassigned degree of accuracy by the value $f'(u)$, the differentiability modulo p^k only requires that this accuracy be not weaker than p^{-k}.

Let us consider the following important subclass in the class of functions differentiable modulo p^k.

1.3.14. Definition. We say that the function $F = (f_1, \dots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$, which is differentiable modulo p^k at all points $u \in \mathbb{Z}_p^{(n)}$, has *integer-valued derivatives modulo* p^k if the matrix $F_k'(u)$ is a matrix over $\mathbb{Z}_p$.

The concept we have introduced is similar to the concept of the so-called *twice integer-valued* function: the latter is defined as the function $F\colon \mathbb{Q}_p^{(n)} \to \mathbb{Q}_p^{(m)}$ such that $F(\mathbb{Z}_p^{(n)}) \subseteq \mathbb{Z}_p^{(m)}$, F is differentiable at all points from $\mathbb{Z}_p^{(n)}$, and $F'(\mathbb{Z}_p^{(n)}) \subseteq \mathbb{Z}_p^{(m)}$.

We can introduce, in the ordinary way, the concept of a function which is uniformly differentiable modulo p^k.

1.3.15. Definition. The function $F = (f_1, \dots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ is *uniformly differentiable modulo* p^k if there exists a positive rational integer N and a function F_k', defined on $\mathbb{Z}_p^{(n)}$ and assuming values in the space of all linear maps from $\mathbb{Z}_p^{(n)}$ into $\mathbb{Q}_p^{(m)}$ such that for all $u = (u_1, \dots, u_n)$ the inequality $\|h_i\|_p \le p^{-K} \le p^{-N}$ yields 1.3.12. For the given F, the smallest N that satisfies the above-mentioned condition is denoted by $N_k(F)$.

It follows from 1.3.9 that the (i,j)th entry d_{ij} of the matrix $F_k'(u)$ is congruent modulo p^k to the element

$$\frac{1}{h_j}(f_i(u_1, \dots, u_{j-1}, u_j + h_j, u_{j+1}, \dots, u_n) - f_i(u_1, \dots, u_n)),$$

where $h_j \in \mathbb{Z}_p \setminus \{0\}$, $\|h_j\|_p \le p^{-N}$, N is the same number as in 1.3.9. The element d_{ij} is called a *partial derivative modulo* p^k *of the function* f_i *with respect to the variable* x_j *at the point* $u = (u_1, \dots, u_n)$ and is denoted

$$d_{ij} = \frac{\partial_k f_i(u)}{\partial_k x_j}.$$

In the special case $m = 1$, the Jacobi matrix modulo p^k is called a *differential modulo* p^k *of the function* F, and if, in addition, $n = 1$, then it is called a *derivative modulo* p^k *of the function* F. If $m = n$, then the determinant $\det(F_k'(u))$ is the *Jacobian modulo* p^k *of the function* F *at the point* u. The Jacobian and the

partial derivative modulo p^k of a function at a point are defined with an accuracy to within the equivalence modulo p^k. They will be set equal to the least nonnegative residues of the corresponding numbers modulo p^k and can be regarded as elements of the residue class ring $\mathbb{Z}/p^k$. Thus, the Jacobian (partial derivative) modulo p^k of the function F, differentiable modulo p^k everywhere in $\mathbb{Z}_p^{(n)}$, is a map from $\mathbb{Z}_p^{(n)}$ into $\mathbb{Z}/p^k$.

"The laws of differentiation modulo p^k" are similar to the corresponding formulas of classical analysis, with the only difference that they are congruences modulo p^k and not equalities.

We shall now give several natural examples of functions which are uniformly differentiable modulo p^k. The operations of the field $\mathbb{Q}_p$, namely, addition and multiplication, are trivial since they are uniformly differentiable. The function $\delta_i(x)$, introduced in Sec. 0.1, serves as another example of a uniformly differentiable function. The derivative of this function is equal to 0 at all points of $\mathbb{Z}_p$: $\delta_i(x+h) = \delta_i(x)$ for sufficiently small h such that $\|h\|_p < p^{-i}$. Recall that, in the p-adic analysis, functions which are not constant and whose derivatives are 0 everywhere are called *pseudoconstants*.

The next example is a function which is no longer uniformly differentiable, but, nevertheless, is uniformly differentiable modulo p. Let us define on $\mathbb{Z}_p$ a new operation $\oplus_p$: $\delta_i(x \oplus_p y) \equiv \delta_i(x) + \delta_i(y) \pmod p$ for all $i = 0, 1, 2, \ldots$. Then, for every pair $u, v \in \mathbb{Z}_p$ such that $\|u\|_p, \|v\|_p \le p^{-k}$ we have $(x+u)\oplus_p(y+v) \equiv x\oplus_p y+u+v \pmod{p^{1+K}}$, where $K \in \mathbb{N} = \{1, 2, 3, \ldots\}$. This means that the function $F(x, y) = x \oplus_p y$ is uniformly differentiable modulo p and

$$\frac{\partial_1 F}{\partial_1 x} \equiv \frac{\partial_1 F}{\partial_1 y} \equiv 1 \pmod p$$

at all points from $\mathbb{Z}_p^{(2)}$. Note that for $p = 2$ this operation is already familiar to us: in this case F is the continuation of the operation (command) XOR to $\mathbb{Z}_2$.

Let us continue the study of functions that are differentiable modulo p^k. It immediately follows from Definition 1.3.9 that if a function is differentiable modulo p^k, then it is differentiable modulo $p^{k-1}, p^{k-2}, \ldots, p$. Therefore, we shall begin with functions differentiable modulo p. We shall need some new concepts.

1.3.16. Definition. The function $F = (f_1, \ldots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Q}_p^{(m)}$ is *asymptotically compatible* if there exists a nonnegative rational integer N such that for every $k \ge N$ the congruence $u \equiv v \pmod{p^k}$ implies $F(u) \equiv F(v) \pmod{p^k}$ for any $u, v \in \mathbb{Z}_p^{(n)}$.

In other words, asymptotically compatible functions are exactly those functions which satisfy the uniform Lipschitz condition

$$\|F(u) - F(v)\|_p \le \|u - v\|_p$$

for every pair (u, v) of points sufficiently close to one another, i.e., points such that $\|u - v\|_p \le p^{-N}$. Thus, asymptotically compatible functions are continuous and, hence, uniformly continuous on $\mathbb{Z}_p$.

1.3.17. Theorem. *If the function $F = (f_1, \ldots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ is uniformly differentiable modulo p and has integer-valued derivatives modulo p at all points from $\mathbb{Z}_p^{(n)}$, then it can be represented as*

$$F(x_1, \ldots, x_n) = P(x_1, \ldots, x_n) + C(x_1, \ldots, x_n),$$

where P is a periodic function with period $p^{N_1(F)}$ and C is a compatible function. Consequently, F is asymptotically compatible and C is uniformly differentiable modulo p. Asymptotically compatible functions are exactly those functions which are sums of a compatible function and a periodic function with period primary with respect to p.

The following proposition shows, in particular, that functions uniformly differentiable modulo p^k are "smooth modulo p^k."

1.3.18. Proposition. *If the function $F = (f_1, \ldots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ is uniformly differentiable modulo p^k, then every one of its partial derivatives is periodic with period $p^{N_k(F)}$.*

Thus, if the function $F = (f_1, \ldots, f_m)\colon \mathbb{N}_0^{(n)} \to \mathbb{N}_0^{(m)}$ can be continued to a function uniformly differentiable modulo p^k on $\mathbb{Z}_p^{(n)}$ (just as in the preceding examples), then it can be continued on $\mathbb{Z}_p^{(n)}$ together with all its

derivatives modulo p^k (and this continuation is unique) since the latter are completely defined by their values at a finite number of points. When necessary, Proposition 1.3.18 allows us to consider derivatives, Jacobi matrices, and Jacobians modulo p^k as functions on the residue ring $\mathbb{Z}/p^{N_k(F)}$.

These results show that the most interesting "component" of a function uniformly differentiable modulo p^k is compatible, and we shall continue to study compatible functions.

Obviously, the function $F = (f_1, \dots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ is compatible if and only if every function f_i, $i = 1, 2, \dots, m$, is compatible. Therefore, it suffices to study the functions $f(x_1, \dots, x_n)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p$.

