ISSN 0081-5438, Proceedings of the Steklov Institute of Mathematics, 2009, Vol. 265, pp. 30–58. © Pleiades Publishing, Ltd., 2009.

Noncommutative Algebraic Dynamics: Ergodic Theory for Profinite Groups

Vladimir S. Anashin[a]

Received December 2008

Abstract—In order to determine transitive polynomials on finite solvable groups, we develop ergodic theory for polynomial transformations on profinite groups with operators.

DOI: 10.1134/S0081543809020035

1. DYNAMICS ON FINITE ALGEBRAIC STRUCTURES AND ULTRAMETRICITY

Everywhere in this paper a (discrete autonomous) *dynamical system* is just a pair $\langle \mathbb{A}, f \rangle$, where $f\colon \mathbb{A} \to \mathbb{A}$ is a map of the set $\mathbb{A}$ into itself. Dynamical systems theory studies trajectories, i.e., sequences of iterations

$$x_0, \quad x_1 = f(x_0), \quad \dots, \quad x_{i+1} = f(x_i) = f^{i+1}(x_0), \quad \dots .$$

Its central questions are the asymptotic behavior of these sequences, their distribution, etc. This implies that $\mathbb{A}$ is endowed with a *metric* and with a *measure*.

When we speak about *algebraic* dynamics, we assume that the space $\mathbb{A}$ is also endowed with a certain algebraic structure (a field, a ring, a group, ...) and that the map f somehow *agrees* with this algebraic structure; e.g., f may be a *compatible* map (that is, for every congruence $\sim$ of $\mathbb{A}$ and all $a, b \in \mathbb{A}$, we have $f(a) \sim f(b)$ whenever $a \sim b$). For instance, a polynomial over $\mathbb{A}$ and an endomorphism of $\mathbb{A}$ are compatible maps.

In real life settings we *never* deal with an infinite $\mathbb{A}$. Yet for a finite $\mathbb{A}$, every trajectory is eventually periodic, and it is meaningless to speak of its asymptotic behavior. Unfortunately, in real life settings the set $\mathbb{A}$ is usually very big—so big that we cannot use computers to determine where a point will be after N iterations for large N. However, we can study the behavior of trajectories on small $\mathbb{A}$ in order to understand what happens to trajectories when $\mathbb{A}$ becomes bigger and bigger. Thus, we have to study the asymptotic behavior of trajectories when the order $\#\mathbb{A}$ of $\mathbb{A}$ goes to infinity, $\#\mathbb{A} \to \infty$.

Obviously, we can say almost nothing nontrivial about this asymptotic behavior in a general case, for arbitrary maps of arbitrary finite sets. It turns out that we can say a lot about this behavior whenever $\mathbb{A}$ is endowed with an algebraic structure and f somehow agrees with this structure, say, when f is compatible and finite algebraic systems $\mathbb{A}_n$ constitute an inverse spectrum:

$$\dots \xrightarrow{\varphi_{n+1}} \mathbb{A}_n \xrightarrow{\varphi_n} \mathbb{A}_{n-1} \xrightarrow{\varphi_{n-1}} \dots \xrightarrow{\varphi_1} \mathbb{A}_0.$$

The inverse limit $\mathbb{A}_\infty$ of the inverse spectrum can be endowed with a profinite topology, with a metric, and with a measure. This metric will necessarily be an ultrametric, a non-Archimedean metric. Therefore, there exists a close connection between the dynamics on finite sets and the dynamics on ultrametric spaces.

[a] Institute for Information Security Issues, Moscow State University, Michurinskii pr. 1, Moscow, 119234 Russia.
E-mail address: vs-anashin@yandex.ru

An important class of such inverse limits is given by the rings of p-adic integers $\mathbb{Z}_p$ ($p > 1$ is a prime number), which are the inverse limits of the residue class rings $\mathbb{Z}/p^n\mathbb{Z}$ modulo p^n (or, briefly, of residue rings modulo p^n), $n = 1, 2, \dots$. The corresponding projections φ_n are just the reductions modulo p^n, which are clearly ring epimorphisms. Thus, p-adic dynamics can be considered as an essential part of algebraic dynamics, which is currently an intensively developing mathematical discipline. It is worth a brief review that follows.

1.1. Towards algebraic dynamics: Brief history of p-adic dynamics. Traditionally, dynamical systems were considered in the fields of real and complex numbers, $\mathbb{R}$ and $\mathbb{C}$. Later there appeared studies of dynamical systems in *finite fields and rings*, in which number theory was widely used. The theory of p-adic dynamical systems was developed as a natural generalization of dynamics in the residue rings modulo p^n. It was generalized to arbitrary *non-Archimedean fields*.[1] This was a combination of *number theoretic and dynamical approaches* to algebraic dynamics. We can mention the studies by W. Narkiewicz, A. Batra, P. Morton, P. Patel, J. Silverman, G. Call, D.K. Arrowsmith, F. Vivaldi, S. Hatjispyros, J. Lubin, T. Pezda, H.-C. Li, and L.-C. Hsia [14–17, 33, 47, 48, 66–73, 76–78, 80–93, 98–103, 119, 120] and the recent studies by J.A.G. Roberts, F. Vivaldi, W.-S. Chou, I.E. Shparlinski, A.-H. Fan, M.-T. Li, J.-Y. Yao, Y.F. Wang, D. Zhou, M. Misiurewicz, J.G. Stevens, D. Thomas, A. Peinado, F. Montoya, J. Muñoz, and A.J. Yuste [34, 38–40, 79, 97, 109, 111].

These studies are closely related to studies initiated in *algebraic geometry*. In algebraic geometry the fields of real and complex numbers, $\mathbb{R}$ and $\mathbb{C}$, do not play an exceptional role. All geometric structures can also be considered over non-Archimedean fields. Therefore, for people working in algebraic geometry, it was natural to try to generalize some mathematical structures to the non-Archimedean case, even if these structures do not directly belong to the domain of algebraic geometry; for example, it was natural to consider dynamics in a non-Archimedean field $\mathbb{K}$. These (algebraic geometric) dynamical studies began with the article of M. Herman and J.-C. Yoccoz [46] on the problem of small divisors in non-Archimedean fields. It seems that this was the first publication on non-Archimedean dynamics. A crucial role in the further development of this dynamical approach was played by J. Silverman (see, e.g., [112–114]). The studies were continued by R. Benedetto [19–28], J. Rivera-Letelier [105–108], C. Favre and J. Rivera-Letelier [41], F. Laubie, A. Movahhedi, and A. Salinier [62], and J.-P. Bézivin [29–32]. Finally, J. Silverman published his fundamental book [115] devoted to arithmetic problems in the theory of dynamical systems.

Another approach to algebraic dynamics has p-adic theoretical physics as its source. The first p-adic physical models were elaborated in the 1990s at the Steklov Mathematical Institute of the Russian Academy of Sciences by V. Vladimirov, I. Volovich, I. Aref'eva, and E. Zelenov in collaboration with A. Khrennikov and B. Dragovich; important contributions to this domain were made by E. Witten, G. Parisi, P. Framton, P.G.O. Freund, M. Olson, and others (see, e.g., the monographs [123, 50, 52] and the pioneering papers of Vladimirov and Volovich [121, 122, 124]). In 1989, Ruelle, Thiran, Verstegen, and Weyers published an interesting article [110] on p-adic quantum mechanics, and a little later Thiran, Verstegen, and Weyers published the article [117] on p-adic dynamics (see also [118]). We also mention the earlier preprint [18] of Ben-Menahem. A. Khrennikov went down this road to p-adic dynamical systems as well, from the study of quantum models with $\mathbb{Q}_p$-valued functions to p-adic and more general non-Archimedean dynamical systems (see, e.g., [51, 52]). The following works in this direction are also worth noting: [1, 57, 75, 94, 95, 116]. In these works, the study of p-adic *monomial dynamics* $x \mapsto x^n$ on $\mathbb{Z}_p$ played an important role. Later Khrennikov, Nilsson, and Nyqvist [56] considered perturbed monomial systems $x \mapsto x^n + q(x)$ on $\mathbb{Z}_p$, where $q(x)$ is a polynomial that is "small" compared with the monomial part of the dynamics;

[1] These are fields with absolute values for which the strong triangle inequality $|x + y| \le \max(|x|, |y|)$ holds. We remark that the fields of p-adic numbers $\mathbb{Q}_p$ are non-Archimedean.

the smallness is defined as the smallness of coefficients with respect to the p-adic absolute value. In [42–44, 55, 74] the problem of ergodicity of perturbed monomial dynamics on p-adic spheres was formulated; it was put forward at numerous international conferences and talks at many universities throughout the world. Nevertheless, it remained unsolved until 2005, when the author of this paper solved it in the most general case [9], for 1-Lipschitz locally analytic dynamical systems.

The latter work was a continuation of studies on p-adic ergodicity started in [3, 4, 6]; we also mention the papers [61, 36] on polynomial dynamics over residue rings. These studies also led to algebraic dynamics and proved to be extremely important for applications to computer science and cryptology, especially in connection with pseudorandom numbers and uniform distribution of sequences. The research in this direction began in 1992 with the publications [3, 4] by the present author, which were succeeded by his works [5–8, 11, 12] on *p-adic ergodic theory* and applications. These studies are motivated mainly by the problem of constructing a computer program that generates a random-looking sequence of numbers. To look any random, the sequence must be at least uniformly distributed in some precise sense; it must also pass common statistical tests; and the performance of the corresponding program (or hardware device) must be sufficiently fast. To satisfy the latter condition, the program must be a not too complicated composition of basic computer instructions (additions, multiplications, ORs, ANDs, XORs, etc.), which turned out to be continuous with respect to a 2-adic metric. Thus, to comply with the first condition, one may combine these instructions to obtain a certain ergodic transformation f on $\mathbb{Z}_2$; then the corresponding sequence of iterations $x, f(x), f^2(x), \dots$, which is actually a trajectory (orbit) of the corresponding dynamical system $\langle \mathbb{Z}_2, f\rangle$, will necessarily be uniformly distributed in $\mathbb{Z}_2$ and hence modulo 2^n for all $n = 1, 2, \dots$. This is a strong motivation to develop p-adic ergodic theory.

We note that the above-mentioned works deal with algebraic dynamics over *commutative* algebraic structures, such as commutative rings and fields. However, motivations to develop algebraic dynamics over *noncommutative* algebraic structures are also rather strong. Let us show how, for instance, the operation of a *noncommutative* dihedral group D_n of order 2^{n+1} arises in computer science. In computers, there are instructions that depend on the value of a one-bit registry, a so-called "flag." Usually program jumps are instructions that depend on flags. Often a flag contains the sign of a number. Consider the following instruction (or a program): If the flag value is 0, then addition is performed, and if it is 1, then subtraction is performed. Here the $*$ operation of the group D_n appears: If ε and ξ are the values of the flag and a and b are n-bit words in the alphabet $\{0,1\}$, then $(\varepsilon, a) * (\xi, b) = (\varepsilon \oplus \xi, b + (-1)^{\xi} a)$, where $\oplus$ is addition modulo 2 and $+$ is addition modulo 2^n. Now, using this instruction and endomorphisms of the group D_n, which can actually be realized as substitutions like $(1,0) \mapsto (\alpha, k)$, $(0,1) \mapsto (\beta, m)$ via look-up tables, one can consider iterations of a polynomial transformation (see (1) below) on the group D_n with a corresponding set of operators, i.e., polynomial dynamics on a noncommutative group.

There are purely mathematical motivations to develop algebraic dynamics over noncommutative algebraic structures as well. In mathematics, the study of ergodic polynomial transformations on (non-Abelian) groups has its own history that started with the following more than 50-year-old problem of P. Halmos [45, p. 26]: Can an automorphism of a locally compact but noncompact group be an ergodic measure-preserving transformation? The problem attracted considerable attention and motivated a related study of affine ergodic transformations on noncommutative groups G (that is, ergodic transformations of the form $x \mapsto gx^{\beta}$, where $g \in G$ and β is an automorphism of the group G) by B. Schreiber with co-workers and by other authors (see, e.g., [104] and references therein). In the late 1960s the theory of polynomials over noncommutative algebraic structures, and especially over groups, emerged (see [65]); its development naturally led to the study of *polynomial transformations on groups with operators*, i.e., transformations of the form

$$x \mapsto g_1(x^{\omega_1})^{n_1} g_2(x^{\omega_2})^{n_2} \dots g_k(x^{\omega_k})^{n_k} g_{k+1} = g(x^{\alpha_1})^{n_1} (x^{\alpha_2})^{n_2} \dots (x^{\alpha_k})^{n_k}, \tag{1}$$

where $g, g_1, \dots, g_{k+1} \in G$, $n_1, \dots, n_k$ are rational integers, $\omega_1, \dots, \omega_k$ are operators, i.e., group endomorphisms, and $\alpha_1, \dots, \alpha_k$ are endomorphisms of the group G. As any profinite group[2] can be endowed with a metric (which is called a profinite metric) and a measure, it is reasonable to ask what continuous transformations with respect to the profinite metric are measure-preserving or ergodic with respect to the measure. The recent paper [58] by J. Kingsbery, A. Levin, A. Preygel, and C.E. Silva gives a general equivalent description of measure-preserving and ergodic transformations in terms of the actions of these transformations on all groups of the inverse spectrum; for instance, to determine whether a transformation is measure-preserving, it is necessary to verify whether it induces a bijection on every group from the inverse limit, i.e., for an infinite number of groups. Thus, it is reasonable to ask whether this verification can be done in a finite number of steps and so to obtain explicit formulas for these transformations.

The latter setting is important for applications. Actually, ergodic transformations on groups can be used to generate pseudorandom sequences of permutations in the same way as ergodic transformations of p-adic integers are used to generate pseudorandom sequences of numbers. Pseudorandom sequences of permutations on finite sets are used in cryptography when constructing the so-called polyalphabetic substitution ciphers. A well-known example of ciphers of this kind is the Enigma, an encryption device used by Germany during World War II.

In Section 4 we consider a problem of determining ergodic transformations on profinite groups with operators. We note that not all profinite groups admit polynomial ergodic transformations; however, using the earlier publication of the author [2], which characterizes finite solvable groups having ergodic polynomials, we determine ergodic polynomial transformations on profinite groups with operators that are the inverse limits of finite solvable groups. We emphasize that these dynamics on profinite groups can somehow be "reduced to," or "composed of," the p-adic dynamics on different spaces of p-adic integers.

These results may be considered, on the one hand, as a contribution to ergodic theory for noncommutative algebraic structures. In this connection, it is interesting to note that actually in Section 4 we mimic the approach from the p-adic ergodic theory, but with the use of a noncommutative differential calculus (instead of p-adic derivation); the latter calculus originally arose in the works of R. Fox on knot theory (see [35]). We believe that this approach can be expanded to develop ergodic theory on noncommutative algebraic systems other than groups with operators.

On the other hand, the ergodic theory for profinite groups, which we develop in Section 4, has applications to pseudorandom generators that are constructed not only with the use of arithmetical and logical instructions of a computer, but also with the use of flags. The basic ideas of this approach lead to new constructions of "flexible" stream ciphers (see, e.g., [11]).

Concluding the review, we only mention two other important areas of application of p-adic dynamics: In 1997, Khrennikov [52] proposed to apply dynamical systems in the rings $\mathbb{Z}_m$ to modeling cognitive processes, especially in psychology. Recently 4-adic and 2-adic dynamical systems were applied to genetics (see [53, 37, 54]).

1.2. Ergodicity and uniform distribution of sequences. As mentioned above, in applications, measure-preserving and ergodic mappings often serve as a tool to construct uniformly distributed sequences for various applied purposes (e.g., for pseudorandom number generation, cryptography, etc.; see, e.g., [3, 5–7, 10, 11]). To construct these sequences, the following basic result of ergodic theory is actually used (see, e.g., [59, Ch. 3, Definition 1.1, Exercise 1.10, Lemma 2.2]):

Proposition 1.1. *Let $\mathbb{S}$ and $\mathbb{T}$ be compact topological groups, and let $f\colon \mathbb{S} \to \mathbb{T}$ be a mapping that is continuous and measurable with respect to the Haar measure. If $(a_n)_{n=0}^{\infty}$ is a uniformly distributed sequence over $\mathbb{S}$ and f is measure-preserving, then the sequence $(f(a_n))_{n=0}^{\infty}$ is uniformly distributed over $\mathbb{T}$.*

[2] A group that is an inverse limit of finite groups.

If additionally $\mathbb{S} = \mathbb{T}$, f is ergodic, and $\mathbb{S}$ is separable, then the sequence $(f^n(a))_{n=0}^{\infty}$ is uniformly distributed for almost all $a \in S$.

