

Contents

Preface	vii
1 Algebraic and number-theoretic background	1
1.1 Facts from number theory	1
1.1.1 Some useful equalities and congruences	1
1.1.2 Möbius and Euler functions, Legendre symbol	3
1.1.3 Distribution of prime numbers	5
1.2 Basic notions and facts from algebra	6
1.2.1 Universal algebras	6
1.2.2 Groups	9
1.2.3 Rings	14
1.3 Fields	17
1.3.1 Finite fields	17
1.3.2 Non-Archimedean fields	19
1.4 p -adic numbers	19
1.4.1 Canonical expansion of p -adic numbers	22
1.4.2 Tree-like structure of the p -adic numbers	24
1.5 Ultrametric spaces	24
1.6 The Haar measure	26
1.7 Non-Archimedean rings, m -adic numbers	28
1.8 Extensions of the field of p -adic numbers	29
1.8.1 Finite extensions of $\mathbb{Q}_p$	29
1.8.2 The algebraic closure of $\mathbb{Q}_p$	32
1.8.3 Complex p -adic numbers	33
1.8.4 Krasner's lemma	33
I The Commutative Non-Archimedean Dynamics	35
2 Dynamics on algebraic structures	37
2.1 Basic notions of dynamics	37
2.1.1 Ergodicity and uniform distribution of sequences	37

2.2	Dynamics on finite algebraic structures	39
2.2.1	Hereditary dynamical properties and compatibility	39
2.2.2	Ergodic polynomial transformations on finite Abelian groups with operators	41
2.2.3	Ergodic polynomial transformations on finite commutative rings	42
3	<i>p</i>-adic analysis	48
3.1	Analysis in complete non-Archimedean fields	48
3.2	Analytic functions	51
3.3	Hensel's lemma	52
3.4	Roots of unity	54
3.5	Non-Archimedean normed spaces	56
3.6	Multidimensional analysis	57
3.7	The differentiability modulo p^k	58
3.8	Compatible functions on $\mathbb{Z}_p$	62
3.8.1	Compatibility is equivalent to 1-Lipschitz	63
3.8.2	Compatibility and differentiability	66
3.9	Mahler expansion	75
3.9.1	Identities modulo p^k	76
3.9.2	Mahler expansions of compatible functions	78
3.10	Special classes of locally analytic functions	80
3.10.1	Class $\mathcal{C}$	80
3.10.2	Class $\mathcal{B}$	83
3.10.3	Class $\mathcal{A}$	87
4	<i>p</i>-adic ergodic theory	90
4.1	Discrete dynamical systems	90
4.2	Periodic points and their character	90
4.3	Monomial dynamics	93
4.3.1	Topologically transitive and minimality	94
4.3.2	Unique ergodicity	96
4.4	Measure-preserving and ergodic isometries on $\mathbb{Z}_p^n$	98
4.4.1	Measure-preserving isometries	100
4.4.2	1-Lipschitz measure-preserving functions	102
4.4.3	1-Lipschitz ergodic functions	105
4.5	Ergodic 1-Lipschitz transformations on $\mathbb{Z}_p$	106
4.5.1	Ergodicity of affine mappings	106
4.5.2	Ergodicity and measure-preservation in terms of coordinate functions	108
4.5.3	Ergodicity and measure-preservation in terms of Mahler ex- pansion	111

4.6	Measure-preservation and ergodicity of uniformly differentiable functions on $\mathbb{Z}_p^n$	119
4.6.1	Conditions for measure-preservation	119
4.6.2	No uniformly differentiable 1-Lipschitz ergodic transformations on $\mathbb{Z}_p^n, n \geq 2$	122
4.6.3	Differentiable ergodic transformations on $\mathbb{Z}_p$	125
4.6.4	Measure-preservation and ergodicity of $\mathcal{A}$ -, $\mathcal{B}$ -, and $\mathcal{C}$ -functions	132
4.7	Ergodic 1-Lipschitz transformations on p -adic spheres	148
4.7.1	1-Lipschitz ergodic transformations on spheres	148
4.7.2	Ergodicity of $\mathcal{B}$ -functions and of analytic functions	151
4.7.3	Ergodicity of perturbed monomial mappings	153
4.7.4	Ergodicity of $\mathcal{A}$ -functions on spheres	155
4.8	Concluding remarks to p -adic ergodic theory	156
4.8.1	Continuous p -adic dynamics	156
4.8.2	Non-minimal dynamics. Non-compatible dynamics. Mixing	159
5	Asymptotic distribution of cycles	162
5.1	Monomial systems in $\mathbb{C}_p$ and in finite extensions of $\mathbb{Q}_p$	163
5.2	Number of cycles of $x \mapsto x^n$ in $\mathbb{Q}_p$	166
5.3	Total number of cycles	169
5.4	Possible values of the number of cycles	171
5.5	Probability on the set of prime numbers	172
5.6	Distribution of cycles	174
5.7	Expectation value and dispersion	176
5.8	Fuzzy cycles	180
II	The Non-Commutative Non-Archimedean Dynamics	197
6	Basics of polynomial dynamics on groups	199
6.1	Non-commutative differential calculus	200
6.2	Bijective polynomials over finite groups	204
7	Ergodic polynomials over groups with operators	205
7.1	Basic properties of groups having ergodic polynomials	206
7.2	Finite solvable groups having ergodic polynomials	209
7.2.1	The multivariate case	209
7.2.2	The univariate case: Nilpotent groups	212
7.2.3	The univariate case: Solvable groups	217
7.3	Ergodic theory for profinite groups	232
7.3.1	Metric and measure on a profinite group	233