For $i = 1, 2, \dots, n$, we set

$$\Delta_i f(x_1, \dots, x_n) = f(x_1, \dots, x_{i-1}, x_1 + 1, x_{i+1}, \dots, x_n) - f(x_1, \dots, x_n)$$

and then, by induction,

$$\Delta_i^s f = \Delta_i^{s-1}(\Delta_i f), \qquad s = 1, 2, \dots,$$

where, by definition, $\Delta_i^0 f = f$.

The following compatibility criterion is valid.

1.3.19. Proposition. *The continuous function $f\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p$ is compatible if and only if the values of each of the functions $\frac{1}{i}\Delta_j^i f$ $(j = 1, 2, \dots, n,\ i = 1, 2, \dots)$ at all points of $\mathbb{Z}_p^{(n)}$ are p-adic integers.*

1.3.20. Theorem. *The compatible function $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is differentiable modulo p at the point $u \in \mathbb{Z}_p$ if and only if there exists $N \in \mathbb{N}$ such that the congruence*

$$\frac{\Delta^i f(u)}{i} \equiv 0 \pmod{p}$$

is satisfied for all rational integers $i \geq N$. In this case

$$f_1'(u) \equiv \sum_{t=1}^{\infty} (-1)^{i-1} \frac{\Delta^i f(u)}{i} \equiv \sum_{t=0}^{\infty} \sum_{k=1}^{p-1} (-1)^{i-1} \frac{\Delta^{kp^t} f(u)}{kp^t} \pmod{p}.$$

1.3.21. Corollary. *If the compatible function $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is differentiable modulo p at the point $u \in \mathbb{Z}_p$, then $f_1'(u) \in \mathbb{Z}_p$.*

We can also characterize compatible functions in terms of the "values of digits," i.e., the functions $\delta_i(f(x_1, \dots, x_n))$.

1.3.22. Proposition. *The function $f\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p$ is compatible if and only if for every $i = 1, 2, \dots$ the function $\delta_i(f(x_1, \dots, x_n))$ is independent of $\delta_{i+k}(x_s)$, $s = 1, 2, \dots, n$, $k = 1, 2, \dots$.*

Let us now generalize somewhat some of our main concepts.

1.3.23. Definition. Let $F = (f_1, \dots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ be an arbitrary function. We say that it is *equiprobable modulo p^k* if all sets

$$\{(a_1, \dots, a_n) \in \{0, 1, \dots, p^k - 1\}^{(n)}\colon\ F(a_1, \dots, a_n) \equiv \bar{a} \pmod{p^k}\}$$

are of the same order for all $\bar{a} \in \{0, 1, \dots, p^k - 1\}^{(m)}$. We say that F is (*asymptotically*) *equiprobable* if it is equiprobable modulo p^k for all (sufficiently large, respectively, i.e., exceeding a certain N) natural k. Similarly, we say that F *asymptotically preserves measure* (respectively, *is asymptotically ergodic*) if the restriction of the function $F \pmod{p^k}$ (the least nonnegative residue F modulo p^k) to the set $\{0, 1, \dots, p^k - 1\}^{(n)}$ is a bijective (transitive, resp.) mapping for all natural k exceeding a certain N.

In what follows in this section, we shall always assume that $F = (f_1, \dots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ and $f\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p$ are functions uniformly differentiable modulo p and that the functions f and F have integer-valued derivative modulo p.

1.3.24. Theorem. *Let $F = (f_1, \dots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(m)}$ be a function uniformly differentiable modulo p with integer-valued derivatives modulo p. The function F is asymptotically equiprobable if it is equiprobable modulo*

some p^k, $k \geq N_1(F)$ and the rank of the Jacobi matrix $F_1'(u)$ modulo p is m at all points $u = (u_1, \ldots, u_n) \in (\mathbb{Z}/p^k)^{(n)}$.

1.3.25. Corollaries. 1°. *Suppose that $m = 1$ under the conditions of the preceding theorem. The function F is asymptotically equiprobable if it is equiprobable some modulo p^k, $k \geq N_1(F)$, and its differential d_1F modulo p does not vanish at any point from $(\mathbb{Z}/p^k)^{(n)}$.*

2°. (cf. [8]). *If $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$, then f is equiprobable if it is equiprobable modulo p and all its derivatives do not vanish simultaneously at any point from $(\mathbb{Z}/p)^{(n)}$.*

For $m = n$, the sufficient conditions given above are also necessary conditions.

1.3.26. Criterion. *The function $F = (f_1, \ldots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(n)}$, which is uniformly differentiable modulo p and has integer-valued derivatives modulo p, asymptotically preserves measure if and only if it is bijective modulo $p^{N_1(F)}$ and its Jacobian modulo p does not vanish at any point from $(\mathbb{Z}/p^k)^{(n)}$, $k = N_1(F)$ (equivalently, when it is bijective modulo $p^{N_1(F)+1}$).*

1.3.27. Corollaries. 1°. *If $n = 1$ under the conditions of the preceding criterion, then F asymptotically preserves measure if and only if it is bijective modulo $p^{N_1(F)}$ and its derivative modulo p does not vanish at any point from $\{0, 1, \ldots, p^{N_1(F)} - 1\}$.*

2°. (cf. [8, Sec. 4.5]). *Let $F = (f_1, \ldots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(n)}$, where $f_i(x_1, \ldots, x_n) \in \mathbb{Z}_p[x_1, \ldots, x_n]$, $i = 1, 2, \ldots, n$. The function F preserves measure if and only if it is bijective modulo p and $\det F'(u) \not\equiv 0 \pmod p$ for all $u \in \{0, 1, \ldots, p-1\}^{(n)}$ (equivalently, when it is bijective modulo p^2).*

3°. *If $A = \langle \mathbb{Z}_p, \Omega \rangle$ is a universal algebra of finite signature Ω and all operations from Ω are uniformly differentiable modulo p and have integer-valued derivatives modulo p, then the polynomial f over A asymptotically preserves measure if and only if it is bijective modulo $p^{k(A)}$, where $k(A) = \max\{N_1(\omega)\colon \omega \in \Omega\} + 1$.*

Comparing statements 1.3.24 and 1.3.26, we can pose a natural question of whether the sufficient conditions of Theorem 1.3.24 are also necessary. The answer is in the negative: the function $f(x, y) = 2x + y^3$ on $\mathbb{Z}_2$ is a counterexample, a fact that can be proved using the results of [18].

Let us now begin studying asymptotically ergodic functions in the class of all functions which are uniformly differentiable modulo p and have integer-valued derivatives modulo p. It turns out that all functions of this kind are only of dimension 1.

1.3.28. Theorem. *Let $F = (f_1, \ldots, f_m)\colon \mathbb{Z}_p^{(n)} \to \mathbb{Z}_p^{(n)}$ be an asymptotically ergodic function which is uniformly differentiable modulo p and has integer-valued derivatives modulo p. Then $n = 1$.*

There does not yet exist a full characterization of all asymptotically ergodic functions from the class of all functions which are uniformly differentiable modulo p and have integer-valued derivatives modulo p. However, if we impose an additional constraint that the function should be uniformly differentiable modulo p and have an integer-valued derivative modulo p^2, then we can give the following description of these functions.

1.3.29. Criterion. *Let $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ be a function uniformly differentiable modulo p^2 and having an integer-valued derivative modulo p^2. The function f is asymptotically ergodic if and only if it is transitive modulo $p^{N_2(f)+1}$ for an odd prime p or modulo $p^{N_2(f)+2}$ for $p = 2$.*

1.3.30. Corollary. *Suppose that $A = \langle \mathbb{Z}_p, \Omega \rangle$ is a universal algebra of finite signature Ω and all its operations are uniformly differentiable modulo p^2 and have integer-valued derivatives modulo p^2. Then we can effectively indicate a natural $k(A)$ such that the polynomial $f(x) \in A[x]$ is asymptotically ergodic if and only if it is transitive modulo $p^{k(A)}$.*

Criterion 1.3.29 reduces the problem of verification of the ergodicity of the function f to the problem of computing the number $N_2(f)$ and verifying the transitivity of f modulo the corresponding power of p. However, it may turn out to be difficult even to estimate $N_2(f)$, and therefore it would pay to indicate, for the given class $\mathcal{K}$ of functions that are uniformly differentiable modulo p^2 and have integer-valued derivatives modulo p^2, a certain function $\xi(\mathcal{K})$ such that f would be asymptotically ergodic if and only if it is transitive modulo $p^{\xi(\mathcal{K})}$. This proved to be possible for the class of all compatible integer-valued polynomials over $\mathbb{Q}_p$.