As mentioned above, in real life settings we deal with dynamical systems on finite sets; that is, the order $\#\mathbb{A}$ of the group $\mathbb{A}$ is finite. Then every subset U of $\mathbb{A}$ is open and closed simultaneously, and $\mu(U) = \#U \cdot (\#\mathbb{A})^{-1}$. Moreover, if the groups $\mathbb{A}$ and $\mathbb{B}$ are of finite order, then the map $f\colon \mathbb{A} \to \mathbb{B}$ is measure-preserving if and only if $\#f^{-1}(a) = \#f^{-1}(b)$ for all $a, b \in \mathbb{A}$. Such maps are called *balanced*. Obviously, the map $f\colon \mathbb{A} \to \mathbb{A}$ preserves the measure μ if and only if it is bijective, that is, if f is a permutation on $\mathbb{A}$. Finally, f is ergodic if and only if this permutation has only one cycle, of length $\#\mathbb{A}$. In the latter case we say that f is *transitive* on $\mathbb{A}$. Note that whenever f is transitive, the corresponding trajectory is just a periodic sequence, and its shortest period is of length $\#\mathbb{A}$; that is, every element from $\mathbb{A}$ occurs in the period exactly once.

1.3. Hereditary dynamical properties and compatibility. Let A be a universal algebra (e.g., a group or a ring), and let $f\colon A \to A$ be a compatible map. Let $\varphi\colon A \to B$ be an epimorphism of the universal algebra A onto a universal algebra B of the same type, and let $x, y \in A$ be arbitrary elements of A such that their φ-images coincide, $\varphi(x) = \varphi(y)$. Then $\varphi(f(x)) = \varphi(f(y))$ since f is compatible. Thus, the map $f\varphi\colon B \to B$ defined as $(f\varphi)(b) = \varphi(f(a))$ for $b \in B$ and $a \in \varphi^{-1}(b)$ is well defined. So each compatible transformation on A defines a unique transformation on each epimorphic image of A. As each epimorphism of A defines a unique congruence of A and vice versa, we say that f *possesses some property* $\mathfrak{P}$ *modulo a congruence* η if the map induced by f on the corresponding epimorphic image possesses $\mathfrak{P}$. The following simple proposition holds:

Proposition 1.2. *Let A be a finite group, let η be a congruence of A, and let $F\colon A^n \to A^m$ (where $m \le n$) be a balanced (respectively, bijective, transitive) compatible map of the nth Cartesian power A^n onto the mth Cartesian power A^m of the group A. Then F is balanced (respectively, bijective, transitive) modulo η. If H is the kernel of the congruence η and $k = |A : H|$, then the map F for $m = n$ is transitive if and only if F is transitive modulo η and the iterated map $F^{kn}\colon H^n \to H^n$ is transitive on H^n.*

Moreover, if A is a direct product of groups B and C, $A = B \times C$, then F is balanced on A if and only if F is balanced both on B and C, i.e., modulo each congruence corresponding to the projection onto a direct factor. Finally, the map F for $n = m = 1$ is transitive if and only if it is transitive both on B and C and the orders $\#B$ and $\#C$ are coprime.

The most "natural" compatible transformation of a universal algebra is a polynomial transformation. However, ergodic polynomials (i.e., polynomials that induce ergodic transformations on the universal algebra) exist not over every universal algebra. Actually, the existence of an ergodic polynomial imposes strict limitations on the structure of a universal algebra. As ergodicity is the leading theme of the paper, we first introduce some important examples of universal algebras *having ergodic polynomials*, i.e., of algebras over which there exist polynomials that induce ergodic transformations on these algebras. In this section, we consider only finite universal algebras; now we describe finite Abelian groups with operators and finite commutative rings that admit ergodic (hence, transitive) polynomials. A similar problem for finite non-Abelian groups is much more complicated; we consider it in Section 3.

1.4. Ergodic polynomial transformations on finite Abelian groups with operators. Let G be a finite Abelian group with operation $+$ written additively, and let Ω be a set of operators on G; that is, every element $\omega \in \Omega$ induces an endomorphism of the group G: $(a+b)^\omega = a^\omega + b^\omega$ for all $a, b \in G$. It is clear that as the group G is Abelian, any ergodic (i.e., transitive) polynomial transformation must be of the form $x \mapsto a + x^\alpha$, where α lies in the ring $\operatorname{Env}\Omega$ generated by endomorphisms of G induced by operators from Ω; moreover, α must be an automorphism of G. Recall that as G is Abelian, all its endomorphisms form a ring with respect to addition and multiplication

(i.e., composition) of endomorphisms. That is, finite Abelian groups having ergodic polynomials are exactly finite Abelian groups having transitive *affine* transformations $x \mapsto a + x^\alpha$. Groups having transitive affine transformations were studied in [49], under the name of *single orbit groups*. In the following theorem we summarize the results from [49] concerning Abelian groups (with operators) that have transitive polynomials:

Theorem 1.3. *A finite Abelian group G with a set of operators Ω has ergodic polynomials if and only if G is isomorphic to one of the following groups*:

(i) *a cyclic group* $\mathrm{C}(m)$, $m = 1, 2, \dots$, *with an arbitrary set of operators* Ω;

(ii) *the Klein group* K_4 *with* $\Omega \ni \omega$ *inducing a nonidentity involution on* K_4;

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

Remark 1.4. We recall that the Klein group K_4 is isomorphic to the additive group of a 2-dimensional vector space over the field $\mathbb{F}_2$ of two elements. It is not difficult to see that the affine transformation $x \mapsto a + x^\psi$ on the Klein group K_4 ($a \in \mathrm{K}_4$, $\psi \in \mathrm{End}(\mathrm{K}_4)$) is transitive on K_4 if and only if ψ is a nonidentity automorphism whose square $\psi^2 = \psi \circ \psi$ is an identity automorphism and $a^\psi \neq a$.

As every endomorphism of the cyclic group $\mathrm{C}(n)$ (written additively) is a multiplication by m, all affine transformations of $\mathrm{C}(n)$ are in fact transformations of the form $x \mapsto (a + mx) \bmod n$ of the residue ring $\mathbb{Z}/n\mathbb{Z}$ modulo n. Thus, in view of the Chinese remainder theorem and Proposition 1.2, to characterize transitive transformations of this form it suffices to consider only the case of a prime power n. Theorem 1.9 (see below) completely describes transitive affine transformations of the residue rings $\mathbb{Z}/p^k\mathbb{Z}$, p prime, by virtue of Theorem 1.8.

All these results, in view of Proposition 1.2, give us a complete description of all finite Abelian groups (with operators) having transitive polynomials, as well as of transitive polynomial transformations themselves, in an explicit form. Starting at this point, we can try to expand these considerations in two directions: first, to the case of non-Abelian groups, and second, to the case of other commutative universal algebras; the most important of the latter are commutative rings. We deal with ergodic polynomial transformations on non-Abelian groups in Sections 3 and 4; we consider commutative rings having transitive polynomials in the next subsection. As we will see, in both cases the problem of description of the corresponding ergodic transformations will inevitably lead us to the non-Archimedean dynamics.

1.5. Ergodic polynomial transformations on finite commutative rings. In this subsection we demonstrate that except for some "sporadic" examples, residue rings and finite fields are the only finite commutative rings on which there exist polynomial ergodic transformations; that is, for applied purposes such as pseudorandom number generation, it is enough to restrict ourselves to dynamics on residue rings or finite fields rather than on more exotic rings.

Let R be a finite commutative ring with identity 1 (i.e., 1 is a multiplicative neutral element of R). The existence of univariate transitive polynomials over R imposes significant restrictions on the structure of R:

Proposition 1.5. *Whenever R has transitive polynomials, R is a principal ideal ring.*

Proposition 1.5 shows that whenever R has a transitive polynomial, R is a direct sum of local rings; that is, every direct summand is either a field or a ring that has a unique maximal ideal, which is called a radical of the ring. By Proposition 1.2, the ring R has a transitive polynomial if and only if every direct summand has a transitive polynomial and the orders of direct summands are pairwise coprime. However, it is well known that every finite field is polynomially complete; that is, every transformation on this field can be represented as a polynomial over this field. In particular, every finite field has transitive polynomials. Thus, to characterize finite commutative rings that have transitive polynomials, it suffices to restrict ourselves to finite local rings with nonzero radicals.

Theorem 1.6 [2]. *A local ring R has transitive polynomials if and only if one of the following alternatives holds*[3]:

(i) $R = \mathbb{F}_{p^n}$, *a field of* p^n *elements,* $n = 1, 2, \dots$;

(ii) $R = \mathbb{Z}/p^n\mathbb{Z}$, *a residue ring modulo* p^n, p *prime,* $n = 1, 2, \dots$;

(iii) $R = \mathbb{F}_p[x]/x^2\mathbb{F}_p[x]$, p *prime*;

(iv) $R = \mathbb{F}_p[x]/x^3\mathbb{F}_p[x]$, $p \in \{2, 3\}$;

(v) $R = \mathbb{Z}[x]/p^2\mathbb{Z}[x] + x^3\mathbb{Z}[x] + (x^2 - p)\mathbb{Z}[x]$, $p \in \{2, 3\}$;

(vi) $R = \mathbb{Z}[x]/9\mathbb{Z}[x] + x^3\mathbb{Z}[x] + (x^2 + 3)\mathbb{Z}[x]$.

Remark 1.7. It is obvious that the ring $R = \mathbb{Z}[x]/p^2\mathbb{Z}[x] + x^3\mathbb{Z}[x] + (x^2 - p)\mathbb{Z}[x]$ is a factor ring of the ring of polynomials in x over the residue ring $\mathbb{Z}/p^2\mathbb{Z}$ modulo the ideal generated by two polynomials, x^3 and $x^2 - p$. That is, the order of this ring R is p^3.

In a similar manner, it is easy to show that the ring $R = \mathbb{Z}[x]/9\mathbb{Z}[x] + x^3\mathbb{Z}[x] + (x^2 + 3)\mathbb{Z}[x]$ is a factor ring of the ring of polynomials in x over the residue ring $\mathbb{Z}/9\mathbb{Z}$ modulo the ideal generated by two polynomials, x^3 and $x^2 + 3$. That is, the order of this ring R is 27.

1.6. Ergodic polynomials over p-adic integers. Among the rings listed in Theorem 1.6, only the residue rings modulo p^k form a spectrum. However, the inverse limit of the residue rings $\mathbb{Z}/p^k\mathbb{Z}$ is the ring of p-adic integers $\mathbb{Z}_p$, which is endowed with a non-Archimedean (p-adic) metric and with a natural probabilistic measure, the normalized Haar measure.

It is clear that every polynomial over $\mathbb{Z}/p^k\mathbb{Z}$ can be considered as a polynomial with rational integer coefficients, that is, as a polynomial over $\mathbb{Z}_p$. This polynomial induces a transformation on $\mathbb{Z}_p$, which is compatible; thus, it is 1-Lipschitz with respect to the p-adic metric. Therefore, the problem of determining ergodic (that is, transitive) polynomials over the residue rings $\mathbb{Z}/p^n\mathbb{Z}$ becomes a problem of p-adic dynamics.

The following theorem holds:

Theorem 1.8 [6, 9]. *For $m = n = 1$, a 1-Lipschitz map $F\colon \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ is measure-preserving (or ergodic) if and only if it is bijective (respectively, transitive) modulo p^k for all $k = 1, 2, 3, \dots$.*

For $n \geq m$, the map F is measure-preserving if and only if it is balanced modulo p^k for all $k = 1, 2, 3, \dots$.

Further we will need the following criterion for ergodicity of affine transformations on $\mathbb{Z}_p$:

Theorem 1.9. *The map $f(x) = ax + b$, where $a, b \in \mathbb{Z}_p$, is an ergodic transformation on $\mathbb{Z}_p$ if and only if the following conditions hold simultaneously*:

$$b \not\equiv 0 \pmod{p}, \tag{2}$$

$$a \equiv 1 \pmod{p} \qquad \text{for odd } p, \tag{3}$$

$$a \equiv 1 \pmod{4} \qquad \text{for } p = 2. \tag{4}$$

The following theorem determines ergodic uniformly differentiable transformations on $\mathbb{Z}_p$:

Theorem 1.10 [3]. *Let a 1-Lipschitz map $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ be uniformly differentiable on $\mathbb{Z}_p$. Then f is ergodic if and only if it is transitive modulo p^n for some sufficiently large n.*

Note that in some interesting cases this "sufficiently large" n is actually rather small:

Corollary 1.11 (cf. [61, 36]). *A polynomial $f \in \mathbb{Z}_p[x]$ is ergodic if and only if f is transitive modulo p^2 for $p \notin \{2, 3\}$ and modulo p^3 for $p \in \{2, 3\}$.*

[3] We characterize rings up to isomorphisms.

2. BASICS OF POLYNOMIAL DYNAMICS ON GROUPS

Now we begin a study of measure-preserving (in particular, ergodic) transformations on a group G (whose operation is written multiplicatively henceforth) in the class of all maps $G^n \to G$ of the form

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

Here $g_1,\dots,g_{k+1}$ are elements of the group G, $n_1,\dots,n_k$ are rational integers, $i_1,\dots,i_k \in \{1,2,\dots,n\}$, and $\omega_1,\dots,\omega_k \in \Omega$. The image of an element $h \in G$ under the action of an operator ω is denoted by h^ω. Note that every operator $\omega \in \Omega$ acts on G by an endomorphism, which we denote by the same symbol ω. Thus, raising an element $h \in G$ to the power $n \in \mathbb{Z}$ commutes with the operator $\omega \in \Omega$, $(h^\omega)^n = (h^n)^\omega$; so we write $h^{n\omega}$ (or $h^{\omega n}$) instead of $(h^\omega)^n$ for short. Under these conventions, a polynomial $w(x_1,\dots,x_n)$ in variables $x_1,\dots,x_n$ over the group G with the set of operators Ω is an expression of the form

$$w(x_1,\dots,x_n) = g_1 x_{i_1}^{\omega_1 n_1} g_2 x_{i_2}^{\omega_2 n_2} \dots g_k x_{i_k}^{\omega_k n_k} g_{k+1}. \tag{5}$$

Below maps $G^n \to G$ of the form (5) will be referred to as (n-variate) polynomial functions over groups with operators. Note that whenever G is an "ordinary group," that is, a group with an empty set of operators, a polynomial $w(x_1,\dots,x_n)$ in variables $x_1,\dots,x_n$ over the group G can be written as

$$w(x_1,\dots,x_n) = g_1 x_{i_1}^{n_1} g_2 x_{i_2}^{n_2} \dots g_k x_{i_k}^{n_k} g_{k+1}. \tag{6}$$

Sometimes it is convenient to represent polynomials in a form other than (5) (or (6)), namely, in the form

$$w(x_1,\dots,x_n) = w(1,\dots,1) x_{i_1}^{h_1\omega_1 n_1} x_{i_2}^{h_2\omega_2 n_2} \dots x_{i_k}^{h_k\omega_k n_k}, \tag{7}$$

where $h_1,\dots,h_k \in G$. Indeed, as $xg = gx^g$ for all $x \in G$, where $x \mapsto x^g = g^{-1}xg$ is an automorphism of G induced by the conjugation by an element $g \in G$, we can rewrite (5) in the form (7) and vice versa. Note that in the case of univariate polynomials (i.e., when $n = 1$) in a variable x, the polynomial can be represented in the form

$$w(x) = w(1) x^{h_1\omega_1 n_1 + \dots + h_k\omega_k n_k}, \tag{8}$$

where $x^{h\omega_1 n + g\alpha m}$ stands for $x^{h\omega_1 n} x^{g\alpha m} = h^{-1}(x^\omega)^n h g^{-1}(x^\alpha)^m g$. A representation of the form (8) is convenient if, say, we consider a map induced by a polynomial $w(x)$ on a normal Abelian Ω-invariant subgroup $N \subset G$. In the latter case the sum $h_1\omega_1 n_1 + \dots + h_k\omega_k n_k$ can be treated as an element of the commutative ring $\mathrm{End}(N)$ of endomorphisms of the group N if we associate every $\omega \in \Omega$ with an endomorphism of N induced by the operator ω and every $g \in G$ with an automorphism of N induced by the conjugation by g. For instance, if N is an elementary Abelian p-group, p prime, we can treat N as a vector space over $\mathbb{F}_p$ (and hence $\mathrm{End}(N)$ is merely the algebra of all square matrices over $\mathbb{F}_p$); so the sum $h_1\omega_1 n_1 + \dots + h_k\omega_k n_k$ can then be treated as just the sum of the matrices $h_1\omega_1 n_1,\dots,h_k\omega_k n_k$, i.e., as a matrix over $\mathbb{F}_p$.