7.3.2	Equations, the non-commutative Hensel's lemma, and measure-preserving polynomials over profinite groups	235
7.3.3	Ergodic polynomials over profinite groups	237
III	Applications	243
8	Automata, computers, combinatorics	245
8.1	Automata functions are continuous	245
8.2	Computers think 2-adically	252
8.3	Differentiable instructions and programs	259
8.4	Latin squares	262
9	Pseudorandom numbers	269
9.1	Pseudorandom generator is a dynamical system	271
9.1.1	What pseudorandom generators are good?	272
9.1.2	Why p -adic ergodic theory?	274
9.2	Congruential generators of the longest period	275
9.2.1	Types of congruential generators	277
9.2.2	Periods of congruential generators	279
10	Stream ciphers	305
10.1	How secure are congruential generators?	306
10.2	Wreath products	309
10.3	Counter-dependent generators	314
10.3.1	Special output functions	325
10.4	Generators based on multivariate functions	328
10.5	Security issues	334
10.5.1	The number of transitive compatible mappings	335
10.5.2	Key recovery and intractability	337
11	Structure of trajectories	340
11.1	Distribution in Euclidean space	340
11.1.1	Points falling on hyperplanes	341
11.1.2	Lacunae	347
11.2	Properties of coordinate sequences	358
11.2.1	Linear and 2-adic complexities	359
11.2.2	Structure of coordinate sequences	366
11.3	Distribution of k -tuples	371
12	p-adic probability theory	377
12.1	Historical remarks	377
12.2	Frequency probability theory	379

12.3	Ensemble probability	385
12.3.1	Ensembles of infinite volumes	386
12.3.2	The rules for working with p -adic probabilities	391
12.3.3	Negative probabilities and p -adic ensemble probabilities	396
12.4	Measures	396
12.5	p -adic probability space	400
12.6	p -adic probability measures on the space of binary sequences	402
12.7	Some technical p -adic results	403
12.8	p -adic tests for randomness	404
12.9	Some limit theorems	408
12.10	Recursive enumeration of the set of p -adic tests	410
12.11	No p -adic universal test	413
13	p-adic valued quantization	415
13.1	Toward quantum mechanics with p -adic valued wave functions	415
13.2	Hilbert spaces	417
13.3	Groups of unitary isometric operators in the p -adic Hilbert space	419
13.4	Axiomatics of quantum mechanics with p -adic valued wave functions	421
13.5	Gaussian integral and spaces of square integrable functions	422
13.6	Gaussian representations of position and momentum operators	425
13.7	One parameter groups generated by position and momentum operators	427
13.8	Operator calculus	427
13.9	Spectrum of p -adic position operator	428
13.10	Concluding remarks on p -adic quantization	431
14	m-adic modeling in cognitive science and psychology	433
14.1	On modeling of mental quantities	434
14.1.1	Representation of mental states by numbers	434
14.1.2	Encoding by branches of trees	437
14.1.3	Dynamical system approach, artificial intelligence	438
14.1.4	Unconscious and conscious dynamics – Freudian approach	439
14.1.5	Neuronal hierarchy	441
14.2	Mental space	442
14.3	Dynamical thinking in mental space	442
14.4	Associations and ideas	443
14.5	Neuronal realization	444
14.6	Model of cognitive psychology	446
14.7	Dynamics of associations and ideas	447
14.8	Advantages of dynamical processing of associations and ideas	448
14.9	Transformation of unconscious mental flows into conscious flows	449
14.10	Hidden forbidden wishes, psychoanalysis	458
14.10.1	Hysteric reactions	460

14.10.2	Feedback control based on doubtful ideas	461
14.11	Neuro and mental cybernetic bases for the pleasure and reality principles	462
14.12	Consequences for psychology and neuropsychology	464
14.13	Consequences for psychoanalysis	465
14.14	Psycho-robots	467
15	Neuronal hierarchy behind the ultrametric mental space	468
15.1	Hierarchic neural pathways	469
15.2	Model: thinking on neuronal tree	470
15.2.1	Mental field on the brain	470
15.2.2	Probabilistic dynamics in the mental space	475
15.3	Diffusion model of dynamics of statistical mental state	478
15.3.1	Markovean body $\rightarrow$ mind fields	478
15.3.2	Thinking as m -adic diffusion	479
15.3.3	Discussion	481
15.4	Postulates	485
16	Gene expression from dynamics in the 2-adic space	487
16.1	Description of model	488
16.1.1	4-adic representation of nucleotides	488
16.1.2	DNA-reproduction and 4-adic dynamics	489
16.2	Genetic space	490
16.2.1	4-adic encoding of DNA and RNA	490
16.2.2	2-adic encoding	491
16.3	Dynamical model for degeneracy of the genetic code	492
17	Genetic code on the diadic plane	494
17.1	Vertebral mitochondrial and eucaryotic codes	495
17.2	Parametrization of the set of codons by the diadic plane	495
17.3	Genetic code on the diadic plane	498
17.4	Physical-chemical regularity of the genetic code	501
	Bibliography	503
	Notation	527
	Index	529