Moreover, the corresponding result is also valid for a wider class $\mathcal{A}$, namely, for all compatible functions $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ such that the coefficients of their interpolation series decrease not slower than $i!$ (recall that $\lim\limits^{p}_{i\to\infty} i! = 0$). Here is the exact definition of the class $\mathcal{A}$: a function f of the form

$$f(x) = \sum_{i=0}^{\infty} a_i \binom{x}{i} \qquad (*)$$

(where $a_i \in \mathbb{Z}_p$, $i = 1, 2, \ldots$) lies in $\mathcal{A}$ if and only if it is compatible and $\|\frac{a_i}{i!}\|_p \le p^{\rho(f)}$, where $\rho(f) \in \mathbb{N}_0$. The class $\mathcal{A}$ is rather wide: it contains, for instance, all compatible integer-valued functions analytic on $\mathbb{Z}_p$, i.e., compatible functions $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ which admit of the representation as convergent power series of the form $\sum_{i=0}^{\infty} a_i x^i$. It is known (see [22, Chapter 4, Theorem 4, p. 224]) that a function f of the form $(*)$ is analytic if and only if $\lim\limits^{p}_{i\to\infty} \frac{a_i}{i!} = 0$. Next we suppose that $f \in \mathcal{A}$. We set

$$\lambda(f) = \min\Big\{k\colon\ 2\frac{p^k - 1}{p - 1} - k > \rho(f)\Big\}.$$

1.3.31. Theorem. *The function $f \in \mathcal{A}$ for $p \ne 2, 3$ ($p = 3$ resp.) is ergodic if and only if it is transitive modulo p ($3^{\lambda(f)+2}$ resp.).*

Using this theorem, we can verify whether the given integer-valued and compatible polynomial $f(x) \in \mathbb{Q}_p[x]$ is ergodic. (Recall that integer-valued compatible polynomials $f(x) \in \mathbb{Q}_p[x]$ are described by Theorem 1.3.3.) For our purposes, we represent $f(x)$ in the form $\frac{1}{r}g(x)$, where $r \in \mathbb{Z}_p$, $g(x) \in \mathbb{Z}_p[x]$, and at least one of the coefficients of the polynomial $g(x)$ is not divisible by p. Then $\rho(f) = \operatorname{ord}_p r$, and we easily find $\lambda(f)$ and verify whether f is transitive on $\mathbb{Z}/p^{\lambda(f)+1}$ (say, by direct calculations).

We can also apply Theorem 1.3.31 to other classes of the functions $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$. Let us consider, for example, the formal power series over $\mathbb{Z}_p$:

$$s(x) = \sum_{i=0}^{\infty} a_i x^i.$$

It is known (see [22]) that this series converges for all x such that $\|x\|_p < 1$. We denote by $\mathcal{C}(x)$ the class of all functions represented by series of this form which also converge for $\|x\|_p = 1$. In other words, $s(x) \in \mathcal{C}(x)$ if and only if $\lim\limits^{p}_{i\to\infty} = 0$. In particular, $\mathcal{C}(x)$ contains all functions defined by the polynomials from $\mathbb{Z}_p[x]$. The class $\mathcal{C}(z)$ is a subclass of $\mathcal{A}$ and $N_2(s) \le 2$ and $\rho(s) = 0$, i.e., $\lambda(s) = 1$ for all $s(x) \in \mathcal{C}(x)$.

1.3.32. Proposition. *The function $s(x) \in \mathcal{C}(x)$ is ergodic if and only if it is transitive modulo p^2 when $p \ne 2, 3$, or p^3 when $p = 2, 3$.*

1.3.33. Corollaries. 1° (M. V. Larin). *The polynomial $f(x) \in \mathbb{Z}[x]$ is ergodic if and only if it is transitive modulo p^2 if $p \ne 2, 3$ or p^3 if $p = 2, 3$.*

2°. *For $u(x)$, $g(x) \in \mathcal{C}(x)$ the function $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ of the form $f(x) = \frac{u(x)}{1+pg(x)}$ is ergodic if and only if it is transitive modulo p^2 if $p \ne 2, 3$ or p^3 if $p = 2, 3$.*

Incompatible functions. All preceding statements, beginning with 1.3.24, were proved on the assumption that the corresponding functions were not only uniformly differentiable modulo a certain p^k, but that all its derivatives modulo p^k were integer-valued. By virtue of Theorem 1.3.17, this assumption means the asymptotic compatibility of these functions. Consequently, all preceding results of this section describe equiprobable or ergodic functions only in the class of asymptotically compatible functions. However, among the commands of the processor mentioned above, there is an operation which is not compatible — it is the operation SHL of a shift toward the lower positions. Its 2-adic continuation is a uniformly differentiable function whose derivative is no longer integer-valued. This does not mean that the preceding results can be applied only to the polynomials over the universal algebra

$$A = \langle \mathbb{Z}/2^n, \{\oplus, \odot, \mathrm{XOR}, \mathrm{OR}, \mathrm{AND}, \mathrm{SHL}, \mathrm{SHR}\}\rangle,$$

into which the operation SHL does not enter (i.e., in other words, only to programs that do not use the command SHL). However, when we use the tools indicated above in a specific situation, we must make sure that the polynomial we use satisfies, for instance, the hypothesis of Theorem 1.3.3, i.e., it should be compatible as a function on $\mathbb{Z}_2$. From the point of view of a programmer, this is not quite natural (why should we choose the law of recursion of a generator of random numbers from the set of functions with integer-valued derivatives?), and therefore a mathematician faces the problem of trying to understand how much the requirement of integer-valuedness of the derivative (or asymptotic compatibility) of the function being studied restricts the class of possible program generators of random numbers. In order to pose the corresponding mathematical problem, we must return, for some time, to the applied problems mentioned in the introduction to this work.

Our final aim is to learn to use the enumerated "computer" operations for constructing polynomials that define the laws of recursion of "good" generators of random numbers, and we have agreed to consider transitive functions on finite sets to be polynomials of this kind. In this section we considered, in fact, the following technique of constructing these functions on the set of p^n elements with a sufficiently large n: we take an ergodic function f on the space of p-adic integers which is compatible (or asymptotically compatible) with all congruences of the ring $\mathbb{Z}_p$ and consider the map $f_n = \phi_n(f)$ of the ring $\mathbb{Z}/p^n$ into itself induced by the function f as the required map (see the last subsection of Sec. 0.1). In other words, the required transitive function on the set $M_n = \{0, 1, 2, \dots, p^n - 1\}$ is constructed as the function $\mathrm{MOD}_{p^n}(f \mid M_n)$, which associates every element $i \in M_n$ with the least nonnegative residue modulo p^n of the value of the function $f \mid M_n$ (which, by definition, is the restriction of the function f to the set M_n) at the point i. For asymptotically compatible f, the maps f_n and $\mathrm{MOD}_{p^n}(f \mid M_n)$ obviously coincide for all sufficiently large n. Now if we omit the requirement of the asymptotic compatibility of the function f, then the map $\mathrm{MOD}_{p^n}(f \mid M_n)$ may turn out to be not only intransitive but not even bijective, and the map f_n will, generally speaking, be incorrectly defined. Hence, we need only those functions $g\colon \mathbb{Z}_p \to \mathbb{Z}_p$ for which the corresponding maps $\mathrm{MOD}_{p^n}(g \mid M_n)$ are at least bijective for all sufficiently large n. We denote the class of these functions by $\mathcal{G}(p)$. Thus, we are interested in how much the class of all functions uniformly differentiable modulo p^k from $\mathcal{G}(p)$ is wider than the class of all functions uniformly differentiable modulo p^k whose derivatives modulo p^k are integer-valued.

Clearly, all functions from $\mathcal{G}(p)$ asymptotically preserve measure. We can show that if the function f, which is uniformly differentiable modulo p^k, lies in $\mathcal{G}(p)$, then the p-adic norm of its derivative modulo p^k at every point from $\mathbb{Z}_p$ cannot be smaller than 1. The case where this norm is equal to 1 at all points from $\mathbb{N}_0$ (or, what is the same, at all points of $\mathbb{Z}_p$) is equivalent to the asymptotic compatibility of the function f. It is also clear that if $h\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is a certain asymptotically compatible and measure-preserving function and $g \in \mathcal{G}(p)$, then the function $h(g)$ lies in $\mathcal{G}(p)$. The first example of a uniformly differentiable and not asymptotically compatible function from $\mathcal{G}(p)$ was found by A. A. Nechaev: for $p = 2$, it is the function $\frac{x^2+x}{2}$. It turns out that with an accuracy to within the indicated composition with asymptotically compatible and measure-preserving functions, this example is unique, namely, the following theorem is valid.