2.1. Noncommutative differential calculus. We need to develop necessary tools for studying polynomial dynamics over groups (with operators). In the case of a commutative structure, e.g., a ring $\mathbb{Z}_p$ of p-adic integers, one of the key points in our study of a dynamical system $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ was the "formula of small increments" that expresses the value of the function f at the point $x+h$, where h is p-adically small, via the derivative $f'(x)$: the congruence

$$f(x+h) \equiv f(x) + h \cdot f'(x) \pmod{p^{\mathrm{ord}_p h + 1}} \tag{9}$$

holds for any polynomial $f(x) \in \mathbb{Z}_p[x]$ and all $h \in \mathbb{Z}_p$. Using this formula, we actually reduced the problem of determining whether f is measure-preserving (or ergodic) to the study of the action of f on the residue ring $\mathbb{Z}/p^k\mathbb{Z}$, where k is small, and to the study of the behavior of the derivative $f'(x)$ (actually to the study of an affine map $h \mapsto a + h \cdot f'(x)$ on the field $\mathbb{F}_p$) (see, e.g., Hensel's lemma or Theorem 1.10). Our aim is to obtain an analog of formula (9) for non-Abelian groups. For this purpose, we need a notion of the derivative of a polynomial over a group with operators. This notion is a further generalization of the concept of free differential calculus (i.e., derivatives of elements of a free group $F(X)$ freely generated by X) put forth by R. Fox in connection with knot theory (see [35]) and of Lausch's notion of the derivative of a polynomial over a group with an empty set of operators (see [63, 65]).

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 (5), 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 in 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 $\{x_i^\omega \colon i = 1, 2, \ldots,\ \omega \in \Omega\}$. 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 $\mathbb{Z}\langle G, \Omega, X\rangle$ the 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 $z_i \in \mathbb{Z}$, $\omega_j \in \Omega$, $w_j \in G[X^\Omega]$, and i and j run over a finite set of subscripts. By definition, the *differentiation with respect to the variable* x_i is a map

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

that 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 $u, v \in G[X^\Omega]$.

This differentiation differs from the ordinary differentiation, e.g., of polynomials over commutative rings only by identity (iv). From this identity it follows that for $n \in \mathbb{Z}$

$$\frac{\partial x^n}{\partial x} = \begin{cases} x^{n-1} + x^{n-2} + \ldots + 1 & \text{if } n > 0, \\ 0 & \text{if } n = 0, \\ x^n + x^{n+1} + \ldots x^{-1} & \text{if } n < 0. \end{cases}$$

It is easy to verify that there exists a unique map that satisfies all these conditions (i)–(iv). The image $\frac{\partial w}{\partial x_i}$ of the polynomial $w \in G[X^\Omega]$ under this map is called the *derivative of the polynomial* w *with respect to the variable* x_i. Furthermore, if $N \lhd G$ is an Abelian Ω-invariant normal subgroup of G, then, given $g_1, g_2, \ldots \in G$, we associate every element $W(x_1, x_2, \ldots, x_n) = \sum_{(i)} z_i \prod_{(j)} \omega_j w_j(x_1, \ldots, x_n)$ with an endomorphism $W(g_1, \ldots, g_n) \in \mathrm{End}(N)$ induced on N by $W(g_1, \ldots, g_n)$:

$$h^{W(g_1,\ldots,g_n)} = ((h^{z_1})^{\omega_1})^{w_1(g_1,\ldots,g_n)} \cdot ((h^{z_2})^{\omega_2})^{w_1(g_1,\ldots,g_n)} \ldots,$$

where $(\cdot)^{w_i(g_1,\ldots,g_n)}$ is the conjugation by the element $w_i(g_1, \ldots, g_n) \in G$. In the case of $W = \frac{\partial w}{\partial x_i}$, this endomorphism is called the *value of the derivative* of the polynomial w at the point $(g_1, \ldots, g_n)$ and is denoted as $\frac{\partial w(g_1,\ldots,g_n)}{\partial x_i}$. The following formula, which follows directly from group laws, is now

obvious:

$$w(g_1h_1,\dots,g_nh_n)=w(g_1,\dots,g_n)\cdot h_1^{\frac{\partial w(g_1,\dots,g_n)}{\partial x_1}}\dots h_n^{\frac{\partial w(g_1,\dots,g_n)}{\partial x_n}}, \tag{10}$$

where $h_1,h_2,\dots,h_n\in N$.

Example 2.1. For instance, let G be an arbitrary group with an empty set of operators, and let $w(x)=ax^2bx^{-1}c$ be a polynomial over G, $a,b,c\in G$. Now, if $h\in N\lhd G$, then "pulling" the element h to the right-hand position, i.e., using the identities $hg=gh^g$, $(hg)^2=g^2h^{g^2+g}$, … and $(hg)^{-1}=g^{-1}h^{-1}$, $(hg)^{-2}=g^{-2}h^{-g^{-1}-1}$, …, we see that (cf. (8))

$$w(xh)=w(x)h^{xbx^{-1}c+bx^{-1}c-x^{-1}c}.$$

Note that $xbx^{-1}c+bx^{-1}c-x^{-1}c$ is the derivative of the polynomial $w(x)$.

In the case of polynomials in one variable x, we denote the derivative of the polynomial $w(x)$ by ∂w, for short. Thus, if $N\lhd G$ is an Abelian Ω-invariant normal subgroup of a group G with a set of operators Ω, and if $w(x)$ is a polynomial over G, then for all $g\in G$ the following equality holds:

$$w(gh)=w(g)h^{\partial w(g)}, \tag{11}$$

where $\partial w(g)$ is the *value of the derivative* ∂w at the point (element) $g\in G$, i.e., an endomorphism of N. Note that if, additionally, N is a minimal normal subgroup of a finite group G, then N is isomorphic to the additive group of a vector space over $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$. Thus, we can treat the values of derivatives of polynomials as linear transformations of this vector space.

Example 2.2. In Example 2.1 let $G=\mathrm{Sym}(4)$ be a symmetric group of permutations of a set of four elements, and let $N=\mathrm{K}_4\lhd\mathrm{Sym}(4)$ be its unique minimal normal subgroup, which is the Klein group K_4. Note that K_4 is isomorphic to the additive group of a 2-dimensional vector space over the field $\mathbb{F}_2$. The group $\mathrm{Sym}(4)$ is a semidirect product $\mathrm{Sym}(4)=A\leftthreetimes B\leftthreetimes\mathrm{K}_4$, where A is a cyclic group of order 2 and B is a cyclic group of order 3. Let a and b be generators of the groups A and B, respectively; then $b^a=b^{-1}$. Moreover, we may assume[4] that a and b act on K_4 by linear transformations with matrices

$$\begin{pmatrix}1&0\\1&1\end{pmatrix}\qquad\text{and}\qquad\begin{pmatrix}0&1\\1&1\end{pmatrix},$$

respectively. Let $c\in\mathrm{K}_4$; then the value of the derivative of the polynomial $w(x)$ at the point a is

$$\partial w(a)=aba^{-1}+ba^{-1}-a^{-1}=b^{-1}+ba-a=\begin{pmatrix}1&1\\1&0\end{pmatrix}+\begin{pmatrix}0&1\\1&1\end{pmatrix}\begin{pmatrix}1&0\\1&1\end{pmatrix}-\begin{pmatrix}1&0\\1&1\end{pmatrix}=\begin{pmatrix}1&0\\0&0\end{pmatrix}.$$

If G is a finite solvable group, we can define the value of the derivative in the ring of endomorphisms of a certain chief factor of the group G similarly to the case when N is a minimal normal Ω-invariant subgroup of G. Recall that a chief factor of the group G with a system of operators Ω is, by definition, any factor 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 $H\supseteq S\supseteq K$, $H\neq S$, $S\neq K$. Thus, for any polynomial $w(x)$ over G, the action of $w(x)$ on the factor group G/K is well defined: $w(g)=(w\psi)(g)$, where $g\in G/K$ and $\psi\colon G\to G/K$ is a canonical epimorphism. Furthermore, as G is solvable and H/K is a minimal normal Ω-invariant subgroup of G/K, H/K is Abelian and is therefore an elementary Abelian p-group for some prime p. Thus, the values of the derivative ∂w in the rings of endomorphisms of the chief factors are well defined and can be

[4]By choosing an appropriate basis of the vector space associated with K_4.

regarded as matrices over the corresponding finite field $\mathbb{F}_p$. We denote these values as $\partial_{H/K}w(g)$. Note that here we may also take $g \in G$, meaning that $\partial_{H/K}w(g) = \partial_{H/K}w(\psi(g))$. It is clear that "small increment" formulas (10) and (11) hold in this case as well; however, they are identities in the factor group G/K rather than in the group G.

Example 2.3. Consider a group $G = \mathrm{Sym}(3) \leftthreetimes \mathrm{Q}_2$, where the symmetric group Sym(3) (of order 6) acts on the quaternion group Q_2 (of order 8) by outer automorphisms. We recall that $\mathrm{Aut}(\mathrm{Q}_2) \cong \mathrm{Sym}(4)$ and the subgroup $\mathrm{K}_4 \subset \mathrm{Sym}(4)$ is isomorphic to the group of inner automorphisms $\mathrm{Q}_2/\mathrm{Z}(\mathrm{Q}_2)$. The center $\mathrm{Z}(\mathrm{Q}_2)$, which is of order 2, is a fully invariant subgroup in G, and $G/\mathrm{Z}(\mathrm{Q}_2) \cong \mathrm{Sym}(4)$; so $A = \mathrm{Q}_2/\mathrm{Z}(\mathrm{Q}_2)$ is a chief factor of G. As $A \cong \mathrm{K}_4$, A is isomorphic to the additive group of a 2-dimensional vector space over $\mathbb{F}_2$. We can consider the polynomial $w(x)$ from Example 2.1 as a polynomial over G assuming that a is a transposition in Sym(3), b is an element of order 3 in Sym(3), and $c \in \mathrm{Q}_2$. Then, identifying the automorphisms induced by conjugations by a and b with the respective 2×2 matrices over $\mathbb{F}_2$ as in Example 2.2, we conclude that the value $\partial_A w(a)$ of the derivative in the ring of endomorphisms $\mathrm{End}(A)$ of the chief factor A is the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = aba^{-1} + ba^{-1} - a^{-1} = b^{-1} + ba - a = \partial_A w(a).$$

Thus, (11) in this case reads

$$w(ah) \cdot \mathrm{Z}(\mathrm{Q}_2) = w(a)h^{\partial_A w(a)} \cdot \mathrm{Z}(\mathrm{Q}_2)$$

for all $h \in \mathrm{Q}_2$.

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 chief series of a finite nilpotent group are central (i.e., H/K lies in the center of the factor group G/K) and are prime-order groups (say, of order p), the value of the derivative of the polynomial (6) with respect to the ith variable at any point in the ring of endomorphisms of any principal factor is congruent modulo the corresponding p to the degree of the polynomial in the ith variable:

$$\deg_i w(x_1, \dots, x_n) = \sum_{i_j = i} n_j;$$

so the "small increment" formula (10) becomes especially simple:

$$w(g_1h_1, \dots, g_nh_n) = w(g_1, \dots, g_n) \cdot h_1^{\deg_1 w(x_1,\dots,x_n)} \dots h_n^{\deg_n w(x_1,\dots,x_n)} \tag{12}$$

for all $g_1, \dots, g_n \in G$, $h_1, \dots, h_n \in A$, and for every central factor $A = H/K$ of G. Of course, (12) holds in G/K but *not* necessarily in G.

2.2. Bijective polynomials over finite groups. In this subsection, we apply derivations on groups to determining whether a polynomial $w(x)$ over a finite solvable group G is measure-preserving, that is, whether w induces a bijective transformation $g \mapsto w(g)$ on G. Further, in Section 4, we will see that this problem is connected to the following one: Does a polynomial over a profinite group preserve the Haar measure on this group?

Let A be a minimal normal Ω-invariant subgroup of a finite solvable group G with operators Ω; then A is an elementary Abelian p-group for a suitable prime p; i.e., A is isomorphic to the additive group of a vector space over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Thus, for any polynomial $w(x) \in G[x]$ and every $g \in G$ the derivative $\partial w(g)$ is a linear transformation on this vector space. Furthermore, the polynomial $w(x)$ naturally induces a transformation on the factor group G/A: If $\varphi\colon G \to G/A$ is a canonical

epimorphism, this transformation is a well-defined map $w\varphi\colon \varphi(g) \mapsto \varphi(w(g))$, $g \in G$. If this map is a bijection, we will say that w is *bijective modulo the subgroup* A. The following proposition is an immediate consequence of Proposition 1.2 combined with formula (11):

Proposition 2.4. *A polynomial $w(x) \in G[x]$ is bijective on G if and only if the following two conditions hold simultaneously*:

(i) *the polynomial w is bijective modulo A, and*

(ii) *the derivative $\partial w(g)$ induces a nonsingular linear transformation on A for all $g \in G$.*

From here, by easy induction on the length of the chief series of G we deduce the following

Theorem 2.5. *A polynomial $w(x)$ over a finite solvable group G with a set of operators Ω is bijective on G if and only if every matrix $\partial_A w(g)$ is nonsingular for any chief factor A of the group G and any element $g \in G$.*

This theorem is a trivial generalization of the result of Lausch [63], 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.

Corollary 2.6. *If G is a finite nilpotent group (with an empty set of operators), then a polynomial $w(x) \in G[x]$ is bijective on G if and only if its degree is coprime to the order of G.*

Example 2.7. Let G be a symmetric group of degree 4 (with an empty set of operators), and let $w(x) = ax^2bx^{-1}c$, where $a, b, c \in G$. If a, b, and c are as in Example 2.2, then w is not bijective on G since $\partial_A w(g)$ is singular whenever $A = \mathrm{K}_4$ and $g = a$. However, the polynomial $v(x) = ax^2cx^{-1}b$ is bijective on G. Indeed, in the notation of Example 2.2, $\partial_{\mathrm{K}_4} v(g) = b$ and $\partial_A v(g) = \partial_B v(g) = 1$ for all $g \in G$.

3. ERGODIC POLYNOMIALS OVER FINITE GROUPS WITH OPERATORS

In this section, we study ergodic polynomial transformations on finite (noncommutative) groups G with a set of operators Ω; that is, we study transitive transformations of the form (5). Similarly to the commutative case, this problem inevitably leads to ergodic theory for infinite (although profinite) groups endowed with a non-Archimedean metric. The latter theory is considered in Section 4.

The existence of an ergodic polynomial imposes specific constraints both on the group G and on the set of operators Ω. So, at the first stage, we must describe all groups G and sets of operators Ω such that the group G with the set of operators Ω has ergodic polynomials. At the second stage, we must describe these ergodic polynomials. Thus, at the first stage we must prove a group-theoretic analog of Theorem 1.6 and then develop a version of ergodic theory for groups including non-Abelian ones. We will see that the second stage will necessarily force us to consider ergodic (with respect to the Haar measure) transformations on profinite groups endowed with a non-Archimedean metric. Thus, the situation in the noncommutative case resembles the one for the commutative case when the problem of characterization of transitive polynomials over residue rings led us to p-adic ergodic theory on the ring of p-adic integers $\mathbb{Z}_p$.

We restrict our considerations to ergodic polynomials over finite groups since in real-life settings that we currently know only finite groups occur.

3.1. Basic properties of groups having ergodic polynomials. Denote by $\mathcal{G}$ the class of all finite groups G with a set of operators Ω that have ergodic polynomials in one variable, that is, groups for which there exist transitive transformations of the form

$$x \mapsto w(x) = g_1 x^{\omega_1 n_1} g_2 x^{\omega_2 n_2} \dots g_k x^{\omega_k n_k} g_{k+1}, \tag{13}$$

where $g_1, \dots, g_{k+1} \in G$, $\omega_1, \dots, \omega_k \in \Omega$, and $n_1, \dots, n_k \in \mathbb{Z}$. The class $\mathcal{G}$ obviously contains all polynomially complete groups; it is well known that the latter are (except for the group of order 2) all finite simple non-Abelian groups, and vice versa. In other words, any transitive transformation of a finite simple non-Abelian group can be represented by a polynomial over this group, and for applications it is important to find an explicit form of this polynomial. Note that in order to solve an analogous problem for a polynomially complete universal algebra of another kind, namely, for a finite field, we can use interpolation formulas that allow us to express any map of a finite field into itself as a polynomial over this field. However, this solution is of no practical value unless the field is of small order, since constructing the corresponding polynomial via the interpolation formula requires a number of calculations comparable to the order of the field. Arguments of this kind, but only in the superlative degree, are also applicable to polynomials over finite simple non-Abelian groups. Indeed, at present interpolation formulas are only known for one, the smallest, group of this kind, the alternating group Alt(5) of degree 5 (see [64, 13]). However, transitive polynomials that were obtained in this way are of length about 10^4; that is, $k \approx 10^4$ in representation (13) of these polynomials. This is absolutely unacceptable for practical purposes, e.g., for cryptology, especially being compared to the order of the group, which is only 60. There is no hope that in the nearest future somebody will find out whether there exist short transitive polynomials over large finite simple non-Abelian groups, e.g., for $\mathrm{Alt}(n)$, $n > 5$, let alone express these polynomials explicitly.

By virtue of what has been said, it is reasonable to exclude finite simple non-Abelian groups from further consideration. But then, together with these groups, all nonsolvable groups must necessarily be excluded as well. Indeed, suppose that G is a finite nonsolvable group with a set of operators Ω, $w(x)$ is transitive polynomial over G, and N is a fully invariant subgroup; that is, N is closed under the action of all endomorphisms from $\mathrm{End}(G)$. Let $|G : N| = k$. Then it is easy to see that the kth iterate $w^k(x)$ is an ergodic polynomial over the group N considered as a group with the set of operators $\mathrm{End}(N)$ (cf. Proposition 1.2). Furthermore, if K is a fully invariant subgroup in N, then, by Proposition 1.2, $w^k(x)$ induces a transitive polynomial transformation on the factor group N/K. However, since the group G is nonsolvable, there exist fully invariant subgroups N and K such that the factor group N/K is isomorphic to the direct power of a finite simple non-Abelian group H, i.e., $N/K \cong H^m$. Indeed, as G is nonsolvable, at least one factor G_i/G_{i+1} of the composite fully invariant series $G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = \{1\}$ must be non-Abelian. Recall that a series is called fully invariant if every G_i is a fully invariant subgroup in G; a series is composite if G_{i+1} is a maximal fully invariant subgroup of G that is a subgroup of G_i. So G_i/G_{i+1} is a minimal fully invariant subgroup in G_{i-1}/G_{i+1}. However, a minimal fully invariant subgroup of a finite group is isomorphic to a direct power of a simple group, either Abelian or non-Abelian. This means that if we know how to construct an ergodic polynomial $w(x)$ over the finite nonsolvable group G (with some set of operators), then we can also construct an m-dimensional ergodic polynomial transformation on the finite simple non-Abelian group H (with operators). But the arguments used above show that there is no hope of solving the latter problem in the nearest future. Hence, all finite groups for which we may hope to explicitly find transitive polynomials must not contain simple non-Abelian sections[5]; thus, we have to restrict our considerations to solvable groups only.

Now we state some important properties of groups having transitive polynomials.

Proposition 3.1. *Let G be a finite group with a set of operators Ω, let $w(x)$ be a transitive polynomial on G, let N be an Ω-invariant normal subgroup of G, and let $|G : N| = k$. Then the following is true*:

1. *The polynomial $w^k(x)$ is transitive on the group N, which is considered as a group with a set of operators Ω.*

[5]Recall that a *section* of a group is a factor group of a subgroup.

2. *The polynomial* $(w\varphi)(x)$, *where* φ *is a canonical epimorphism of* G *onto* G/N, *is transitive on the group* G/N, *which is considered as a group with a set of operators* Ω.
3. *The subgroup* N *is a normal* Ω*-invariant closure of some* $g \in N$; *that is,* N *is a minimal subgroup of* G *that contains all* $g^{h\omega}$, *where* $h \in G$ *and* $\omega \in \Omega$.[6]
4. *If* N *is Abelian, then either* N *is a cyclic group or* N *is isomorphic to the direct product of the Klein group* K_4 *by a cyclic group* $\mathrm{C}(m)$ *of odd order* m, $m \in \mathbb{N}$ (*i.e., the case* $m = 1$ *is also possible*).
5. *If* $N \cong \mathrm{K}_4$, *then there exists either an element* $a \in G$ *or an operator* $\alpha \in \Omega$ *that acts on* N *as an automorphism of order* 2.

Claims 1 and 2 of Proposition 3.1 in combination with Proposition 1.2 can serve as a tool to determine whether a given polynomial $w(x)$ is transitive on a finite group G. The following obvious corollary holds:

Corollary 3.2. *Let* G, N, φ, *and* k *be the same as in Proposition* 3.1. *Then a polynomial* $w(x)$ *is transitive on* G *if and only if the polynomial* $(w\varphi)(x)$ *is transitive on* G/N *and* $w^k(x)$ *is transitive on* N.

Using Corollary 3.2, we are able to determine whether a polynomial $w(x)$ is transitive on a solvable group G: We first verify whether $(w\varphi)(x)$ is transitive on the factor group G/G', where $\varphi\colon G \to G/G'$ is a canonical epimorphism; then we verify whether $(w^k\psi)(x)$ is transitive on the factor group G'/G'', where $\psi\colon G \to G/G''$ is a canonical epimorphism and $k = |G : G'|$, etc.

Example 3.3. The polynomial $w(x) = ax^2uvx^5b$ is transitive on the symmetric group $\mathrm{Sym}(4)$ whenever $\mathrm{Sym}(4)$ is represented as a semidirect product $A \leftthreetimes B \leftthreetimes \mathrm{K}_4$, where A is a cyclic subgroup of order 2 with a generator a, B is a cyclic subgroup of order 3 with a generator b, $\mathrm{K}_4 = \{1, u, v, uv\}$ is the Klein group of order 4, $b^a = b^{-1}$, $u^a = u$, $v^a = uv$, $u^b = v$, and $v^b = uv$.

Indeed, $(w\varphi)(x) = ax^7b$, where $\varphi\colon \mathrm{Sym}(4) \to \mathrm{Sym}(4)/\mathrm{K}_4 = A \leftthreetimes B \cong \mathrm{Sym}(3)$ is an epimorphism. As $\#\mathrm{Sym}(3) = 6$, the polynomial $(w\varphi)(x)$ induces the same transformation on the factor group $\mathrm{Sym}(4)/\mathrm{K}_4$ as the polynomial $\overline{w}(x) = axb$ on the group $A \leftthreetimes B$. Since every element from $A \leftthreetimes B$ has a unique representation in the form a^ib^j, where $i \in \mathbb{Z}/2\mathbb{Z}$ and $j \in \mathbb{Z}/3\mathbb{Z}$, the polynomial $\overline{w}(x)$ is transitive on $A \leftthreetimes B$.

Now we calculate $w^6(h)$ for $h \in \mathrm{K}_4$. Using derivation formulas from Subsection 2.1, for $s \in A \leftthreetimes B \subset \mathrm{Sym}(4)$ we obtain $w(sh) = w(s)h^{\partial w(s)} = \overline{w}(s) \cdot (uv)^{s^5b} \cdot h^{\partial w(s)}$; hence for $i = 1, 2, \dots$ we have

$$w^i(sh) = \overline{w}^i(s) \cdot (uv)^{\sum_{k=0}^{i-1}(\overline{w}^k(s))^5 \cdot b \cdot \prod_{\ell=k+1}^{i-1} \partial w(\overline{w}^\ell(s))} \cdot h^{\prod_{k=0}^{i} \partial w(\overline{w}^k(s))}.$$

Note that the products in this formula are not commutative; e.g.,

$$(\overline{w}^k(s))^5 \cdot b \cdot \prod_{\ell=k+1}^{i-1} \partial w(\overline{w}^\ell(s)) = (\overline{w}^k(s))^5 \cdot b \cdot \partial w(\overline{w}^{k+1}(s)) \cdot \partial w(\overline{w}^{k+2}(s)) \dots \partial w(\overline{w}^{i-1}(s))$$

in that order (we assume as usual that a product over an empty set of indices is 1). Note that we make all these calculations in the ring $\mathrm{End}(\mathrm{K}_4)$ of all endomorphisms of the group K_4. As the latter group is merely the additive group of the 2-dimensional vector space over the two-element field $\mathbb{F}_2$, we may actually work with 2×2 matrices over $\mathbb{F}_2$: We arbitrarily choose a basis in this vector space, for instance, associating $u \in \mathrm{K}_4$ with the vector $(1, 0)$ and $v \in \mathrm{K}_4$ with the vector $(0, 1)$; then, as $u^b = v$ and $v^b = uv$, we associate, e.g., the element b with the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$. Alternatively, rather than working with matrices, we can perform multiplications in $\mathrm{Aut}(\mathrm{K}_4) = A \leftthreetimes B$ and perform

[6] Everywhere in this section we assume that Ω contains the identity operator Id.

additions with the use of the following relations that hold in the (noncommutative) ring $\mathrm{End}(\mathrm{K}_4)$ of all endomorphisms of the group K_4:

$$\alpha_1+\alpha_1+\alpha_3=0, \qquad \alpha_1,\alpha_1,\alpha_3 \text{ are automorphisms of order 2 of } \mathrm{K}_4, \tag{14}$$

$$\beta_1+\beta_2+1=0, \qquad \beta_1,\beta_2 \text{ are automorphisms of order 3 of } \mathrm{K}_4. \tag{15}$$

Here 1 stands for the identity automorphism, and 0, for the zero endomorphism of the group K_4 (i.e., $g^1=g$ and $g^0=1$ for all $g\in\mathrm{K}_4$). Recall that the group K_4 is isomorphic to the additive group of the 2-dimensional vector space over the field $\mathbb{F}_2$, so $\mathrm{End}(\mathrm{K}_4)$ is isomorphic to the algebra of all 2×2 matrices over $\mathbb{F}_2$; hence, the above-mentioned identities can be verified directly. As a and b are just automorphisms of respective orders 2 and 3 in $\mathrm{Aut}(K_4)$ (which are induced by conjugation by $a,b\in\mathrm{Sym}(4)$), relations (14) and (15) of the ring $\mathrm{End}(\mathrm{K}_4)$ can be rewritten in the following form:

$$ab^2+ab+a=0, \tag{16}$$

$$b^2+b+1=0. \tag{17}$$

Using either of these ways, we calculate the values of the derivative $\partial w(t)=(t+1)t^5b+(t^4+t^3+t^2+t+1)b$ for relevant $t=\overline{w}^i(1)$ and finally obtain

$$w^6(h)=(uv)^{b^2+ab^2}h^a=vuh^a.$$

However, by Remark 1.4, the transformation $h\mapsto vuh^a$ is transitive on K_4. By Proposition 1.2 this finally proves that the polynomial $w(x)=ax^2uvx^5b$ is transitive on $\mathrm{Sym}(4)$.

3.2. Finite solvable groups having ergodic polynomials. In this subsection, we characterize finite solvable groups (with operators) having ergodic polynomials. First, we consider the multivariate case. We characterize finite solvable groups G with a system of operators Ω such that there exist a transitive transformation $W=(w_1,\dots,w_n)\colon G^n\to G^n$, where $w_1,\dots,w_n$ are polynomials in n variables.

3.2.1. *The multivariate case.* It turns out that actually only univariate or bivariate transitive polynomial transformations may exist over finite solvable groups with operators:

Proposition 3.4. *Let G be a finite solvable group with a system of operators Ω. If the map $W=(w_1,\dots,w_n)\colon G^n\to G^n$ is transitive, where $w_1,\dots,w_n$ are polynomials in variables $x_1,\dots,x_n$ over the group G with operators Ω, then either $n=1$, or $n=2$ and $\#G=2$.*

Now, to characterize finite solvable groups (with operators) having ergodic polynomials, we can restrict our considerations to univariate polynomials. 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 a system of operators Ω not only restricts the possible structure of the group G, but also imposes certain constraints on Ω. A transitive polynomial may exist for a given group G with one system of operators and may not exist for the same group G with another 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 $\mathrm{Aut}(\mathrm{K}_4)$ 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 has no ergodic polynomial by Theorem 1.3. Therefore, in order to characterize all finite solvable groups with operators that have ergodic polynomials, it is reasonable to do the following. We should first try to find a description of all finite solvable groups G that admit ergodic polynomial functions and possess a 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 another way, $\Omega = \mathrm{End}(G)$, where $\mathrm{End}(G)$ 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 $\Omega = \mathrm{End}(G)$ and, in particular, for every ergodic polynomial w make a list $\mathrm{E}(w)$ of endomorphisms ω that occur in the canonical representation (5) of the polynomial w. Then the final formulation of the corresponding classification theorem will be as follows: A finite solvable group G with a system of operators Ω has ergodic polynomials if and only if the group G with the system of operators $\mathrm{End}(G)$ has ergodic polynomials and Ω induces on G all endomorphisms from $\mathrm{E}(w)$ for a certain ergodic polynomial w over the group G with the system of operators $\mathrm{End}(G)$. In other words, actually we must describe all finite solvable groups G with operators $\Omega = \mathrm{End}(G)$ having ergodic polynomials, and then describe all ergodic polynomials over every such group.

The corresponding classification theorem may be proved, although the proof would require significant technical efforts and split into a number of separate cases. Actually the proof does not yet exist since the significance of such a general theorem for applications is questionable in our view. However, to demonstrate methods of proof, we consider further in this paper several cases that look the most instructive and also may be useful in applications to cryptography and computer science. Namely, we will describe solvable groups G having transitive polynomials in three cases, $\Omega = \varnothing$, $\Omega = \mathrm{Aut}(G)$, and $\Omega = \mathrm{End}(G)$. So denote by $\mathcal{C}_0$, $\mathcal{C}_\mathrm{A}$, and $\mathcal{C}_\mathrm{E}$ the classes of all finite groups with the systems of operators $\Omega = \varnothing$, $\Omega = \mathrm{Aut}(G)$, and $\Omega = \mathrm{End}(G)$, respectively, that have ergodic polynomials. Clearly, $\mathcal{C}_0 \subseteq \mathcal{C}_\mathrm{A} \subseteq \mathcal{C}_\mathrm{E}$. When describing solvable $\mathcal{C}_0$-, $\mathcal{C}_\mathrm{A}$-, and $\mathcal{C}_\mathrm{E}$-groups, we will mainly follow the paper [2].

After we determine solvable groups in all these three classes, we describe ergodic (i.e., transitive) polynomials over some of these groups that we consider the most important in view of possible applications. The latter problem turns out to be a problem of characterization of polynomial ergodic transformations on infinite pro-2-groups endowed with a non-Archimedean metric.

We note that part of the work is already done in the paper [49], which studies the so-called *single orbit groups*. Recall that the latter are groups G having transitive affine transformations, i.e., transitive transformations of the form $x \mapsto ax^\alpha$, where $a \in G$ and $\alpha \in \mathrm{Aut}(G)$. It turns out that all these finite groups are extensions of cyclic groups by cyclic groups: They have cyclic normal subgroups such that the corresponding factor groups are cyclic. Groups of this type are called *cyclic-by-cyclic* or *metacyclic groups*; note that the derived length of every such group is 2 whenever the group is non-Abelian. The paper [49] also describes automorphisms α that occur in transitive affine transformations of these groups.

As we will see, all three classes of solvable $\mathcal{C}_0$-, $\mathcal{C}_\mathrm{A}$-, and $\mathcal{C}_\mathrm{E}$-groups are wider than the class of finite single orbit groups: There are a number of finite solvable groups that have ergodic (i.e., transitive) polynomials but do not have transitive affine transformations.

3.2.2. *The univariate case*: *Nilpotent groups.* Now we determine which finite nilpotent groups G with operators Ω have transitive polynomials for the cases $\Omega = \varnothing$, $\Omega = \mathrm{Aut}(G)$, and $\Omega = \mathrm{End}(G)$; i.e., we find all nilpotent groups in the classes $\mathcal{C}_0$, $\mathcal{C}_\mathrm{A}$, and $\mathcal{C}_\mathrm{E}$. Here and in what follows we represent groups by generators and relations, if necessary. For instance, the cyclic group $\mathrm{C}(m)$ of order m generated by c will be written as $\mathrm{C}(m) = \mathrm{gp}(c \parallel c^m = 1)$.

The following theorem is true:

Theorem 3.5. *A finite nilpotent group lies in $\mathcal{C}_\mathrm{E}$ if and only if it is either trivial or isomorphic to one of the following groups*:

(1) *the cyclic group* $\mathrm{C}(m)$ *of order* m, $m = 1, 2, 3, \ldots$;

(2) *the Klein group* K_4;

(3) *the dihedral group* $\mathrm{D}_n = \mathrm{gp}(u, v \parallel u^2 = v^{2^n} = 1,\ v^u = v^{-1})$ *of order* 2^{n+1}, $n = 2, 3, 4, \ldots$;

(4) *the (generalized) quaternion group* $\mathrm{Q}_n = \mathrm{gp}(u, v \parallel v^{2^n} = 1, v^u = v^{-1}, u^2 = v^{2^{n-1}})$ *of order* 2^{n+1}, $n = 2, 3, 4, \dots$;

(5) *the semidihedral group* $\mathrm{SD}_n = \mathrm{gp}(u, v \parallel u^2 = v^{2^n} = 1, v^u = v^{2^{n-1}-1})$ *of order* 2^{n+1}, $n = 3, 4, 5, \dots$;

(6) *the direct product* $H \times \mathrm{C}(m)$, *where* H *is a group of type* (2), (3), (4), *or* (5) *and* $m > 1$ *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* $\mathcal{C}_\mathrm{A}$. *Finally, the class* $\mathcal{C}_0$ *consists exactly of all cyclic groups* $\mathrm{C}(m)$, $m = 1, 2, 3, \dots$.