1.3.34. Theorem (I. A. Yurov). *If $f \in \mathcal{G}(p)$ is uniformly differentiable modulo some p^k, then it is asymptotically compatible for $p \neq 2$, and for $p = 2$ it is either asymptotically compatible or has the form $f = h(\frac{x^2+x}{2})$, where h is asymptotically compatible and preserves measure.*

The proof of this theorem uses the methods of non-Archimedean analysis and algebraic geometry and will be published in the near future. (Already published. See I.A.Yurov,"On p-adic functions which preserve Haar measure", *Mat. Zametki*,**63**, No.6, 1998, 935-950 - *Added by V.S.Anashin to the original text after its publication.*)

Thus, ergodic functions from $\mathcal{G}(p)$ such that they are uniformly differentiable modulo some p^k, but their derivatives modulo p^k are not integer-valued, can only exist for $p = 2$; then these functions must have the form indicated in Theorem 1.3.34. The latter have not yet been described. Moreover, we have no examples of functions of this kind; neither do we know whether they exist at all.

Chapter 2

POLYNOMIALS OVER NONCOMMUTATIVE GROUPS WITH OPERATORS

Beginning the study of uniformly distributed sequences generated by polynomials over noncommutative groups with multioperators, we must first restrict both the class of the groups under investigation and the possible systems of multioperators. Just as in the preceding sections, we shall be guided by common sense and try not to neglect the cases that are most important for applications and, at the same time, not to formulate problems in the a priori hopeless statement. If, in accordance with these principles, we try to restrict the class of possible systems of multioperators, then it is reasonable to study now only *groups with operators* since applications give some examples of commands which can be interpreted as operators on a group (see the introduction), and I have no other, more exotic, examples of elementary procedures, performed by processors, which could be regarded as multioperators on a non-Abelian group.

This means that we shall study equiprobable, measure-preserving, or ergodic functions on the group G (whose operation is written multiplicatively here and henceforth) in the class of all functions of the form

2.1. $$w(x_1, \dots, x_n) = g_1(x_{i_1}^{\omega_1})^{n_1} g_2(x_{i_2}^{\omega_2})^{n_2} \dots g_k(x_{i_k}^{\omega_k})^{n_k} g_{k+1}.$$

Here $g_1, \dots, g_{k+1}$ are elements of the group G, $n_1, \dots, n_k$ are rational integers, $i_1, \dots, i_k \in \{1, 2, \dots, n\}$, $\omega_1, \dots, \omega_k$ are endomorphisms of the group G, and the image of the element $h \in G$ under the action of the endomorphism ω is denoted by h^ω. For the time being, we shall call functions of the form 2.1 polynomial functions with operators.

Using common sense, we shall now restrict the class of possible noncommutative group operations. Let $\mathcal{G}$ be the class of all finite groups that admit of ergodic polynomial functions in one variable with operators. The class $\mathcal{G}$ obviously contains all polynomially complete groups, i.e., all finite simple non-Abelian groups (see Sec. 0.1). In other words, any ergodic function in one variable on a finite simple non-Abelian group can be represented as a polynomial over this group. Our aim is to find the explicit form of this polynomial. In the case of a different polynomially complete structure, namely, a finite field, in order to solve this problem in principle, we used interpolation formulas which allow us to find a polynomial representation for any function on a finite field. We had to state that the solution obtained was practically unacceptable since the construction of an interpolation polynomial for high-order fields is impossible in real time (see the corresponding discussion in Sec. 1.2 of Chapter 1). Arguments of this kind, only in the superlative degree, are also applicable to polynomials over finite simple non-Abelian groups. By way of example, we must point out that at present interpolation formulas are only known for one, the smallest, group of this kind, the alternating group A_5 of degree 5 [4, 19]. The length (as an element of the corresponding free product of groups, see Sec. 0.1) of an ergodic polynomial over A_5 presently known is about 10^4. Recall that A_5 contains only 60 elements.

By virtue of what has been said, it is reasonable to exclude from further consideration finite simple non-Abelian groups. But then, together with them, all non-solvable groups must also be excluded from consideration.

Indeed, suppose that G is a finite non-solvable group, $w(x)$ is an ergodic polynomial function with operators on G, N is a completely characteristic subgroup of index k. Then it is easy to see that the function $w^k(x)$ is an ergodic polynomial function with operators on the group N. Furthermore, if K is a completely

characteristic subgroup in N, then, by virtue of Proposition 0.1.5, $w^k(x)$ induces an ergodic polynomial function $g(x)$ with operators on the quotient group N/K. Since the group G is non-solvable, there exist fully invariant subgroups N and K such that the quotient group N/K is isomorphic to the direct power of the finite simple non-Abelian group H, i.e., $N/K \cong H^{(m)}$. (The last statement is a well-known fact from the theory of finite groups.) This means that if we know how to construct ergodic polynomial functions $w(x)$ with operators on the finite unsolvable group G, then we could also construct an m-dimensional ergodic polynomial function with operators on the finite simple non-Abelian group H. But the arguments used above show that the solution of the last problem is impossible for the present, and, hence, all finite groups under investigation must not contain simple non-Abelian sections, i.e., must be solvable.

Thus, in this part of the work, we restrict our discussion to equiprobable, measure-preserving, or ergodic functions defined by polynomials over finite solvable groups with operators. True enough, as in the first chapter of this work, some naturally arising problems will lead us outside of the class of finite groups.

2.1. Equiprobable Polynomial Functions

Just as in the case of polynomial functions on finite commutative rings, before describing the conditions of equiprobability of a function defined by a polynomial over a solvable group with operators, we must first learn to differentiate these functions. Let G be a group with a system of operators Ω. Then any polynomial $w(x_1, \ldots, x_n)$ over G can be represented in the form 2.1, where $\omega_1, \ldots, \omega_k \in \Omega$. The polynomial $w(x_1, \ldots, x_n)$ is an element of the group $G[X^\Omega]$ of all polynomials of the set of variables $X = \{x_1, x_2, \ldots\}$ over the group G with the system of operators Ω. The group $G[X^\Omega]$ is a free product of the group G by the free group $F(X^\Omega)$ freely generated by the set $\{x_i^\omega : i = 1, 2, \ldots, \omega \in \Omega\}$. Let us consider the semigroup free product of the group $G[X^\Omega]$ by a free semigroup freely generated by the elements of the set Ω. We denote by $\mathbb{Z}\langle G, \Omega, X\rangle$ a semigroup ring of the above-mentioned semigroup free product over the ring of rational integers $\mathbb{Z}$. The elements of this semigroup ring can be represented as finite sums $\sum_{(i)} z_i \prod_{(j)} \omega_j w_j$, where $z_i \in \mathbb{Z}$, $\omega_j \in \Omega$, $w_j \in G[X^\Omega]$, i and j run over a finite set of subscripts. By definition, the *differentiation with respect to the variable* x_i is the mapping

$$\frac{\partial}{\partial x_i}: G[X^\Omega] \to \mathbb{Z}\langle G, \Omega, X\rangle,$$

which satisfies the following conditions:

(i) $\frac{\partial x_j}{\partial x_i} = \delta_{ij}$ is the Kronecker delta;

(ii) $\frac{\partial g}{\partial x_i} = 0$ for any $g \in G$;

(iii) $\frac{\partial x_j^\omega}{\partial x_i} = \delta_{ij}\omega$ for any $\omega \in \Omega$;

(iv) $\frac{\partial uv}{\partial x_i} = \frac{\partial u}{\partial x_i}v + \frac{\partial v}{\partial x_i}$ for any $u, v \in G[X^\Omega]$.

It is easy to verify that these conditions are satisfied by one and only one map. Under this mapping the image $\frac{\partial f}{\partial x_i}$ of the polynomial $f \in G[X^\Omega]$ is called the *derivative of the polynomial* f *with respect to the variable* x_i. The concept of the derivative of a polynomial over a group with operators is a further generalization of the concept of the derivative of a free polynomial (i.e., an element of $F(X)$) put forth by R. Fox [10] and of the derivative of a polynomial over a group with an empty set of operators introduced by Lausch [20].