Remark 3.6. Note that Theorem 3.5, together with the results of [49], implies that all $\mathcal{C}_\mathrm{A}$-groups are single orbit groups, whereas $\mathcal{C}_\mathrm{E}$-groups are not: Semidihedral groups SD_n lie in $\mathcal{C}_\mathrm{E} \setminus \mathcal{C}_\mathrm{A}$.

3.2.3. *The univariate case: Solvable groups.* Here we determine which finite solvable groups G with operators Ω have transitive polynomials for the cases $\Omega = \varnothing$, $\Omega = \mathrm{Aut}(G)$, and $\Omega = \mathrm{End}(G)$; i.e., we find all solvable groups in the classes $\mathcal{C}_0$, $\mathcal{C}_\mathrm{A}$, and $\mathcal{C}_\mathrm{E}$. It turns out that there are not too many types of finite solvable nonnilpotent groups of this kind. Loosely speaking, these groups are either noncyclic metacyclic groups or extensions of (meta)cyclic groups by groups that in some sense "look like" either a symmetric or an alternating group of degree 4. Moreover, the derived lengths of all $\mathcal{C}_\mathrm{E}$-groups are not greater than 3, although from Theorem 3.5 we know that there exist nilpotent $\mathcal{C}_\mathrm{E}$-groups of arbitrarily large class.

In order to formulate the corresponding theorem, we introduce the following groups:

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

Here $m, k = 2, 3, 4, \dots$, $s \not\equiv 1 \pmod k$, $s^m = 1 \pmod k$, and m and k are coprime; so $\mathrm{M}(m, k, s) = \mathrm{C}(m) \leftthreetimes \mathrm{C}(k)$. These groups are metacyclic and, thus, metabelian, i.e., solvable of derived length exactly 2. Note that we assume that the groups $\mathrm{M}(m, k, s)$ are non-Abelian (otherwise $s = 1$ and the group is cyclic, $\mathrm{C}(mk)$). It is clear that all Sylow p-subgroups of these groups $\mathrm{M}(m, k, s)$ are cyclic: If p^n is the maximum power of a prime p that divides mk, then either $p^n \mid m$ or $p^n \mid k$, so the Sylow p-subgroup of $\mathrm{M}(m, k, s)$ is conjugate either to a Sylow p-subgroup of the group $\mathrm{C}(m)$ or to a Sylow p-subgroup of the group $\mathrm{C}(k)$. Furthermore, these groups $\mathrm{M}(m, k, s)$ form a class of the so-called *Z-groups*, i.e., finite groups whose Sylow p-subgroups are all cyclic, for every prime $p \mid mk$ (see, e.g., [96]). As $\mathrm{C}(m) \leftthreetimes \mathrm{C}(k) = (\mathrm{C}(m_1) \times C) \leftthreetimes \mathrm{C}(k) = \mathrm{C}(m_1) \leftthreetimes (\mathrm{C}(k) \times C)$, where C is the direct product of all Sylow p-subgroups of $\mathrm{C}(m)$ that centralize the subgroup $\mathrm{C}(k)$, different triples m, k, s may correspond to isomorphic groups. Among all representations of a Z-group G as a semidirect product of cyclic groups of coprime orders, one is distinguished: $G = \mathrm{C}(m) \leftthreetimes \mathrm{C}(k)$ with $\mathrm{Z}(G) \cap \mathrm{C}(k) = \{1\}$; so the action of the generator of $\mathrm{C}(m)$ on $\mathrm{C}(k)$ fixes only one element from $\mathrm{C}(k)$, namely, 1. This representation will be referred to as a *canonical representation of a Z-group* and denoted by $\mathrm{Z}(m_1, k_1, s_1)$; so $\mathrm{M}(m, k, s) \cong \mathrm{Z}(m_1, k_1, s_1)$ for suitable m_1, k_1, and s_1. From [96, Proposition 12.11] it follows, in particular, that $s_1 - 1$ is coprime to k_1. Note that $\mathrm{M}(2, 3, 2) = \mathrm{Z}(2, 3, 2) = \mathrm{Sym}(3)$ is a symmetric group of degree 3.

- $\mathrm{A}(r) = \mathrm{gp}(b, u, v \parallel b^{3^r} = u^2 = v^2 = 1, uv = vu, u^b = v, v^b = uv)$.

The group $\mathrm{A}(r)$ is a split extension of the Klein group K_4 by a cyclic group of order 3^r, $r = 1, 2, 3, \dots$: $\mathrm{A}(r) = \mathrm{C}(3^r) \leftthreetimes \mathrm{K}_4$. The group $\mathrm{A}(r)$ is solvable of derived length 2, i.e., is a metabelian group; in particular, $\mathrm{A}(1) = \mathrm{Alt}(4)$, the alternating group of degree 4.

- $\mathrm{S}(r) = \mathrm{gp}(a \parallel a^2 = 1) \leftthreetimes \mathrm{A}(r)$, $r = 1, 2, 3, \dots$.

Here $b^a = b^{-1}$, $u^a = u$, and $v^a = uv$. This group is a split extension of the group $\mathrm{A}(r)$ by the cyclic group $\mathrm{C}(2)$ of order 2. The derived length of $\mathrm{S}(r)$ is 3; in particular, $\mathrm{S}(1) = \mathrm{Sym}(4)$ is a symmetric group of degree 4.

- $\mathrm{AQ}(r) = \mathrm{gp}(b \parallel b^{3^r} = 1) \leftthreetimes \mathrm{Q}_2$, $r = 1, 2, 3, \dots$.

Here $u^b = v^{-1}$ and $v^b = uv^{-1}$. The group $\mathrm{AQ}(r)$ is a split extension of the quaternion group Q_2 of order 8 by a cyclic group $\mathrm{C}(3^r)$ of order 3^r. The group $\mathrm{AQ}(r)$ is a metabelian group.

- $\mathrm{SQ}_1(r) = \mathrm{gp}(a \parallel a^2 = 1) \leftthreetimes \mathrm{AQ}(r)$, $r = 1, 2, 3, \ldots$.

Here $b^a = b^{-1}$, $u^a = u^{-1}$, and $v^a = uv$. This group is a solvable group of derived length 3.

- $\mathrm{SQ}_2(r) = \mathrm{gp}(a, b, u, v \parallel b^{3^r} = v^4 = 1,\ b^a = b^{-1},\ u^a = u^{-1},\ v^a = uv,\ u^b = v^u = v^{-1},\ v^b = uv^{-1},\ a^2 = u^2 = v^2)$, $r = 1, 2, \ldots$.

The group $\mathrm{SQ}_2(r)$ is a partial semidirect product of the group $\mathrm{AQ}(r)$ by the cyclic group $A = \mathrm{gp}(a \parallel a^4 = 1)$ of order 4; the amalgamated subgroups (those generated by $a^2 \in A$ and by $u^2 \in \mathrm{Q}_2 \subset \mathrm{AQ}(r)$) are cyclic groups of order 2. The group $\mathrm{SQ}_2(r)$ is a solvable group; its derived length is 3.

Neither of the above groups is nilpotent. These groups are main "building blocks" of solvable groups with operators that have transitive polynomials. It turns out that the latter groups are (semi)direct products of the above groups and of nilpotent groups from Theorem 3.5.

Theorem 3.7. *A finite solvable group lies in $\mathcal{C}_{\mathrm{E}}$ if and only if it is isomorphic to one of the following groups*:

(1) $\mathrm{C}(m)$;

(2) $\mathrm{M}(m, k, s)$;

(3) K_4;

(4) Q_n;

(5) D_n;

(6) SD_n;

(7) $\mathrm{A}(r)$;

(8) $\mathrm{AQ}(r)$;

(9) $\mathrm{S}(r)$;

(10) $\mathrm{SQ}_1(r)$;

(11) $\mathrm{SQ}_2(r)$;

(12) $A \leftthreetimes B$, *where the orders of the groups A and B are coprime, A is any group of types* (3)–(11), *and B is any group of type* (1) *or* (2).

Out of these groups, the following groups lie in $\mathcal{C}_{\mathrm{A}}$: All groups that are isomorphic to groups of types (1)–(5), (7)–(11) *and all groups that are isomorphic to certain groups of type* (12), *namely, to groups of the following types* (13)–(15):

(13) $A \times B$, *where A is any group of types* (3)–(5), (7)–(11) *and B is any group of type* (1) *or* (2);

(14) *A is any group of types* (3)–(5), *B is any group of type* (1) *or* (2), *A acts on B by an automorphism of order* 2, *and the centralizer of B in A is cyclic*[7];

(15) *A is any group of types* (9)–(11), *and B is any group of type* (1) *or* (2).

Finally, out of these groups, exactly all groups that are isomorphic to groups of types (1), (2), (9)–(11), *and* (15) *lie in $\mathcal{C}_0$.*

[7] This means that if A is either a dihedral group or a generalized quaternion group of order > 8, the centralizer is a subgroup generated by v; see the representation of these groups by generators and relations in the statement of Theorem 3.5.

4. ERGODIC THEORY FOR PROFINITE GROUPS

In this section, we develop ergodic theory for polynomials over profinite groups. Actually we consider groups (with operators) that can be approximated by finite solvable groups. These groups can be naturally endowed with a non-Archimedean metric and a probabilistic measure, the normalized Haar measure. Polynomials over these groups induce continuous and measurable transformations on these groups, and we study conditions under which these transformations are measure-preserving or ergodic.

The main problem we are concerned with is how to determine bijective and/or transitive polynomials over finite groups with operators. In this section we will see that this problem leads to the question of how to determine measure-preserving/ergodic polynomial transformations on a profinite group. As a matter of fact, we will act in a manner similar to that we proceeded during the study of ergodic polynomial transformations over residue rings. In the latter case, we considered a spectrum of residue rings modulo p^k, $k = 1, 2, \dots$, p prime,

$$\dots \xrightarrow{\bmod p^{k+1}} \mathbb{Z}/p^{k+1}\mathbb{Z} \xrightarrow{\bmod p^k} \mathbb{Z}/p^k\mathbb{Z} \xrightarrow{\bmod p^{k-1}} \dots \xrightarrow{\bmod p} \mathbb{Z}/p\mathbb{Z},$$

where the projection epimorphisms are the reductions modulo p^k. The inverse limit of this spectrum is the ring $\mathbb{Z}_p$ of p-adic integers

$$\mathbb{Z}_p = \varprojlim_{k\to\infty} \mathbb{Z}/p^k\mathbb{Z},$$

and Theorem 1.8 states that a 1-Lipschitz transformation on $\mathbb{Z}_p$ is ergodic if and only if it is transitive modulo p^k (i.e., ergodic on $\mathbb{Z}/p^k\mathbb{Z}$) for all $k = 1, 2, \dots$. In particular, the corresponding result for polynomials (Corollary 1.11) is as follows: a polynomial over $\mathbb{Z}_p$ is ergodic if and only if it is transitive modulo p^3 for $p \in \{2, 3\}$ or modulo p^2 for other p. A practical impact of this result is that if one needs to determine whether a polynomial is transitive modulo p^k, where k is large, he only has to determine whether it is transitive on a much smaller set, of order p^3. This is a general effect that follows from the compatibility of polynomial maps and from the properties of the measure on $\mathbb{Z}_p$. In this section, we demonstrate that a similar effect takes place for noncommutative algebraic structures, namely, for non-Abelian groups with operators. We prove a group-theoretic analog of the result on ergodic polynomials over p-adic integers for polynomials over the inverse limits of finite solvable groups. We also develop a similar technique to determine measure-preserving polynomials. The difference between these two cases is that measure-preserving polynomials exist over the inverse limits of arbitrary finite solvable groups, whereas ergodic polynomials exist only over the inverse limits of some special finite solvable groups, namely, those described in Theorem 3.7.

4.1. Metric and measure on a profinite group. First, following [58], we recall some facts about profinite groups. Let

$$\dots \xrightarrow{\varphi_{n+1}} G_n \xrightarrow{\varphi_n} G_{n-1} \xrightarrow{\varphi_{n-1}} \dots \xrightarrow{\varphi_1} G_0 \xrightarrow{\varphi_0} \{1\}$$

be an inverse spectrum of groups G_n, $n = 0, 1, 2, \dots$, and let

$$G_\infty = \varprojlim_{n\to\infty} G_n$$

be the corresponding inverse limit. That is, the group G_∞ possesses an (infinite) decreasing chain of normal subgroups $G_\infty \rhd N_n$,

$$G_\infty \rhd N_0 \rhd N_1 \rhd N_2 \rhd \dots \rhd \{1\}$$

such that $G_\infty/N_n = G_n$, $\bigcap_{n=0}^\infty N_n = \{1\}$, and $\ker\varphi_n = N_{n-1}/N_n$, $n = 1, 2, \dots$. The group G_∞ is said to be *profinite* if all N_n are of finite indices, that is, if all G_n are finite groups, $n = 0, 1, 2, \dots$. A profinite group G_∞ can be endowed with a natural topology, a *profinite topology*, where $\mathcal{N} = \{N_n\colon n = 0, 1, 2, \dots\}$ form a base of open neighborhoods of 1, and so all cosets with respect to all these normal subgroups N_n form a base of this topology. The group G_∞ is compact with respect to this topology. Moreover, if $\mathfrak{B}$ is the smallest σ-algebra containing the compact subsets of G_∞, then there is a unique measure μ on $\mathfrak{B}$ such that $\mu(gS) = \mu(Sg) = \mu(S)$ for $g \in G_\infty$ and $S \in \mathfrak{B}$, μ is regular, and $\mu(G_\infty) = 1$. The measure μ is the (normalized) Haar measure on G_∞; actually μ is a natural probability measure on G_∞. Now, given a measurable transformation $g \mapsto w(g)$, $g \in G_\infty$ (where, e.g., $w(x) \in G_\infty[x]$ is a polynomial over G_∞), we may consider whether this transformation is measure-preserving or ergodic with respect to μ. Note that a polynomial transformation of G_∞ is a measurable transformation as it is a composition of multiplications, which are measurable. Furthermore, the group G_∞ can be endowed with a metric d that agrees with the profinite topology on G_∞ and is a non-Archimedean metric. If $\pi_n\colon G_\infty \to G_\infty/N_n$ is a canonical epimorphism, put

$$d(x, y) = 2^{-\ell}, \qquad \text{where} \quad \ell = \min\{n\colon \pi_n(x) \neq \pi_n(y)\},$$

and $d(x, y) = 0$ if $\pi_n(x) = \pi_n(y)$ for all $n \geq 0$. Note that given a sequence $\mathcal{G} = (g_n \in G_n)_{n=0}^\infty$ such that $\varphi_n(g_n) = g_{n-1}$ for all $n = 1, 2, \dots$, we consider a sequence $\mathcal{G}' = (g'_n \in G_\infty)_{n=0}^\infty$ such that $\pi_n(g'_n) = g_n$ for all $n = 0, 1, 2, \dots$. The latter sequence $\mathcal{G}'$ converges with respect to the metric d to some element $g \in G_\infty$, which has the following property: $\pi_n(g) = g_n$ for all $n = 0, 1, 2, \dots$. The element $g \in G_\infty$ does not depend on the choice of representatives g'_n in cosets with respect to the normal subgroups N_n; so we call the element g a *limit* of the sequence $\mathcal{G} = (g_n \in G_n)_{n=0}^\infty$. Every element $g \in G_\infty$ is then a limit (in this sense) of a suitable sequence $(g_n \in G_n)_{n=0}^\infty$ such that $\varphi_n(g_n) = g_{n-1}$, $n = 1, 2, \dots$.