The concept of the derivative of a polynomial over a group with operators was introduced for an arbitrary group with an arbitrary set of operators. We shall assume now that the group G is finite and solvable and introduce the concept of the *value of the derivative of a polynomial over the group* G *with the system of operators* Ω *in a ring of endomorphisms of the principal factor* A *of the group* G. We shall begin with the case where A is the minimal Ω-invariant (i.e., $A^\omega \subseteq A$ for any $\omega \in \Omega$) normal subgroup in G. Since G is finite and solvable, A is an elementary Abelian p-group for a certain prime p, and therefore the structure of the vector space of some dimension n over the field $\mathbb{Z}/p$ is defined in the natural way on A. We denote

by $E(A)$ the ring of all endomorphisms of the group A, and then we can regard $E(A)$ as the ring of all $n \times n$ matrices over $\mathbb{Z}/p$. We associate every element $g \in G$ with the element $\pi_A(g) \in E(A)$, which is an automorphism induced on the subgroup A by means of conjugation with the aid of the element g. Similarly, for every $\omega \in \Omega$ we denote by $\rho_A(\omega)$ the endomorphism of the subgroup A induced on it by the action of the operator ω. Let $h = (h_1, \ldots, h_n)$ be an arbitrary collection of n elements from G. There exists one and only one homomorphism $\tau_{A,h}$ of the ring $\mathbb{Z}\langle G, \Omega, X\rangle$ in the ring $E(A)$ such that $\tau_{A,h}(g) = \pi_A(g)$ for every $g \in G$, $\tau_{A,h}(\omega) = \rho_A(\omega)$, and $\tau_{A,h}(x_i^\omega) = h_i^\omega$ for all $\omega \in \Omega$, $i = 1, 2, \ldots, n$. If $w(x_1, \ldots, x_n)$ is a polynomial of the form 2.1, then the endomorphism

$$\frac{\partial_A w(h_1, \ldots, h_n)}{\partial_A x_i} = \tau_{A,\mathbf{h}}\Big(\frac{\partial w(x_1, \ldots, x_n)}{\partial x_i}\Big) \in E(A)$$

is the *value of the derivative of the polynomial w with respect to the variable x_i at the point $(h_1, \ldots, h_n)$ in the ring $E(A)$*. The relation

$$w(h_1 a_1, \ldots, h_n a_n) = w(h_1, \ldots, h_n) a_1^{\left(\frac{\partial_A w(h_1, \ldots, h_n)}{\partial_A x_1}\right)} \ldots a_n^{\left(\frac{\partial_A w(h_1, \ldots, h_n)}{\partial_A x_n}\right)}$$

is valid, where $h_1, \ldots, h_n \in G$, $a_1, \ldots, a_n \in A$. Note that here the elements from A play the part of "small increments of the arguments," and the relation itself is an analog of the formula from classical differential calculus. In the same way, we define the value of the derivative in the ring of endomorphisms of a certain principal factor of the group G. Recall that the principal factor of the group G with the system of operators Ω is, by definition, any quotient group H/K, where H and K are normal Ω-invariant subgroups in G, $H \supseteq K$, $H \neq K$, and there is no normal Ω-invariant subgroup S in G such that $H \supseteq S \supseteq K$, $H \neq S$, $S \neq K$. All principal factors of a finite solvable group are elementary Abelian p-groups in some prime p, and therefore the values of the derivatives in the rings of endomorphisms of the principal factors can also be regarded as matrices over the corresponding finite fields of prime orders. The analog of the above-mentioned "formula of small increments" is valid in this case with an accuracy to within some factor from K (i.e., the analog of an "infinitely small term" from the classical formula) or, in other words, is no longer an equality but a congruence modulo K. In general, the situation concerning differential calculus for finite solvable groups is similar, in many important details, with the situation for the case of finite commutative rings. First and foremost, it concerns the "small increments formula," which makes it possible, just as for finite rings, to use induction (in this case on the length of the principal series) for proving the criteria of equiprobability of polynomial maps. It should be pointed out, however, that since the "derivative of the product" is asymmetric with respect to the cofactors for the case of polynomials over a group (see (iv)), the analogs of the "differentiation formulas" already differ essentially from their classical prototypes. For instance, $\frac{\partial x^n}{\partial x} = 1 + x + \ldots + x^{n-1}$ for positive integers n.

It should also be pointed out that differential calculus on groups becomes noticeably simpler in one special case, namely, for finite nilpotent groups with an empty set of operators. Since all factors of the principal series of a finite nilpotent group are central (i.e., H/K lies at the center of the quotient group G/K) and are prime-order groups, the value of the derivative of polynomial 2.1 with respect to the ith variable at any point in the ring of endomorphisms of any principal factor is compatible modulo the corresponding prime number p with

$$\deg{}_i w(x_1, \ldots, x_n) = \sum_{i_j = i} n_j,$$

i.e., with the degree of the polynomial $w(x_1, \ldots, x_n)$ with respect to the variable x_i. The following criterion of the equiprobability of a polynomial mapping on a finite solvable group with operators is valid. For simplicity, we shall formulate this criterion only for the case of polynomials in one variable.

2.1.1. Proposition. *The polynomial $w(x)$ in the variable x over the finite solvable group G with the system of operators Ω is bijective on G (i.e., preserves measure) if and only if every matrix $\frac{\partial_A w(g)}{\partial_A x_i}$ is nonsingular,*

being a matrix over the corresponding finite prime-order field for any principal factor F of the group G and any element $g \in G$.

This proposition is a trivial generalization of the result of Lausch [20], proved by him for $\Omega = \varnothing$, to the case of a nonempty system of operators Ω. The corresponding result for nilpotent groups with $\Omega = \varnothing$ is especially simple.

2.1.2. Corollary (see [21]). *If G is a finite nilpotent group (with an empty system of operators), then the polynomial $w(x)$ in one variable x over it is bijective on G if and only if its degree is coprime with the order of the group.*

2.2. Ergodic Polynomial Functions

Let us now cope with the problem of characterization of finite solvable groups with operators which admit of ergodic polynomial mappings. Here the multidimensional case is even simpler than the corresponding analog for finite commutative rings.

2.2.1. Proposition. *If the finite solvable group G with the system of operators Ω admits of the ergodic polynomial mapping $F = (f_1, \ldots, f_n)\colon G^{(n)} \to G^{(n)}$, then either $n = 1$ or $n = 2$, and $|G| = 2$.*

The proof of this proposition is rather simple and makes it possible to demonstrate some general ideas, and therefore we shall give it here.

Suppose that N is a minimal nontrivial normal Ω-invariant subgroup in G (then N is an elementary Abelian p-group for some prime p) and let m be the index of N in G. If $m = 1$, then we are in the situation of Sec. 1.1 of this work, i.e., F is an affine transformation of the Abelian group $G^{(n)}$, and, in accordance with Theorem 1.1.1, the only possibilities are either $n = 1$ and G is a cyclic group of order p, or $n = 2$ and $G^{(2)}$ is a Klein group, i.e., $|G| = 2$.

Let $m \neq 1$, i.e., N be a proper subgroup. The restriction of the transformation of F^{nm} to the subgroup $N^{(n)}$ is a transitive transformation of the subgroup $N^{(n)}$. Since N is Abelian, it follows from the "small increments formula" given above that this restriction of the transformation F^{nm} to the subgroup $N^{(n)}$ has the form $u \mapsto au^{\xi}$ $(u \in N^{(n)})$, where $a \in N^{(n)}$, $\xi \in E(N^{(n)})$. Therefore, for $n \geq 2$ it follows from Theorem 1.1.1 that the only case that is possible is where $n = 2$ and $|N| = 2$. However, since N is normal and Ω-invariant, it follows from the condition $|N| = 2$ that N lies at the center of the group G and either $a^{\omega} = a$ or $a^{\omega} = 1$ for any $\omega \in \Omega$, $a \in N$. Therefore, if $w(x_1, \ldots, x_n)$ is represented as 2.1, then, for any $a_1, \ldots, a_n \in N$, we have

$$w(a_1, \ldots, a_n) = h(w) a_1^{d_1(w)} \ldots a_n^{d_n(w)},$$

where $h(w) = g_1 \ldots g_{k+1}$, $d_i(w)$ is the least nonnegative residue modulo 2 of the integer

$$\sum_{i_s = i,\, N^{\omega_s} = N} n_s.$$

Let us associate the map $F = (f_1, f_2)$ with the 2×2 matrix $D = (d_{ij})$ over the field $\mathrm{GF}(2)$, where $d_{ij} = d_j(f_i)$, $i, j \in \{1, 2\}$. Then D induces the endomorphism δ of the subgroup $N^{(2)}$ and