Further, if $f\colon G_\infty \to G_\infty$ is a compatible map (i.e., $f(gN) \subset f(g) \cdot N$ for every $g \in G_\infty$ and $N \lhd G_\infty$), then the map $f \bmod N\colon \pi(g) \mapsto \pi(f(g))$, $g \in G_\infty$, where $\pi\colon G_\infty \to G_\infty/N$ is a canonical epimorphism, is a well-defined map of G_∞/N into G_∞/N; so we may speak of *bijectivity and transitivity of the map f modulo the normal subgroup N* meaning the bijectivity (respectively, transitivity) of the map $f \bmod N\colon G_\infty/N \to G_\infty/N$. As usual, when we speak about maps induces by polynomials, we do not distinguish between polynomials and the respective polynomial maps; so in what follows we speak of measure-preserving, ergodic, transitive, etc. polynomials meaning the respective properties of the corresponding polynomial maps. The following analog of Theorem 1.8 holds:

Theorem 4.1 [58]**.** *Let $w(x) \in G_\infty[x]$ be a polynomial over a profinite group G_∞. Then, the following statements are equivalent*:

- *w is measure-preserving with respect to the Haar measure μ;*
- *w is bijective modulo N_n for all $n = 0, 1, 2, \dots$;*
- *w is an isometry with respect to the metric d.*

Also, the following statements are equivalent:

- *w is ergodic with respect to μ;*
- *w is transitive modulo N_n for all $n = 0, 1, 2, \dots$.*

Theorem 4.1 is a special case of [58, Theorem 1.1]; we refer the reader to [58] for proofs and more detailed information on topological, metric, and other relevant properties of profinite groups. We note that similar statements remain true for groups with a set of operators Ω; we only must consider Ω-invariant normal subgroups rather then ordinary normal subgroups.

4.2. Equations, noncommutative Hensel's lemma, and measure-preserving polynomials over profinite groups. Let $w(x)$ be a polynomial over the profinite group G_∞ from Subsection 4.1. We wonder how to determine whether there exists a solution of the equation $w(x)=1$ in G_∞, i.e., whether there exists $g\in G_\infty$ such that $w(g)=1$, a "root of the polynomial $w(x)$." It is clear that such g exists if and only if the equation $w(x)=1$ is solvable in all G_n, that is, if and only if there exist $g_n\in G_n$ such that $(w\pi_n)(g_n)=1$ in G_n for all $n=0,1,2,\dots$. Indeed, if for every $n=0,1,2,\dots$ we denote $R_n=\{g\in G_\infty\colon \pi_n(w(g))=1\}$, then R_n is closed in G_∞ with respect to the profinite topology, these R_n form a nested sequence (i.e., $R_{n+1}\subset R_n$ for all $n=0,1,2,\dots$), and the intersection $R=\bigcap_{n=0}^{\infty}R_n$ is nonempty (see, e.g., [60, Ch. 3, Section 34, I]).

In the notation of Subsection 4.1, let G_∞ be the inverse limit of finite solvable groups G_n, $n=0,1,2,\dots$. We may assume that $A_n=N_n/N_{n+1}$ is a minimal normal subgroup in $G_{n+1}=G_\infty/N_{n+1}$ for all $n=0,1,2,\dots$; otherwise we make corresponding refinements. Thus, every A_n is an elementary Abelian p_n-group for a suitable prime p_n. Denote by $\psi_n=\varphi_1\circ\ldots\circ\varphi_n\colon G_n\to G_0$ the composition of epimorphisms $\varphi_n,\dots,\varphi_1$. Then the following analog of Hensel's lemma for profinite groups holds:

Proposition 4.2. *If the equation $w(x)=1$, where $w(x)\in G_\infty[x]$, has a solution g_0 modulo N_0 (i.e., $(w\pi_0)(g_0)=1$ in G_0) and if for all $n=0,1,2,\dots$ the derivative $\partial_{A_n}w(g_0')$ is a nonsingular matrix over $\mathbb{F}_{p_n}$ for some (equivalently, for any) $g_0'\in\psi_{n+1}^{-1}(g_0)$, then this equation has a solution $g\in G_\infty$ such that $\pi_0(g)=g_0$.*

Proof. Induction on n shows that for any $n=1,2,\dots$ there exists a solution $g_n\in G_n$ of the equation $(w\pi_n)(x)=1$ such that $\psi_n(g_n)=g_0$. Indeed, if $g_n\in G_n$, $(w\pi_n)(g_n)=1$, and $\psi_n(g_n)=g_0$, then $(w\pi_{n+1})(g_n')\in A_n$ for any $g_n'\in\varphi_n^{-1}(g_n)$; thus, in view of (11), we can choose $h\in A_n$ so that $(w\pi_{n+1})(g_n'h)=1$, and then put $g_{n+1}=g_n'h$.

It is now obvious that the sequence g_n has a limit $g\in G_\infty$ and that g is the required solution. □

From the proof of Proposition 4.2, with the use of (12) we immediately deduce the following:

Corollary 4.3. *If, under the conditions of Proposition 4.2, all groups G_n are p-groups for some prime p and if $p\nmid\deg w$, then the equation $w(x)=1$ has a solution in G_∞.*

The latter result has interesting connections with the 2-adic dynamics: Now we can solve functional equations in the group $\mathrm{Syl}_2(\infty)$ of 1-Lipschitz measure-preserving transformations on the space $\mathbb{Z}_2$ of 2-adic integers. The latter group is the inverse limit of 2-groups (of orders 2^{2^n-1}, $n=1,2,\dots$). Actually this group is isomorphic to a Sylow 2-subgroup $\mathrm{Syl}_2(2^n)$ of the symmetric group $\mathrm{Sym}(2^n)$ of all permutations on $\mathbb{Z}/2^n\mathbb{Z}$.

Example 4.4. Given arbitrary measure-preserving transformations a and b on $\mathbb{Z}_2$, every 1-Lipschitz measure-preserving transformation g on $\mathbb{Z}_2$ can be represented as $f(a(f(b(f(x)))))=g(x)$ for a suitable 1-Lipschitz measure-preserving transformation f on $\mathbb{Z}_2$.

Indeed, we can rewrite this representation as an equation $f\circ a\circ f\circ b\circ f=g$ for the unknown f in the group $\mathrm{Syl}_2(\infty)$, where $\circ$ stands for the composition of transformations. The conclusion now follows from Corollary 4.3.

To conclude, we note that combining Theorem 4.1 and Theorem 2.5, we obviously obtain a criterion for determining measure-preserving polynomials over the profinite group G_∞, which is the inverse limit of finite solvable groups G_n:

Theorem 4.5. *A polynomial $w(x)\in G_\infty[x]$ is measure-preserving if and only if it is bijective modulo the subgroup N_0 and all derivatives $\partial_{A_n}w(g)$ are nonsingular matrices over $\mathbb{F}_{p_n}$ for all $g\in G_{n+1}$ and all $n=0,1,2\dots$.*

Remark 4.6. Theorem 4.5 remains true if G_∞ is a group with a nonempty set of operators Ω; we must only consider Ω-invariant minimal normal subgroups A_n rather than merely minimal normal subgroups.

Corollary 4.7. *If, under the conditions of Theorem* 4.5, *all* G_n *are* p*-groups for some prime* p, *then the polynomial* $w(x)$ *is measure-preserving if and only if* $p \nmid \deg w$.

Proof. We may assume that G_0 is an (Abelian) group of order p; otherwise we make refinements to the inverse spectrum using the chief series of G_0. Furthermore, we may assume that all $N_n/N_{n+1} \in \mathrm{Z}(G_n)$ for the same reason. Thus, $\partial_{A_n} w(g) = \deg w$ for all $g \in G_{n+1}$, $n = 0, 1, 2, \dots$, and $(w\pi_0)(g) = (w\pi_0)(1) \cdot g^{\deg w}$ for all $g \in G_0$. However, given $a \in G_0$, the equation $(w\pi_0)(1) \cdot x^{\deg w} = a$ in the unknown x has a solution in G_0 if and only if $p \nmid \deg w$. $\square$

In view of Example 4.4 the following assertion is obvious:

Example 4.8. For arbitrary 1-Lipschitz measure-preserving transformations $a, b, c, d \in \mathrm{Syl}_2(\infty)$ on $\mathbb{Z}_2$, the polynomial $axbxcxd$ over $\mathrm{Syl}_2(\infty)$ induces a measure-preserving transformation on this group.

4.3. Ergodic polynomials over profinite groups. In contrast to the case of measure-preserving polynomials over groups, ergodic ones exist not over every profinite group G_∞, even if all the groups G_n forming the corresponding inverse spectrum are solvable. From Theorem 4.1 it follows that whenever a profinite group G_∞ has an ergodic polynomial, the group must be the inverse limit of finite groups having transitive polynomials; and *not* every finite solvable group has a transitive polynomial. From Theorems 3.5 and 3.7 we can see that the groups listed there fall into several inverse spectra. For instance, all dihedral groups D_k, $k = 2, 3, 4, \dots$, form an inverse spectrum

$$\dots \xrightarrow{\varphi_{k+1}} \mathrm{D}_k \xrightarrow{\varphi_k} \mathrm{D}_{k-1} \xrightarrow{\varphi_{k-1}} \dots \xrightarrow{\varphi_3} \mathrm{D}_2,$$

where the kernels of the epimorphisms φ_k are the centers of the corresponding dihedral groups:

$$\ker \varphi_k = \mathrm{Z}(\mathrm{D}_{k+1}) = \bigl\{1, v^{2^{k-1}}\bigr\}, \qquad k = 2, 3, 4, \dots .$$

The limit group of this inverse spectrum is a group $\mathbf{D}_\infty$, which is a split extension of the additive group $\mathbb{Z}_2^+$ of 2-adic integers by a cyclic group of order 2; the latter group acts on $\mathbb{Z}_2^+$ by taking negatives: $z \mapsto -z$, $z \in \mathbb{Z}_2$.[8] Thus, we may think of elements of the group $\mathbf{D}_\infty$ as pairs (ε, z), where $\varepsilon \in \mathbb{F}_2 = \{0, 1\}$ and $z \in \mathbb{Z}_2$. The multiplication $\cdot$ of these pairs is defined by the rule

$$(\varepsilon_1, z_1) \cdot (\varepsilon_2, z_2) = \bigl(\varepsilon_1 \oplus \varepsilon_2, (-1)^{\varepsilon_2} z_1 + z_2\bigr),$$

where $\oplus$ stands for addition modulo 2. The subgroup $Z \cong \mathbb{Z}_2^+$ and the subgroup $V \subset \mathrm{D}_k$, which is a cyclic subgroup of order 2^k generated by $v \in \mathrm{D}_k$, are characteristic subgroups in D_∞ and D_k, respectively. Hence, combining Corollary 3.2 with Theorem 4.1, we conclude that a polynomial $w(x)$ over the group $\mathbf{D}_\infty$ with operators $\Omega = \mathrm{Aut}(\mathbf{D}_\infty)$ is ergodic if and only if it is transitive on the factor group $\mathbf{D}_\infty/Z$ and the polynomial $w^2(x)$ is ergodic on Z. However, as every automorphism of $Z \cong \mathbb{Z}_2^+$ is a multiplication by a unit from $\mathbb{Z}_2$ (and vice versa), the polynomial $w^2(x)$ induces an affine transformation $x \mapsto a + bx$ on $\mathbb{Z}_2$ for suitable $a, b \in \mathbb{Z}_2$. By Theorem 1.9, an affine transformation is ergodic on $\mathbb{Z}_2$ if and only if it is transitive modulo 4. So we have finally proved the following result:

Proposition 4.9. *A polynomial over the group* $\mathbf{D}_\infty$ *with operators* $\mathrm{Aut}(\mathbf{D}_\infty)$ *is ergodic if and only if it is transitive on the dihedral group* D_2 *of order* 8.

Example 4.10. The polynomial $\widetilde{w}(x) = zx^{\widetilde{\alpha}}$, where $z = (1, 1) \in \mathbf{D}_\infty$ and the automorphism $\widetilde{\alpha}$ takes $(1, 0)$ to $(1, 1)$ and acts on the subgroup $\mathbb{Z}_2^+ \subset \mathbf{D}_\infty$ identically, is ergodic on the group $\mathbf{D}_\infty$ with operators $\mathrm{Aut}(\mathbf{D}_\infty)$.

[8] Note that the group $\mathbf{D}_\infty$ is *not* the infinite dihedral group D_∞; the latter group is a split extension of $\mathbb{Z}^+$ by the group of order 2.

Consider a polynomial $w(x) = uvx^\alpha$ over the group D_2 with operators $\mathrm{Aut}(\mathrm{D}_2)$, where the automorphism α takes u to $u^\alpha = uv$ and v to $v^\alpha = v$. The polynomial $w(x)$ is transitive on the dihedral group D_2. Indeed, the second iterate $w^2(x) = vx^{\alpha^2}$ induces a transitive transformation $v^i \mapsto v^{i+1}$ on the subgroup V generated by $v \in \mathrm{D}_2$, and the polynomial $w(x)$ induces a transitive transformation $x \mapsto ux$ on the factor group D_2/V, so the conclusion follows from Corollary 3.2. In view of Proposition 4.9, this proves the ergodicity of the polynomial $\widetilde{w}(x)$ on the group $\mathbf{D}_\infty$.

After minor modification the argument that proves Proposition 4.9 can be applied to the group $\mathbf{D}_\infty$ with operators $\mathrm{End}(\mathbf{D}_\infty)$. Since the subgroups Z and V are not fully invariant in the respective groups, we must use the first derived groups $\mathbf{D}'_\infty$ and D'_k instead. Note that $\mathbf{D}'_\infty \cong 2\mathbb{Z}_2^+$ and D'_k is a cyclic group of order 2^{k-1} generated by v^2. Thus we obtain

Proposition 4.11. *A polynomial over the group $\mathbf{D}_\infty$ with operators $\mathrm{End}(\mathbf{D}_\infty)$ is ergodic if and only if it is transitive on the dihedral group D_3 of order 16.*

Combining Theorem 4.1 with Proposition 1.2, from Propositions 4.9 and 4.11 we immediately deduce the following corollary:

Corollary 4.12. *A polynomial over the dihedral group D_k with operators $\mathrm{Aut}(\mathrm{D}_k)$ (respectively, $\mathrm{End}(\mathrm{D}_k)$, $k \geq 3$) is transitive if and only if it is transitive on the dihedral group D_2 of order 8 (respectively, on the dihedral group D_3 of order 16).*

We can now determine whether a given polynomial over a semidihedral or generalized quaternion group is transitive on these groups, although neither semidihedral groups nor generalized quaternion groups form inverse spectra. Indeed, by Corollary 3.2 a polynomial $w(x)$ over the semidihedral group SD_k with operators $\mathrm{End}(\mathrm{SD}_k)$ is transitive on this group if and only if $w(x)$ is transitive modulo the derived group SD'_k (i.e., on the factor group $\mathrm{SD}_k/\mathrm{SD}'_k \cong \mathrm{K}_4$) and the polynomial $w^4(x)$ is transitive on the subgroup SD'_k, which is a fully invariant cyclic subgroup of order 2^{k-1} generated by the element v^2. Note that $(v^2)^u = v^{2(2^{k-1}-1)} = v^{-2}$. Since $\mathrm{End}(\mathrm{SD}'_k) \cong \mathbb{Z}/2^{k-1}\mathbb{Z}$, the polynomial $w^4(x)$ acts on $\mathrm{SD}'_k \cong (\mathbb{Z}/2^{k-1}\mathbb{Z})^+$ as an affine map, which is transitive on this subgroup if and only if it is transitive modulo 4, by Theorem 1.9. However, by this theorem an affine polynomial on a cyclic group of order 2^s is transitive on this group if and only if it is transitive modulo 2^{s-i} for some (equivalently, any) $i \leq s-2$, i.e., on an arbitrary proper factor group whose order is ≥ 4. Hence, the polynomial $w^4(x)$ is transitive on SD'_k if and only if the polynomial $(w^4\psi)(x)$ is transitive on the factor group SD'_k/V, where V is a cyclic subgroup generated by $v^{2^{k-1}}$ and $\psi\colon \mathrm{SD}_k \to \mathrm{SD}_k/V$ is a canonical epimorphism. However, $V = L_k(\mathrm{SD}_k)$, the kth subgroup from the lower central series of the group SD_k; so V is fully invariant. Furthermore, $\mathrm{SD}_k/V \cong \mathrm{D}_{k-1}$, the dihedral group of order 2^k, $\mathrm{SD}_k/\mathrm{SD}'_k \cong \mathrm{D}_{k-1}/\mathrm{D}'_{k-1} \cong \mathrm{K}_4$, and thus $w(x)$ is transitive on $\mathrm{SD}_k/\mathrm{SD}'_k$ if and only if $(w\psi)(x)$ is transitive on $\mathrm{D}_{k-1}/\mathrm{D}'_{k-1}$. So we conclude that the polynomial $w(x)$ is transitive on SD_k if and only if the polynomial $(w\psi)(x)$ is transitive on the dihedral group D_{k-1}. However, by Corollary 4.12, a polynomial over the dihedral group D_{k-1} with operators $\mathrm{End}(\mathrm{D}_{k-1})$ is transitive if and only if it is transitive on the dihedral group of order 16. Thus, we have proved the following statement:

Corollary 4.13. *A polynomial $w(x)$ over the semidihedral group SD_k, $k \geq 4$, with operators $\mathrm{End}(\mathrm{SD}_k)$ is transitive on this group if and only if the polynomial $(w\varphi)(x)$ is transitive on the dihedral group D_3 of order 16. Here $\varphi\colon \mathrm{SD}_k \to \mathrm{D}_3$ is an epimorphism with a kernel $L_4(\mathrm{SD}_k)$, which is a cyclic subgroup generated by v^8.*

Remark 4.14. The statement of Corollary 4.13 remains true after replacing the semidihedral group SD_k by the generalized quaternion group Q_k. Furthermore, if we also replace $\mathrm{End}(\mathrm{Q}_k)$ by $\mathrm{Aut}(\mathrm{Q}_k)$, then we may replace D_3 by D_2 without affecting the validity of the statement. The proof mimics the one for semidihedral groups, and we omit it.