$$F(a, b) = h \cdot (a, b)^{\delta}$$

for any $a, b \in N$, $(a, b) \in N^{(2)}$, $h \in G^{(2)}$. It follows from the last relation that for all $a, b \in N$ we have

$$F^{2m}(a, b) = g \cdot (a, b)^{\delta^{2m}}$$

for a suitable $g \in G^{(2)}$, with g being independent of a, b. On the other hand, as was shown above, F^{2m} is a transitive transformation of the subgroup $N^{(2)}$, and, hence, $g \in N^{(2)}$. Since $N^{(2)}$ is an elementary Abelian group of type (2.2), it follows from 1.1.2 that the endomorphism δ^{2m} must be a nontrivial involution in the

group of automorphisms of the group $N^{(2)}$. However, the algebra of all endomorphisms of the group $N^{(2)}$ is isomorphic to the algebra $L_2(2)$ of all 2×2 matrices over the field GF (2) and the group of all automorphisms of the group $N^{(2)}$ is isomorphic to the complete linear group $\mathrm{GL}_2(2)$ of dimension 2 over GF (2), which, in turn, is isomorphic to a symmetric group of degree 3. It is easy to show now that no even degree of any element of the group $L_2(2)$ and, in particular, δ^{2m}, can be a nontrivial involution. The contradiction obtained shows that for $m \neq 1$ only $n = 1$ is possible, and this completes the proof of the proposition.

Thus, when we characterize finite solvable groups with operators, which admit of ergodic polynomial functions, we can restrict our discussion to the case of polynomials in one variable. However, we must first impose some more constraints on the system of operators.

Clearly, the existence of a transitive polynomial over a certain group G with the system of operators Ω not only restricts the possible structure of the group G, but also imposes certain constraints on Ω. A transitive polynomial can exist for the given group G with one system of operators and cannot exist for the group G with some other system of operators. The Klein group K_4 (an elementary Abelian group of type (2.2)) can serve as an example: if we take the whole group $\mathrm{Aut}\, K_4$ of automorphisms of the group K_4 as Ω, then such a polynomial exists, but if we take as Ω the set of all automorphisms of order 3, then the group K_4 with this system of operators does not admit of an ergodic polynomial function (see 1.1.2). Therefore, in order to characterize all finite solvable groups with operators that admit of ergodic polynomial functions, it is reasonable to do the following. We should first try to find the description of all finite solvable groups G that admit of ergodic polynomial functions and possess the maximal system of operators Ω, i.e., a system such that any endomorphism of the group G can be induced by a certain operator from Ω, or, to put it otherwise, $\Omega = \mathrm{E}(G)$, where $\mathrm{E}(G)$ is the set of all endomorphisms of the group G. Then we should describe all ergodic polynomials over each of the finite solvable groups G with the system of operators $\Omega = \mathrm{E}(G)$ and, in particular, for every ergodic polynomial w to obtain a list $\mathcal{E}(w)$ of endomorphisms entering into its canonical form. Then the final formulation of the corresponding classification theorem will be as follows: the finite solvable group G with the system of operators Ω admits of an ergodic polynomial function if and only if G admits of an ergodic polynomial function being regarded as a group with the system of operators $\mathrm{E}(G)$ and Ω induces on G all endomorphisms from $\mathcal{E}(w)$ for a certain ergodic polynomial w over the group G with the system of operators $\mathrm{E}(G)$. Although the corresponding classification theorem has not yet been proved, the ways of proving it are sufficiently clear, and we shall show, in what follows, a certain possible approach to obtaining this classification. As we see, the essential part of the proof must consist of the classification of finite solvable groups G with the system of operators $\mathrm{E}(G)$ that admit of ergodic polynomials. Such a theorem has already been proved, and below we give the classification of all finite solvable groups G with the system of operators Ω, which admit of ergodic polynomials, for the cases $\Omega = \varnothing$, $\Omega = \mathrm{Aut}\, G$, and $\Omega = \mathrm{E}(G)$. We denote by $\mathcal{C}_0$, $\mathcal{C}_A$, and $\mathcal{C}_E$, respectively, the class of all finite solvable groups with the system of operators $\Omega = \varnothing$, $\Omega = \mathrm{Aut}\, G$, and $\Omega = \mathrm{E}(G)$ which admit of ergodic polynomial functions. Clearly, $\mathcal{C}_0 \subseteq \mathcal{C}_A \subseteq \mathcal{C}_E$. The following theorem describes nilpotent groups from these classes.

2.2.2. Theorem ([2]). *A finite nilpotent group lies in $\mathcal{C}_E$ if and only if it is either trivial or isomorphic to one of the following groups:*

(1) *to the cyclic group $\mathrm{C}(m)$ of order m;*

(2) *to the group $\mathrm{D}_n^k = \mathrm{gp}\,(u, v \parallel v^{2^n} = 1,\ v^u = v^{-1},\ u^2 = v^{2^k})$, where $n = 1, 2, 3, \ldots$, and $k \in \{n, n-1\}$ for $n > 1$ and $k = 1$ for $n = 1$;*

(3) *to the group $\mathrm{SD}_n = \mathrm{gp}\,(u, v \parallel u^2 = v^{2^n} = 1,\ v^u = v^{2^{n-1}-1})$, where $n = 3, 4, 5, \ldots$;*

(4) *to the direct product $H \times \mathrm{C}(m)$, where $H \in \{\mathrm{D}_n^k, \mathrm{SD}_n\}$ and m is odd.*

Out of these groups, the groups SD_n and $\mathrm{SD}_n \times \mathrm{C}(m)$ with an odd m, and only these groups, do not lie in $\mathcal{C}_A$. Finally, the class $\mathcal{C}_0$ consists exactly of all groups $\mathrm{C}(m)$, $m = 2, 3, 4, \ldots$.

Note that $\mathrm{D}_1^1 = K_4$ is Klein's group, D_2^1 is a group of quaternions 8, D_n^{n-1} is a generalized group of quaternions, D_n^n is a dihedral group of order 2^{n+1}, and SD_n is a semidihedral group.

In order to formulate the corresponding theorem for solvable groups, we shall need the following groups

in their representations by the generators and relations or in the form of the semidirect products

$$M(m,k,s) = \operatorname{gp}(c,\, d \parallel c^m = d^k = 1,\, d^c = d^s),$$

where $m, k = 2, 3, 4, \ldots$, $s \not\equiv 1 \pmod{k}$, $s^m = 1 \pmod{k}$, m and k are coprime,

$$A(r) = \operatorname{gp}(b,\, u,\, v \parallel b^{3^r} = u^2 = v^2 = 1,\, uv = vu,\, u^b = v,\, v^b = uv) = K_4 \leftthreetimes \mathrm{C}(3^r)$$

is a semidirect product of a Klein group by a cyclic group of order 3^r, $r = 1, 2, 3, \ldots$,

$$\mathrm{S}(r) = \operatorname{gp}(a \parallel a^2 = 1) \leftthreetimes \mathrm{A}(r),$$

where $b^a = a^{-1}$, $u^a = u$, $v^a = uv$, $r = 1, 2, 3, \ldots$,

$$\mathrm{H}(r) = \mathrm{D}_2^1 \leftthreetimes \mathrm{C}(3^r),$$

where $b^a = a^{-1}$, $u^a = u$, $v^a = uv$, $r = 1, 2, 3, \ldots$,

$$\mathrm{Q}_1(r) = \mathrm{H}(r) \leftthreetimes \operatorname{gp}(a \parallel a^2 = 1),$$

where $b^a = a^{-1}$, $u^a = u$, $v^a = uv$, $r = 1, 2, 3, \ldots$,

$$\mathrm{Q}_2(r) = \operatorname{gp}(a,\, b,\, u,\, v \parallel b^{3^r} = v^4 = 1),$$

where $b^a = b^{-1}$, $u^a = u^{-1}$, $v^a = uv$, $u^b = v^u = v^{-1}$, $v^b = uv^{-1}$, $a^2 = u^2 = v^2$, $r = 1, 2, \ldots$.

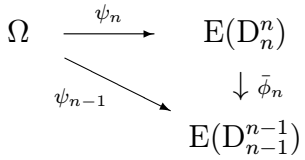
2.2.3. Theorem ([2]). *A finite solvable group lies in $\mathcal{C}_E$ if and only if it is either trivial or isomorphic to one of the following groups:* (1) $\mathrm{C}(m)$, (2) $\mathrm{M}(m,k,s)$, (3) D_n^k, (4) SD_n, (5) $\mathrm{A}(r)$, (6) $\mathrm{H}(r)$, (7) $\mathrm{S}(r)$, (8) $\mathrm{Q}_1(r)$, (9) $\mathrm{Q}_2(r)$, (10) $B\lambda A$, *where the orders of the groups A and B are coprime, A is any group of type* (3)–(9), *B is any group of type* (1)–(2). *Out of these groups, the following groups lie exactly in $\mathcal{C}_A$: all groups which are isomorphic to any group of type* (1)–(3), (5)–(9) *and all groups which are isomorphic to certain groups of type* (10), *namely, to groups in which:* (11) *the semidirect factor A is any group of type* (3), (5)–(9) *and the semidirect factor B is any group of type* (1)–(2), *all elements from A commuting with all elements from B,* (12) *$A = \mathrm{D}_n^k$, B is any group of type* (1)–(2), *the element $v \in \mathrm{D}_n^k$ commuting with all elements from B and the automorphism of the subgroup B, induced on it by means of conjugation with the aid of the element $u \in \mathrm{D}_n^k$, having order* 2, (13) *A is any group of type* (7)–(9), *B is any group of type* (1)–(2). *Finally, out of these groups, exactly all groups which are isomorphic to any group of type* (1)–(2), (7)–(9), (13) *lie in $\mathcal{C}_0$.*

Although the proof of these two theorems is constructive in the sense that the belonging of each of the enumerated groups to the class $\mathcal{C}_0$, $\mathcal{C}_A$, $\mathcal{C}_E$ is proved by constructing a corresponding polynomial, the general problem of describing all ergodic polynomials over finite solvable groups with operators is far from being solved. However, we see the ways that may lead to its solution, and here is one of them which is of interest, since it actually reduces the problem to the field of non-Archimedean analysis.

It should first be pointed out that except for a small number, all groups indicated in Theorems 2.2.2 and 2.2.3 can be combined into series that form spectra. For instance, the series of dihedral groups of orders 2^r, $r = 4, 5, 6, \ldots$, form the spectrum

$$\ldots \xrightarrow{\phi_{n+1}} \mathrm{D}_n^n \xrightarrow{\phi_n} \mathrm{D}_{n-1}^{n-1} \xrightarrow{\phi_{n-1}} \ldots \xrightarrow{\phi_4} \mathrm{D}_3^3.$$

Here ϕ_n is an epimorphism whose kernel is a subgroup of order 2 generated by the element $v^{2^{n-1}}$ of the group D_n^n. This kernel is a fully invariant subgroup in D_n^n, and therefore the epimorphism ϕ_n induces the homomorphism $\bar{\phi}_n$ of the semigroup $\mathrm{E}(\mathrm{D}_n^n)$ of all endomorphisms of the dihedral group D_n^n. We can show that this homomorphism is, in fact, an epimorphism. Now we fix a certain group of operators Ω, i.e., define the mappings $\psi_n \colon \Omega \to \mathrm{E}(\mathrm{D}_n^n)$ such that each of the following diagrams is commutative:



Thus, the spectrum of dihedral groups given above can be regarded as a spectrum of groups with the system of operators Ω. The inverse limit of this spectrum D_∞ is a pro-2-group which is a semidirect product of the additive group $\mathbb{Z}_2^+$ of 2-adic integers by a cyclic group of order 2. We denote by $\tilde{\phi}_n$ a natural epimorphism of the projection of the inverse limit D_∞ to the nth group D_n^n of this spectrum. Now we can put every polynomial function f on the dihedral group D_n^n into correspondence with the polynomial function $\tilde{f}$ on the group D_∞, such that the functions f and $\tilde{\phi}_n(\tilde{f})$ on the group D_n^n coincide. The idea of describing ergodic polynomial functions on the group D_n^n is similar to that used for describing ergodic polynomials over the rings of residues $\mathbb{Z}/2^n$, which also form a spectrum, whose inverse limit is a ring of 2-adic integers $\mathbb{Z}_2$ and the part of the epimorphism of projecting $\tilde{\phi}_n$ is played by the epimorphism of reduction modulo 2^n, namely, we describe (asymptotically) ergodic polynomial functions on the group D_∞, and this last problem reduces to the description of ergodic functions of a special kind on the space of 2-adic integers.

Indeed, the group D_∞ contains a fully invariant subgroup $N = (2\mathbb{Z}_2)^+$, which is an additive group of the ideal of all even 2-adic numbers. It is obvious that $\mathrm{D}_\infty/N \cong K_4$. The polynomial $w(x) \in \mathrm{D}_\infty[x]$ is ergodic if and only if it is ergodic modulo subgroup N and the polynomial $w^{(4)}(x)$ is ergodic as a function on N. But the polynomial $w(x)$ is ergodic modulo N if and only if it induces a transitive affine transformation of the Klein group K_4; this situation is completely described by Theorem 1.1.2, and it only remains to study the conditions of ergodicity of the polynomial $w^{(4)}(x)$ on N. However, since N is an Abelian fully invariant subgroup in D_∞, it follows, by virtue of the "small increments formula" and the fact that all subgroups of the form $(2^i\mathbb{Z}_2)^+$ are also Abelian fully invariant subgroups, that this last problem reduces to the problem for compatible 2-adic functions. Indeed, the subgroup N is isomorphic to the additive group $\mathbb{Z}_2^+$ of the ring of 2-adic integers, and, with an accuracy to within this isomorphism, the polynomial $w^{(4)}(x)$ can be regarded as a compatible 2-adic function. The criteria of ergodicity of these functions are formulated in Sec. 1.3 of this work.

The same arguments can be used for the other series of groups (i.e., for other spectra) enumerated in Theorems 2.2.2 and 2.2.3, since the inverse limits of these spectra also contain fully invariant Abelian pro-p-groups and the corresponding quotient groups are sufficiently "small" (we can show that they are isomorphic to the symmetric groups of degrees 2, 3, or 4 or to the group of quaternions of order 8). Thus, the problem of describing ergodic polynomials over these groups reduces to describing ergodic polynomials over the above-mentioned "small" finite groups and to describing ergodic polynomials over Abelian pro-p-groups and, by virtue of what was stated, this problem does not seem to be hopeless, although it will require considerable efforts. Moreover, sufficiently complicated problems may arise that are connected with the description of the mixed identities of groups. We spoke about this in the introduction. These problems are considered in the last section of this work.

2.3. Mixed Identities of Groups

From this section, the reader will get some general idea of the problems which we encounter when describing mixed identities of a specific group. The problem of describing mixed identities, in turn, is subordinate to the problem of describing polynomial ergodic or equiprobable functions on a group, and therefore a detailed introduction to the theory of mixed identities of groups would divert us from the theme of this work. For this description we refer the reader to [3], where the fundamentals of the theory of mixed identities and mixed varieties of groups are given, as well as some bibliography concerning these themes. Because of the same considerations, we do not discuss mixed identities of groups with an arbitrary system of operators but restrict the discussion to mixed identities of groups (i.e., to the case of an empty system of operators).

Thus, our aim is to describe all mixed identities of a certain group G, i.e., all polynomials over G of the form

$$w(x_1,\dots,x_n)=g_1x_{i_1}^{n_1}g_2x_{i_2}^{n_2}\dots g_kx_{i_k}^{n_k}g_{k+1}$$

(where $g_1,\dots,g_{k+1}$ are elements of the group G, $n_1,\dots,n_k$ are rational integers, $i_1,\dots,i_k\in\{1,2,\dots,n\}$) that assume the value 1 for any values of the variables $x_1,\dots,x_n$ in the group G. The collection of all mixed identities in the set of variables $X=\{x_1,\dots,x_n,\dots\}$ is a normal subgroup $I_G[X]$ in the group $G[X]$ of all polynomials of the set of variables X over G. We can show that $I_G[X]$ is a free subgroup in the free product $G[X]$. It is also obvious that $I_G[X]$ is closed with respect to any replacement of variables by polynomials from $G[X]$, i.e., $w(x_1,\dots,x_n)\in I_G[X]$, $u_1,\dots,u_n\in G[X]$ implies $w(u_1,\dots,u_n)\in I_G[X]$. We call the set $W\subseteq I_G[X]$ the *basis of mixed identities* in the group G if all elements from $I_G[X]$ can be obtained from the elements of the set W by means of the operations of multiplication, transition to the inverse element, conjugation by means of elements from $G[X]$, and replacement of variables by elements from $G[X]$. To describe all mixed identities of the group G means to indicate certain of their bases.