Example 4.15. The polynomial $w(x) = uvx^\alpha$, where the automorphism α takes u to $u^\alpha = uv$ and v to $v^\alpha = v$, is transitive on the generalized quaternion group Q_k with operators $\mathrm{Aut}(\mathrm{Q}_k)$.

Indeed, by Remark 4.14 it suffices to consider a transformation induced by this polynomial on the dihedral group D_2. By Example 4.10, the latter transformation is ergodic on $\mathbf{D}_\infty$; thus, it is transitive on all D_k.

It is clear now that in a similar manner one can prove ergodicity criteria for other groups that are the inverse limits of groups listed in Theorem 3.7. We will not consider all these inverse limits, restricting our considerations to some typical examples.

The cyclic groups $\mathrm{C}(p^k)$, $k = 1, 2, \dots, p$ prime, are groups of type (1) of Theorem 3.7. They form a spectrum whose inverse limit is isomorphic to the additive group $\mathbb{Z}_p^+$ of p-adic integers. As follows from the definition of a polynomial over a universal algebra (see, e.g., [65]), all polynomials over this group are of the form $w(x) = g + hx$, where $g, h \in \mathbb{Z}_p$. Thus, they induce affine transformations. By Theorem 1.9, the latter transformations are ergodic on $\mathbb{Z}_p^+$ if and only if they are transitive either on $\mathbb{Z}/p\mathbb{Z}$ if p is odd or on $\mathbb{Z}/4\mathbb{Z}$ if p is even.

The groups of type (2) of Theorem 3.7 are metacyclic groups $\mathrm{M}(m, k, s)$. They fall into different inverse spectra. For instance, let p and q be distinct primes, $p \mid q-1$. Consider a group $\mathbf{M}(p, q, s) = \mathbb{Z}_p^+ \leftthreetimes \mathbb{Z}_q^+$, where the action of $\mathbb{Z}_p^+$ on $\mathbb{Z}_q^+$ is defined as follows: Take an arbitrary pth root $s \in \mathbb{Z}_q$ of 1, $s \neq 1$. Then for every $z \in \mathbb{Z}_p$ the element $s^z \in \mathbb{Z}_q$ is well defined. Note that $s^z = 1$ for all $z \in p\mathbb{Z}_p$. The elements of the group $\mathbf{M}(p, q, s)$ can be considered as pairs (g, h), where $g \in \mathbb{Z}_p$ and $h \in \mathbb{Z}_q$, and the multiplication $\cdot$ of these pairs is defined as

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 + g_2, s^{g_2} h_1 + h_2).$$

It is clear that the group $\mathbf{M}(p, q, s)$ is a limit group of the inverse spectrum formed by metacyclic groups of type $\mathrm{M}(p^n, q^n, s \bmod q^n)$:

$$\dots \xrightarrow{\varphi_n} \mathrm{M}(p^n, q^n, s \bmod q^n) \xrightarrow{\varphi_{n-1}} \dots \xrightarrow{\varphi_1} \mathrm{M}(p, q, s \bmod q).$$

If we represent the elements of the group $\mathrm{M}(p^n, q^n, s \bmod q^n)$ by pairs (g, h), where $g \in \mathbb{Z}/p^n\mathbb{Z}$ and $h \in \mathbb{Z}/q^n\mathbb{Z}$, and define the multiplication of these pairs in the same way as for the group $\mathbf{M}(p, q, s)$, then the epimorphism φ_{n-1} is the reduction modulo p^{n-1} and q^{n-1} of the respective coordinates; i.e., $\varphi_n \colon (g, h) \mapsto (g \bmod p^{n-1}, h \bmod q^{n-1})$. By Corollary 3.2, a polynomial $w(x)$ over the group $\mathrm{M}(p^n, q^n, s \bmod q^n)$ is transitive if and only if, first, the polynomial $w(x)$ induces a transitive transformation on the factor group $\mathrm{M}(p^n, q^n, s \bmod q^n)/Z_{q^n} \cong Z_{p^n} \cong \mathrm{C}(p^n)$, where $Z_{q^n} \cong \mathrm{C}(q^n)$ and Z_{p^n} are cyclic subgroups generated by $(0, 1)$ and $(1, 0)$, respectively, and, second, the p^nth iterate $w^{p^n}(x)$ of the polynomial $w(x)$ induces a transitive transformation on the subgroup Z_{q^n}. As these transformations are affine transformations of the residue rings $\mathbb{Z}/p^n\mathbb{Z}$ and $\mathbb{Z}/q^n\mathbb{Z}$, respectively, Theorem 1.9 gives sufficient and necessary conditions for their transitivity. So we conclude that *a polynomial over the group* $\mathbf{M}(p, q, s)$ *is ergodic if and only if it induces a transitive transformation either on the factor group* $\mathrm{M}(p, q, s \bmod q)$ *if* p *is odd or on the factor group* $\mathrm{M}(4, q^2, s \bmod q^2)$ *if* $p = 2$. The cases when p and/or q are composite can be reduced to the considered case in view of the Chinese reminder theorem.

Example 4.16. The polynomial $w(x) = (1, 0) \cdot x \cdot (0, 1)$ is ergodic on the group $\mathbf{M}(p, q, s)$.

Indeed, this polynomial induces a transformation $(g, h) \mapsto (g + 1, h + 1)$, which is obviously transitive on the respective group.

In a similar manner we could obtain criteria of ergodicity for polynomials over the inverse limits of other groups listed in Theorem 3.7. Loosely speaking, all these criteria say that *a polynomial over the inverse limit of a spectrum of groups is ergodic if and only if it induces a transitive transformation on the smallest group of the spectrum.*

For instance, consider the groups $\mathrm{SQ}_1(n) \leftthreetimes \mathrm{M}(p^n, q^n, s \bmod q^n)$ of type (15), $n = 1, 2, \dots$, where p, q, and s are as above and $p, q > 3$. These groups obviously form an inverse spectrum. The group

$\mathrm{SQ}_1(n) \leftthreetimes \mathrm{M}(p^n, q^n, s \bmod q^n)$ can be represented as follows:

$$\mathrm{SQ}_1(n) \leftthreetimes \mathrm{M}(p^n, q^n, s \bmod q^n) = \big((\mathrm{C}(2) \leftthreetimes \mathrm{C}(3^n)) \times \mathrm{C}(p^n)\big) \leftthreetimes (\mathrm{Q}_2 \times \mathrm{C}(q^n)).$$

Thus, the limit group $\mathbf{SQ}_1 \leftthreetimes \mathbf{M}(p,q,s)$ of this inverse spectrum can be represented as $((\mathrm{C}(2) \leftthreetimes \mathbb{Z}_3^+) \times \mathbb{Z}_p^+) \leftthreetimes (\mathrm{Q}_2 \times \mathbb{Z}_q^+)$, where $\mathbf{SQ}_1 = \mathrm{C}(2) \leftthreetimes \mathbb{Z}_3 \leftthreetimes \mathrm{Q}_2$, the cyclic group $\mathrm{C}(2)$ of order 2 acts on $\mathbb{Z}_3^+$ and on $\mathbb{Z}_q^+$ by the negation $z \mapsto -z$, the group $\mathrm{C}(2) \leftthreetimes \mathbb{Z}_3^+$ acts on the quaternion group Q_2 as a symmetric group $\mathrm{Sym}(3)$ (so $3\mathbb{Z}_3$ centralizes Q_2),[9] and $\mathbb{Z}_p^+$ centralizes Q_2 and acts on $\mathbb{Z}_q^+$ by multiplication by s, the nonidentity pth root of 1. As in the case of metacyclic groups, we can prove that a polynomial over this inverse limit is ergodic if and only if it is ergodic on the group $\mathrm{SQ}_1(1) \leftthreetimes \mathrm{M}(p,q,s \bmod q)$.

Example 4.17. Let the group $G = \mathbf{SQ}_1 \leftthreetimes \mathbf{M}(p,q,s)$ be represented as above. Then the following polynomial $w(x)$ is ergodic: $w(x) = acx^2uvx^5bx^{24n}d$, where

- a is a generator of the subgroup $\mathrm{C}(2)$,
- $b \in \mathbb{Z}_3^+ \subset G$ is any 3-adic integer congruent to 1 modulo 3,
- $c \in \mathbb{Z}_p^+ \subset G$ is any p-adic integer congruent to 1 modulo p,
- $d \in \mathbb{Z}_q^+$ is any q-adic integer congruent to 1 modulo q,
- n is an arbitrary rational integer such that $6 + 24n \equiv 0 \pmod{pq}$; i.e., $4n \equiv -1 \pmod{pq}$.

Note that we write the operation in the subgroups $\mathbb{Z}_3^+, \mathbb{Z}_p^+, \mathbb{Z}_q^+ \subset G$ additively, although the operation in the group G is written in the multiplicative form.

By what was said, we only need to show that the polynomial $\overline{w}(x) = (w\varphi)(x)$ is transitive on the group $\mathrm{SQ}_1(1) \leftthreetimes \mathrm{M}(p,q,s \bmod q)$, where $\varphi\colon G \to \mathrm{SQ}_1(1) \leftthreetimes \mathrm{M}(p,q,s \bmod q)$ is an epimorphism that maps $\mathbb{Z}_3^+$, $\mathbb{Z}_p^+$, and $\mathbb{Z}_q^+$ onto $\mathrm{C}(3) \subset \mathrm{SQ}_1(1)$, $\mathrm{C}(p) \subset \mathrm{M}(p,q,s \bmod q)$, and $\mathrm{C}(q) \subset \mathrm{M}(p,q,s \bmod q)$, respectively. However, this was already shown during the proof of the sufficiency of the conditions of Theorem 3.7 (see [2]).

It is clear that in the general case the inverse limit of groups listed in Theorem 3.7 is, loosely speaking, a group that is an extension of an additive group of k-adic integers by a group composed of additive groups of m-adic integers and/or small finite groups K_4, Q_8, and $\mathrm{C}(2)$. We do not list all these profinite groups here, leaving this work as an exercise to the interested reader; we only mention that *actually the corresponding dynamics can be reduced to affine actions on ℓ-adic integers $\mathbb{Z}_\ell$*, and the latter actions form a nonautonomous dynamical system on $\mathbb{Z}_\ell$.

It is worth mentioning that the methods developed here for polynomials over groups with operators work in a much more general setting, for polynomial dynamics over noncommutative universal algebras such as groups with multioperators, which are merely groups with extended group signature. Although the latter groups arise in numerous applications, there were no reason, in our view, to develop in this paper a general theory of the corresponding dynamical systems. However, we emphasize that our approach works in a much more general situation, for the inverse limits of finite universal algebras of a very general nature; and we mention once again that the corresponding dynamical systems will inevitably be non-Archimedean.

REFERENCES

1. S. Albeverio, M. Gundlach, A. Khrennikov, and K.-O. Lindahl, "On the Markovian Behavior of p-adic Random Dynamical Systems," Russ. J. Math. Phys. **8** (2), 135–152 (2001).
2. V. S. Anashin, "Solvable Groups with Operators and Commutative Rings Having Transitive Polynomials," Algebra Logika **21** (6), 627–646 (1982) [Algebra Logic **21**, 419–432 (1982)].
3. V. S. Anashin, "Uniformly Distributed Sequences of p-adic Integers," Mat. Zametki **55** (2), 3–46 (1994) [Math. Notes **55**, 109–133 (1994)].

[9] Recall that $\mathrm{Aut}(\mathrm{Q}_2) \cong \mathrm{Sym}(3)$.

4. V. Anashin, "Uniformly Distributed Sequences over p-adic Integers," in *Number Theoretic and Algebraic Methods in Computer Science: Proc. Int. Conf., Moscow, June–July 1993*, Ed. by A. J. van der Poorten, I. Shparlinsky, and H. G. Zimmer (World Sci., Singapore, 1995), pp. 1–18.
5. V. S. Anashin, "Uniformly Distributed Sequences in Computer Algebra or How to Construct Program Generators of Random Numbers," J. Math. Sci. **89** (4), 1355–1390 (1998).
6. V. S. Anashin, "Uniformly Distributed Sequences of p-adic Integers," Diskret. Mat. **14** (4), 3–64 (2002) [Discrete Math. Appl. **12**, 527–590 (2002)]; arXiv: math/0209407.
7. V. S. Anashin, "Pseudorandom Number Generation by p-adic Ergodic Transformations," arXiv: cs/0401030.
8. V. S. Anashin, "Pseudorandom Number Generation by p-adic Ergodic Transformations: An Addendum," arXiv: cs/0402060.
9. V. Anashin, "Ergodic Transformations in the Space of p-adic Integers," in *p-Adic Mathematical Physics: Proc. 2nd Int. Conf. Belgrade, Serbia and Montenegro, Sept. 15–21, 2005*, Ed. by A. Yu. Khrennikov, Z. Rakić, and I. V. Volovich (Am. Inst. Phys., Melville, NY, 2006), AIP Conf. Proc. **826**, pp. 3–24; arXiv: math/0602083.
10. V. S. Anashin, *Non-Archimedean Analysis, T-Functions, and Cryptography* (Maks Press, Moscow, 2006), Mathematical Methods and Technologies in Computer Security: Lect. Notes Int. Summer School, Moscow State Univ., 2006; arXiv: cs/0612038.
11. V. S. Anashin, "Wreath Products in Stream Cipher Design," in *Security and Counteracting Terrorism: Proc. Int. Conf., Moscow, Nov. 2–3, 2005* (MCCME, Moscow, 2006), pp. 135–161; arXiv: cs/0602012.
12. V. Anashin, "Non-Archimedean Ergodic Theory and Pseudorandom Generators," Comput. J., doi:10.1093/comjnl/bxm101 (2008).
13. V. S. Anashin and M. V. Larin, "Interpolation on A_5," in *Abstracts of the 8th All-Union Symp. on Group Theory, Sumy, Ukraine, 1982*, pp. 6–7.
14. D. K. Arrowsmith and F. Vivaldi, "Some p-adic Representations of the Smale Horseshoe," Phys. Lett. A **176**, 292–294 (1993).
15. D. K. Arrowsmith and F. Vivaldi, "Geometry of p-adic Siegel Discs," Physica D **71**, 222–236 (1994).
16. A. Batra and P. Morton, "Algebraic Dynamics of Polynomial Maps on the Algebraic Closure of a Finite Field. I," Rocky Mt. J. Math. **24** (2), 453–481 (1994).
17. A. Batra and P. Morton, "Algebraic Dynamics of Polynomial Maps on the Algebraic Closure of a Finite Field. II," Rocky Mt. J. Math. **24** (3), 905–932 (1994).
18. S. Ben-Menahem, "p-Adic Iterations," Preprint TAUP 1627-88 (Tel Aviv Univ., 1988).
19. R. L. Benedetto, "Fatou Components in p-adic Dynamics," PhD Thesis (Dept. Math., Brown Univ., May 1998).
20. R. L. Benedetto, "p-Adic Dynamics and Sullivan's No Wandering Domains Theorem," Compos. Math. **122**, 281–298 (2000).
21. R. L. Benedetto, "Hyperbolic Maps in p-adic Dynamics," Ergodic Theory Dyn. Syst. **21**, 1–11 (2001).
22. R. L. Benedetto, "Reduction, Dynamics, and Julia Sets of Rational Functions," J. Number Theory **86**, 175–195 (2001).
23. R. L. Benedetto, "Components and Periodic Points in Non-Archimedean Dynamics," Proc. London Math. Soc. **84**, 231–256 (2002).
24. R. L. Benedetto, "Examples of Wandering Domains in p-adic Polynomial Dynamics," C. R., Math., Acad. Sci. Paris **335**, 615–620 (2002).
25. R. L. Benedetto, "Non-Archimedean Holomorphic Maps and the Ahlfors Islands Theorem," Am. J. Math. **125**, 581–622 (2003).
26. R. L. Benedetto, "Heights and Preperiodic Points of Polynomials over Function Fields," Int. Math. Res. Not., No. 62, 3855–3866 (2005).
27. R. L. Benedetto, "Wandering Domains in Non-Archimedean Polynomial Dynamics," Bull. London Math. Soc. **38**, 937–950 (2006).
28. R. L. Benedetto, "Periodic Points of Polynomials over Global Fields," J. Reine Angew. Math. **608**, 123–153 (2007).
29. J.-P. Bézivin, "Sur les points périodiques des applications rationnelles en dynamique ultramétrique," Acta Arith. **100**, 63–74 (2001).
30. J.-P. Bézivin, "Sur les ensembles de Julia et Fatou des fonctions entières ultramétriques," Ann. Inst. Fourier **51**, 1635–1661 (2001).
31. J.-P. Bézivin, "Fractions rationnelles hyperboliques p-adiques," Acta Arith. **112**, 151–175 (2004).
32. J.-P. Bézivin, "Sur la compacité des ensembles de Julia des polynômes p-adiques," Math. Z. **246**, 273–289 (2004).
33. G. S. Call and J. H. Silverman, "Canonical Heights on Varieties with Morphisms," Compos. Math. **89**, 163–205 (1993).