It is known that to describe identities of some group (i.e., in our terminology, polynomials over a group all of whose coefficients are equal to 1 and which assume the value 1 for any values of the variables in this group), it is convenient to consider the varieties of the groups, namely, the classes of all groups which satisfy some system of identities (see [12]). We must act in a similar way when we describe mixed identities of groups. We shall need some new concepts, in particular, the concept of a mixed variety of groups.

Suppose that $Y=\{y_\alpha\colon\alpha\in I\}$ is an alphabet of a certain power, $X=\{x_1,\dots,x_n,\dots\}$ is some alphabet such that $X\cap Y=\varnothing$, whose elements are called *variables*, $F(X\cup Y)$ is a free group with the free base $X\cup Y$, $\mathcal{M}$ is a certain subset in $F(X\cup Y)$. A *mixed variety generated by the set* $\mathcal{M}$ is the class of all groups H for each of which we can define the mapping $\varphi\colon Y\to H$ such that $\mathcal{M}_{\tilde\varphi}\subseteq I_H[X]$, where $\tilde\varphi$ is a homomorphism of the group $F(X\cup Y)$ into the group $H[X]$ induced by the mapping φ, i.e., $x_i\tilde\varphi=x_i$, $y_\alpha\tilde\varphi=y_\alpha\varphi$ for all $\alpha\in I$ and all $i=1,2,\dots$. Note that when $I=\varnothing$ this definition turns into the definition of the variety of groups generated by the set of identities $\mathcal{M}$.

Moreover, for the given group G we denote by mvar G the class of all groups H such that there exists a homomorphism $\varphi\colon G\to H$ for which $I_G[X]\tilde\varphi\subseteq I_H[X]$, where $\tilde\varphi\colon G[X]\to H[X]$ is an induced homomorphism of groups of polynomials, i.e., $x_i\tilde\varphi=x_i$, $g\tilde\varphi=g\varphi$ for all $i=1,2,\dots$ and all $g\in G$. The following statement is valid: *for any group G the class mvar G is a mixed variety of groups* (*called a mixed variety generated by the group G*), *and any mixed variety is generated by certain of its groups.*

By and large, when describing mixed identities of a group, we have to use methods similar to those of the theory of varieties of groups, namely, describe mixed identities of some "simple" objects and employ them to construct more complicated objects by means of various group-theoretic operators and then obtain mixed identities of these complicated objects as compositions of the mixed identities of the "constituents." In the theory of varieties of groups, methods of this kind have Birkhoff's theorem as their source, which, in particular, states that every variety of groups is closed relative to the transition operators from a group to a subgroup, from a group to a quotient group, and from a system of groups to their Cartesian product. A similar (but weaker) statement is valid for mixed varieties of groups: it turns out that any mixed variety of groups is closed relative to the operator $\mathbb{Q}$ of transition from a group to a quotient group, the operator $\mathbb{C}$ of transition from a system of groups to their Cartesian product, and the operator $\mathbb{C}_d$ of transition from the group G to all subgroups, containing a diagonal, of all Cartesian degrees of the group G, and $\mathcal{C}=\mathbb{Q}\mathbb{C}_dH$ for any group H which generates $\mathcal{C}$.

A natural assumption arises that as the basis of mixed identities of the group G we can take their identities, which, in principle, could be described at least for groups indicated in Theorems 2.2.2 and 2.2.3 by means of the developed apparatus of the theory of varieties of groups. The exact formulation of this assumption reads as follows: if $\mathcal{G}$ is the basis of the identities of the group G, then $I_G[X]$ coincides with the verbal subgroup $\mathcal{G}(G[X])$ generated in $G[X]$ by the system $\mathcal{G}$. This statement is valid for the Abelian group G. Unfortunately, in the general case this assumption is incorrect: as is shown in [3], *if the finite group G is not nilpotent, then mvar G is not a variety of groups and, in particular, $I_G[X]\neq\mathcal{G}(G[X])$*. Moreover, even

if mvar G is a variety of groups (i.e., mvar $G = \operatorname{var} G$), this does not mean that $I_G[X] = \mathcal{G}(G[X])$. Finally, already among nilpotent groups of degree 2, there are examples of groups G for which $I_G[X] \neq \mathcal{G}(G[X])$.

All these circumstances suggest that the problem of describing mixed identities of groups from Theorems 2.2.2 and 2.2.3 may turn out to be not so simple, although the methods developed in [3] give grounds to believe that this description can be obtained in the final analysis. In particular, this statement is substantiated by the following result: *mixed identities of a finite nilpotent or metabelian group have a finite basis.*

REFERENCES

1. V. S. Anashin, "Uniformly distributed sequences of p-adic integers," *Mat. Zametki*, **55**, No. 2, 3–46 (1994).
2. V. S. Anashin, "Solvable groups with operators and commutative rings possessing transitive polynomials," *Algebra Logika*, **21**, No. 6, 627–646 (1982).
3. V. S. Anashin, "Mixed identities and mixed varieties of groups," *Mat. Sb.*, **129**, No. 2, 163–174 (1986).
4. V. S. Anashin and M. V. Larin, "On the interpolation on A_5" [in Russian], In: *Abstract of Reports on Group Theory. The 8th All-Union Symposium, Sums, May 24–27, 1982.* (1982), pp. 6–7.
5. E. F. Brickell and E. M. Odlizko, "Cryptoanalysis: review of the latest results," *IEEE*, **76**, No. 5, 75–93 (1988).
6. L. Kuipers and G. Niederreiter, *Uniform Distribution of Sequences*, John Wiley and Sons, New York–London–Toronto (1974).
7. M. Kline, *Mathematics. The Loss of Certainty*, Oxford Univ. Press, Oxford (1980).
8. D. Knuth, *The Art of Computer Programming. 2. Seminumerical Algorithms*, Addison-Wesley, Reading, Massachusetts (1969).
9. N. Koblitz, *p-Adic Numbers, p-Adic Analysis and Zeta-Functions*, Springer, Heidelberg (1977).
10. R. Crowell and R. Fox, *Introduction to the Knot Theory*, Ginu and Co., Boston (1963).
11. A. G. Kurosh, *General Algebra* (lectures of 1969–1970) [in Russian], Nauka, Moscow (1974).
12. H. Neumann, *Varieties of Groups*, Springer-Verlag, Berlin–Heidelberg–New York (1967).
13. V. S. Anashin, "Uniformly distributed sequences over p-adic integers," In: *Number Theoretic and Algebraic Methods in Computer Science, Proc. of Intern. Conf., Moscow, June–July, 1993*, World Scientific (1995), pp. 1–18.
14. V. S. Anashin, *Uniformly Distributed Sequences over p-Adic Integers*, Russian State University for the Humanities, Moscow (1993).
15. J. Eichenauer-Herrmann, "Inversive congruential pseudorandom numbers: a tutorial," *Intern. Statist. Rev.*, **60**, 167–176 (1992).
16. R. R. Hall, "On pseudo-polynomials," *Mathematika* (Gr. Brit.), **18**, No. 1, 71–77 (1971).
17. D. Jonah and B. M. Schreiber, "Transitive affine transformations of discrete groups," *Pacif. J. Math.*, **58**, No. 2, 483–509 (1975).

18. H. K. Kaiser and W. Nöbauer, "Permutation polynomials in several variables over residue class rings," *J. Austral. Math. Soc.*, **A43**, No. 2, 171–175 (1987).

19. H. Lausch, "Interpolation on the alternating group A_5," in: *Contrib. Gen. Algebra. Proc. Klangenfurt Conf. 1978*, J. Heyn, Klangenfurt (1979), pp. 187–192.

20. H. Lausch, "Zur Theorie der Polynompermutationen über endlichen Gruppen," *Arch. Math.*, **19**, No. 3, 284–288 (1968).

21. H. Lausch and W. Nöbauer, *Algebra of Polynomials*, North-Holland, Amsterdam–London (1973).

22. K. Mahler, *p-Adic Numbers and Their Functions*, 2nd ed. Cambridge Univ. Press (1981).

23. B. R. McDonald, *Finite Rings with Identity*, Marcel Dekker, New York (1974).

24. H. Niederreiter, "Nonlinear methods for pseudorandom number and vector generation," *Lect. Notes Econ. Math. Syst.*, 145–153 (1992).

25. H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, Ch. 8 (1992).