34. W.-S. Chou and I. E. Shparlinski, "On the Cycle Structure of Repeated Exponentiation Modulo a Prime," J. Number Theory **107**, 345–356 (2004).
35. R. Crowell and R. Fox, *Introduction to Knot Theory* (Ginn and Co., Boston, 1963).
36. D. L. desJardins and M. E. Zieve, "On the Structure of Polynomial Mappings Modulo an Odd Prime Power," arXiv: math/0103046.
37. B. Dragovich and A. Dragovich, "A p-adic Model of DNA Sequence and Genetic Code," arXiv: q-bio/0607018.
38. A.-H. Fan, M.-T. Li, J.-Y. Yao, and D. Zhou, "p-Adic Affine Dynamical Systems and Applications," C. R., Math., Acad. Sci. Paris **342**, 129–134 (2006).
39. A.-H. Fan, M.-T. Li, J.-Y. Yao, and D. Zhou, "Strict Ergodicity of Affine p-adic Dynamical Systems on $\mathbb{Z}_p$," Adv. Math. **214**, 666–700 (2007).
40. A. Fan, L. Liao, Y. F. Wang, and D. Zhou, "p-Adic Repellers in $\mathbb{Q}_p$ Are Subshifts of Finite Type," C. R., Math., Acad. Sci. Paris **344**, 219–224 (2007).
41. C. Favre and J. Rivera-Letelier, "Théorème d'équidistribution de Brolin en dynamique p-adique," C. R., Math., Acad. Sci. Paris **339**, 271–276 (2004).
42. M. Gundlach, A. Khrennikov, and K.-O. Lindahl, "Topological Transitivity for p-adic Dynamical Systems," in *p-Adic Functional Analysis*, Ed. by A. K. Katsaras, W. H. Schikhof, and L. van Hamme (M. Dekker, New York, 2001), Lect. Notes Pure Appl. Math. **222**, pp. 127–132.
43. M. Gundlach, A. Khrennikov, and K.-O. Lindahl, "On Ergodic Behavior of p-adic Dynamical Systems," Infin. Dimens. Anal. Quantum Probab. Relat. Top. **4** (4), 569–577 (2001).
44. V. M. Gundlach, A. Yu. Khrennikov, and K.-O. Lindahl, "Ergodicity on p-adic Sphere," in *German Open Conference on Probability and Statistics* (Univ. Hamburg Press, Hamburg, 2000), pp. 15–21.
45. P. R. Halmos, *Lectures on Ergodic Theory* (Kenkyusha, Tokyo, 1956), Publ. Math. Soc. Japan, No. 3.
46. M. R. Herman and J.-C. Yoccoz, "Generalizations of Some Theorems of Small Divisors to Non-Archimedean Fields," in *Geometric Dynamics* (Springer, Berlin, 1983), Lect. Notes Math. **1007**, pp. 408–447.
47. L.-C. Hsia, "A Weak Néron Model with Applications to p-adic Dynamical Systems," Compos. Math. **100**, 277–304 (1996).
48. L.-C. Hsia, "Closure of Periodic Points over a Non-Archimedean Field," J. London Math. Soc. **62**, 685–700 (2000).
49. D. Jonah and B. M. Schreiber, "Transitive Affine Transformations on Groups," Pac. J. Math. **58** (2), 483–509 (1975).
50. A. Yu. Khrennikov, *p-Adic Valued Distributions in Mathematical Physics* (Kluwer, Dordrecht, 1994).
51. A. Yu. Khrennikov, "A p-adic Behaviour of the Standard Dynamical Systems," Preprint No. 290 (SFB-237) (Ruhr Univ. Bochum, 1995).
52. A. Yu. Khrennikov, *Non-Archimedean Analysis: Quantum Paradoxes, Dynamical Systems and Biological Models* (Kluwer, Dordrecht, 1997).
53. A. Yu. Khrennikov, "p-Adic Information Space and Gene Expression," in *Integrative Approaches to Brain Complexity*, Ed. by S. Grant, N. Heintz, and J. Noebels (Wellcome Trust Publ., Cambridge, 2006), p. 14.
54. A. Yu. Khrennikov and S. V. Kozyrev, "Genetic Code on the Dyadic Plane," Physica A: Stat. Mech. Appl. **381**, 265–272 (2007).
55. A. Khrennikov, K.-O. Lindahl, and M. Gundlach, "Ergodicity in the p-adic Framework," in *Operator Methods in Ordinary and Partial Differential Equations* (Birkhäuser, Basel, 2002), Operator Methods: Adv. Appl. **132**, pp. 245–251.
56. A. Khrennikov and M. Nilsson, "Behaviour of Hensel Perturbations of p-adic Monomial Dynamical Systems," Anal. Math. **29**, 107–133 (2003).
57. A. Yu. Khrennikov and M. Nilsson, *p-Adic Deterministic and Random Dynamics* (Kluwer, Dordrecht, 2004).
58. J. Kingsbery, A. Levin, A. Preygel, and C. E. Silva, "Measurable Dynamics of Maps on Profinite Groups," Indag. Math. **18** (4), 561–581 (2007); arXiv: math/0701899v1.
59. L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences* (J. Wiley & Sons, New York, 1974).
60. K. Kuratowski, *Topology* (Academic, New York, 1966), Vol. 1.
61. M. V. Larin, "Transitive Polynomial Transformations of Residue Class Rings," Diskret. Mat. **14** (2), 20–32 (2002) [Discrete Math. Appl. **12**, 127–140 (2002)].
62. F. Laubie, A. Movahhedi, and A. Salinier, "Systèmes dynamiques non archimédiens et corps des normes," Compos. Math. **132**, 57–98 (2002).
63. H. Lausch, "Zur Theorie der Polynompermutationen über endlichen Gruppen," Arch. Math. **19** (3), 284–288 (1968).
64. H. Lausch, "Interpolation on the Alternating Group A_5," in *Contributions to General Algebra: Proc. Klagenfurt Conf. 1978* (Klagenfurt, 1979), pp. 187–192.

65. H. Lausch and W. Nöbauer, *Algebra of Polynomials* (North-Holland, Amsterdam, 1973).
66. H.-C. Li, "Counting Periodic Points of p-adic Power Series," Compos. Math. **100**, 351–364 (1996).
67. H.-C. Li, "p-Adic Dynamical Systems and Formal Groups," Compos. Math. **104**, 41–54 (1996).
68. H.-C. Li, "p-Adic Periodic Points and Sen's Theorem," J. Number Theory **56**, 309–318 (1996).
69. H.-C. Li, "When Is a p-adic Power Series an Endomorphism of a Formal Group?," Proc. Am. Math. Soc. **124**, 2325–2329 (1996).
70. H.-C. Li, "Isogenies between Dynamics of Formal Groups," J. Number Theory **62**, 284–297 (1997).
71. H.-C. Li, "p-Adic Power Series Which Commute under Composition," Trans. Am. Math. Soc. **349**, 1437–1446 (1997).
72. H.-C. Li, "On Heights of p-adic Dynamical Systems," Proc. Am. Math. Soc. **130**, 379–386 (2002).
73. H.-C. Li, "p-Typical Dynamical Systems and Formal Groups," Compos. Math. **130**, 75–88 (2002).
74. K.-O. Lindahl, "Dynamical Systems in p-adic Geometry," Licentiate Thesis (School Math. Syst. Eng., Växjö Univ., 2001).
75. K.-O. Lindahl, "On Siegel's Linearization Theorem for Fields of Prime Characteristic," Nonlinearity **17** (3), 745–763 (2004).
76. J. Lubin, "Nonarchimedean Dynamical Systems," Compos. Math. **94**, 321–346 (1994).
77. J. Lubin, "Sen's Theorem on Iteration of Power Series," Proc. Am. Math. Soc. **123**, 63–66 (1995).
78. J. Lubin, "Formal Flows on the Non-Archimedean Open Unit Disk," Compos. Math. **124**, 123–136 (2000).
79. M. Misiurewicz, J. G. Stevens, and D. M. Thomas, "Iterations of Linear Maps over Finite Fields," Linear Algebra Appl. **413**, 218–234 (2006); http://www.csam.montclair.edu/~thomasd/ducci.pdf
80. P. Morton, "Arithmetic Properties of Periodic Points of Quadratic Maps," Acta Arith. **62** (4), 343–372 (1992).
81. P. Morton, "Characterizing Cyclic Cubic Extensions by Automorphism Polynomials," J. Number Theory **49**, 183–208 (1994).
82. P. Morton, "On Certain Algebraic Curves Related to Polynomial Maps," Compos. Math. **103**, 319–350 (1996).
83. P. Morton, "Periods of Maps on Irreducible Polynomials over Finite Fields," Finite Fields Appl. **3**, 11–24 (1997).
84. P. Morton, "Galois Groups of Periodic Points," J. Algebra **201**, 401–428 (1998).
85. P. Morton and P. Patel, "The Galois Theory of Periodic Points of Polynomial Maps," Proc. London Math. Soc. **68**, 225–263 (1994).
86. P. Morton and J. H. Silverman, "Rational Periodic Points of Rational Functions," Int. Math. Res. Not., No. 2, 97–110 (1994).
87. P. Morton and J. H. Silverman, "Periodic Points, Multiplicities, and Dynamical Units," J. Reine Angew. Math. **461**, 81–122 (1995).
88. P. Morton and F. Vivaldi, "Bifurcations and Discriminants for Polynomial Maps," Nonlinearity **8** (4), 571–584 (1995).
89. W. Narkiewicz, "Polynomial Cycles in Algebraic Number Fields," Colloq. Math. **58**, 151–155 (1989).
90. W. Narkiewicz, *Polynomial Mappings* (Springer, Berlin, 1995).
91. W. Narkiewicz, "Arithmetics of Dynamical Systems: A Survey," Tatra Mt. Math. Publ. **11**, 69–75 (1997).
92. W. Narkiewicz, "Finite Polynomial Orbits: A Survey," in *Algebraic Number Theory and Diophantine Analysis: Proc. Int. Conf. Graz, Austria, Aug. 30–Sept. 5, 1998*, Ed. by F. Halter-Koch et al. (W. de Gruyter, Berlin, 2000), pp. 331–338.
93. W. Narkiewicz and T. Pezda, "Finite Polynomial Orbits in Finitely Generated Domains," Monatsh. Math **124**, 309–316 (1997).
94. M. Nilsson, "Fuzzy Cycles of p-adic Monomial Dynamical Systems," Far East J. Dyn. Syst. **5** (2), 149–173 (2003).
95. R. Nyqvist, "Some Dynamical Systems in Finite Field Extensions of the p-adic Numbers," in *p-Adic Functional Analysis*, Ed. by A. K. Katsaras, W. H. Schikhof, and L. van Hamme (M. Dekker, New York, 2001), Lect. Notes Pure Appl. Math. **222**, pp. 243–253.
96. D. Passman, *Permutation Groups* (W.A. Benjamin, Inc., New York, 1968).
97. A. Peinado, F. Montoya, J. Muñoz, and A. J. Yuste, "Maximal Periods of $x^2 + c$ in $\mathbb{F}_q$," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* (Springer, Berlin, 2001), Lect. Notes Comput. Sci. **2227**, pp. 219–228.
98. T. Pezda, "Cycles of Polynomial Mappings in Several Variables," Manuscr. Math. **83**, 279–289 (1994).
99. T. Pezda, "Cycles of Polynomials in Algebraically Closed Fields of Positive Characteristic," Colloq. Math. **67**, 187–195 (1994).
100. T. Pezda, "Polynomial Cycles in Certain Local Domains," Acta Arith. **66**, 11–22 (1994).
101. T. Pezda, "Cycles of Polynomials in Algebraically Closed Fields of Positive Characteristic. II," Colloq. Math. **71**, 23–30 (1996).

102. T. Pezda, "On Cycles and Orbits of Polynomial Mappings $\mathbb{Z}^2 \to \mathbb{Z}^2$," Acta Math. Inform. Univ. Ostrav. **10**, 95–102 (2002).
103. T. Pezda, "Cycles of Polynomial Mappings in Several Variables over Rings of Integers in Finite Extensions of the Rationals," Acta Arith. **108**, 127–146 (2003).
104. M. Rajagopalan and B. Schreiber, "Ergodic Automorphisms and Affine Transformations of Locally Compact Groups," Pac. J. Math. **38** (1), 167–176 (1971).
105. J. Rivera-Letelier, "Dynamique des fractions rationnelles sur des corps locaux," PhD Thesis (Univ. Paris-sud., Centre d'Orsay, 2000).
106. J. Rivera-Letelier, "Dynamique des fonctions rationnelles sur des corps locaux," in *Geometric Methods in Dynamics. II* (Soc. Math. France, Paris, 2003), Astérisque **287**, pp. 147–230.
107. J. Rivera-Letelier, "Espace hyperbolique p-adique et dynamique des fonctions rationnelles," Compos. Math. **138**, 199–231 (2003).
108. J. Rivera-Letelier, "Wild Recurrent Critical Points," arXiv: math/0406417.
109. J. A. G. Roberts and F. Vivaldi, "Signature of Time-Reversal Symmetry in Polynomial Automorphisms over Finite Fields," Nonlinearity **18** (5), 2171–2192 (2005).
110. P. Ruelle, E. Thiran, D. Verstegen, and J. Weyers, "Adelic String and Superstring Amplitudes," Mod. Phys. Lett. A **4**, 1745–1752 (1989).
111. I. E. Shparlinski, "On Some Dynamical Systems in Finite Fields and Residue Rings," Discrete Contin. Dyn. Syst. **17**, 901–917 (2007).
112. J. H. Silverman, "Geometric and Arithmetic Properties of the Hénon Map," Math. Z. **215**, 237–250 (1994).
113. J. H. Silverman, "The Field of Definition for Dynamical Systems on $\mathbb{P}^1$," Compos. Math. **98**, 269–304 (1995).
114. J. H. Silverman, "Rational Functions with a Polynomial Iterate," J. Algebra **180**, 102–110 (1996).
115. J. H. Silverman, *The Arithmetic of Dynamical Systems* (Springer, New York, 2007), Grad. Texts Math. **241**.
116. P.-A. Svensson, "Dynamical Systems in Unramified or Totally Ramified Extensions of the p-adic Number Field," in *Ultrametric Functional Analysis: Proc. Seventh Int. Conf. on p-adic Analysis* (Am. Math. Soc., Providence, RI, 2003), Contemp. Math. **319**, pp. 405–412.
117. E. Thiran, D. Verstegen, and J. Weyers, "p-Adic Dynamics," J. Stat. Phys. **54**, 893–913 (1989).
118. D. Verstegen, "p-Adic Dynamical Systems," in *Number Theory and Physics* (Springer, Berlin, 1990), Springer Proc. Phys. **47**, pp. 235–242.
119. F. Vivaldi, "Dynamics over Irreducible Polynomials," Nonlinearity **5** (4), 941–960 (1992).
120. F. Vivaldi and S. Hatjispyros, "Galois Theory of Periodic Orbits of Rational Maps," Nonlinearity **5** (4), 961–978 (1992).
121. V. S. Vladimirov and I. V. Volovich, "Superanalysis. I: Differential Calculus," Teor. Mat. Fiz. **59** (1), 3–27 (1984) [Theor. Math. Phys. **59**, 317–335 (1984)].
122. V. S. Vladimirov and I. V. Volovich, "Superanalysis. II: Integral Calculus," Teor. Mat. Fiz. **60** (2), 169–198 (1984) [Theor. Math. Phys. **60**, 743–765 (1984)].
123. V. S. Vladimirov, I. V. Volovich, and E. I. Zelenov, *p-Adic Analysis and Mathematical Physics* (Nauka, Moscow, 1994; World Sci., Singapore, 1994).
124. I. V. Volovich, "p-Adic String," Class. Quantum Grav. **4**, L83–L87 (1987).

This article was submitted by the author in English